Securing Cognitive Wireless Sensor Networks: A Survey

Alexandros Fragkiadakis, Vangelis Angelakis and Elias Z. Tragos

Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 393248, 12 pages
http://dx.doi.org/10.1155/2014/393248

Review Article

Securing Cognitive Wireless Sensor Networks: A Survey

Alexandros Fragkiadakis,[1] Vangelis Angelakis,[2] and Elias Z. Tragos[1]

[1] *Institute of Computer Science, Foundation for Research and Technology-Hellas, Heraklion, 71110 Crete, Greece*
[2] *Department of Science and Technology, Linköping University, 58183 Linköping, Sweden*

Correspondence should be addressed to Alexandros Fragkiadakis; alfrag@ics.forth.gr

Received 1 January 2014; Accepted 23 February 2014; Published 27 March 2014

Academic Editor: Christos Verikoukis

Wireless sensor networks (WSNs) have gained a lot of attention recently due to the potential they provide for developing a plethora of cost-efficient applications. Although research on WSNs has been performed for more than a decade, only recently has the explosion of their potential applicability been identified. However, due to the fact that the wireless spectrum becomes congested in the unlicensed bands, there is a need for a next generation of WSNs, utilizing the advantages of cognitive radio (CR) technology for identifying and accessing the free spectrum bands. Thus, the next generation of wireless sensor networks is the cognitive wireless sensor networks (CWSNs). For the successful adoption of CWSNs, they have to be trustworthy and secure. Although the concept of CWSNs is quite new, a lot of work in the area of security and privacy has been done until now, and this work attempts to present an overview of the most important works for securing the CWSNs. Moreover, a discussion regarding open research issues is also given in the end of this work.

1. Introduction

WSNs are daily gaining more ground into our lives with applications ranging from construction monitoring and intelligent transport to smart home control and assisted living. Through the novel communication standards of the past decades such as Zigbee and IEEE 802.15.4, along with the pervasiveness of IEEE 802.11, the development of interoperability and commercial solutions has been enabled. Typically though, these solutions do suffer from strict deployment design and poor scalability. At the same time, the reliability of WSNs is a key topic for their mass adoption for more critical, rather than luxury or pilot, applications, such as the smart metering [1].

Cognitive radio (CR) features, such as the opportunistic spectrum (white space) usage, the introduction of secondary users in licensed bands, and the ability to learn the environment through sensing, present themselves as a mean to overcome spectrum shortage. Enabling such CR characteristics over "traditional" WSNs allows them to change their transmission parameters according to the radio environment and possibly enhance the reliability of WSNs in areas densely populated by wireless devices. These cognitive radio-imbued WSNs (CWSNs) can have access to new spectrum bands with better propagation characteristics. By adaptively changing system parameters like the modulation schemes, transmit power, carrier frequency, channel coding schemes, and constellation size, a wider variety of data rates can be achieved, especially when CWSNs operate on software-defined radios. This can improve device energy efficiency, network lifetime, and communication reliability.

The adoption of CR technology in CWSNs has largely improved network performance, but not without any cost. CWSNs, aside from being still open to a host of pure networking research issues, are also vulnerable to new types of threats. Attacks targeting a CWSN can come from both internal and external network sources. Adversaries can exploit vulnerabilities in different communication layers, many of which target the CR characteristics of the CWSN. There are also special types of attacks that try to infer sensitive information on the application and that execute in the sensors themselves [2]. Our work here aims to make a brief, yet succinct, overview of possible attacks on CWSNs. We therefore begin providing a background of WSNs and CWSNs in Sections 2 and 3, respectively. We then move to identify the common features and attacks in both of these types of networks in

Section 4. In Section 5, we specify attacks applicable only to CWSNs, and in Section 6 we detail security mechanisms for attack detection at different communication layers. Our work concludes with a discussion of open issues in Section 7.

2. Overview of Wireless Sensor Networks

WSNs have become widely available from the early 2000s, as sensing components and communication modules were already becoming cheap and small [3]. Monitoring the environment with such low cost devices became since then efficient, with a large volume of research having been conducted in the last almost two decades (one can trace the origins of WSNs in [4]). By now, WSN solutions are deployed in large scales and in various places and are being widely used in a variety of applications ranging from military [5] to agriculture [6] and from health care [7] to traffic management [8].

A WSN typically comprises a set of sensor nodes equipped with limited, low-power/short-range communication capabilities. Each of these nodes is a computational/communication platform which consists of (at least) a sensing module, a transceiver, a processor unit, and a power unit. The sensor node has typically small physical dimensions and its components are inexpensive. To make these sensor nodes more appealing, communication is commonly based on the license-free industrial, scientific, and medical (ISM) frequency band [9], in order to further limit operational costs for the overall WSN installation and to enable direct use of off-the-shelf communication solutions [10].

Depending on the application and deployment scenario, WSNs may vary in the communication paradigm they employ [11]. WSN applications set up to observe and consequently report to a "fusion center" the occurrence of an event (such as a fire), not needing to transmit continuously all measurements acquired by the sensors [12]. On the other hand, in scenarios such as pollution measurements [13] or seismic activity, the raw data can well be meaningful in its entirety; in such a case, the transmissions required would clearly be producing a heavy communication load; thus efficient channel access between the nodes as presented in [14] is required. These two extremely different cases indicate a mapping to the range of communication modes that may have to be used to handle the WSN most limiting resources: spectrum and energy (see [15, 16] and the references therein). A very rudimentary method to address these is WSN topological solutions which can be multihop [17], hierarchical [18], or one hop to infrastructure [19]. Each one in the respective references given has reasoning behind the underling spectrum management. Furthermore, in each of these cases a key factor that affects the system design is the power source and lifetime requirement of the WSN [20]. The node power unit, mentioned earlier, may be unlimited: for example, in indoor scenarios where the nodes can be directly plugged to the power grid. In such cases, energy plays little to no role. On the other hand, there can be extremely constrained scenarios such as the Smartdust, where literally every mWatt has to be accounted for, as the battery providing power is constrained even by its physical size, let alone its capacity. Energy harvesting [9] has recently been gathering significant attention as it can enable extension of the node lifetime, leveraging the environment resources (heat, motion, RF radiation, etc.).

3. Enhancing Wireless Sensor Networks with CR Technology

While the WSN solutions were progressing well into the late 2000s, the dramatically rising demand for wireless connectivity brought the spectrum utilization into the spotlight. Cognitive radio [21] and opportunistic communications, especially under the paradigms of opportunistic access or delay tolerant networking, came naturally into the frame of WSNs [22, 23]. Research into considering CR aspects for WSNs has thus begun [24, 25].

Opportunistic access is based on sending the transmissions over the "most suitable" spectrum band under a set of predefined application-driven requirements. With delay tolerance, a temporal aspect comes also into play: nodes can withhold data and transmit them at the "best" possible moment, subject to the application delay constraints. To enable these features, an additional process of dedicated spectrum sensing is required by the nodes, and in some cases local coordination can be used to enable the nodes to cooperatively infer about the radio spectrum usage at a specific area [26, 27]. This flexibility is further employed to adjust transmission parameters (modulation and coding schemes and transmission power) to reduce overall power consumption. Existing schemes developed to obtain spectrum awareness for cognitive radios in some cases consider the power consumption problem [28, 29], a clearly critical issue for CWSN. Reduced power consumption considered in CWSNs can not only extend the lifetime of sensor nodes but also limit the overall spectrum inefficiencies of the network, allowing for a substantial increase in spectrum utilization [30, 31].

4. Features and Common Attacks in WSNs and CWSNs

4.1. Common Features of WSNs and CWSNs. WSNs and CWSNs are two types of sensor networks that have a number of common characteristics. They consist of miniature devices, called motes or sensors that are severe resource constrained devices in terms of memory, processing, and energy [32, 33]. They usually do not perform any computation on the data they collect; they just forward this information to much more powerful devices (called sinks) for further processing.

The communication medium used for both WSNs and CWSNs has a broadcast nature and the used spectrum is split into several channels, depending on the protocol used. For example, there are up to 16 available channels for the IEEE 802.15.4 in the 2.4 GHz frequency band.

In both types of networks, the communication protocols used have a number of inefficiencies and vulnerabilities that allow potential attackers to launch a variety of destructive

attacks against these networks. The result of these attacks has catastrophic consequences including network performance deterioration, information theft, lifetime minimization, and battery depletion.

A multihop type of communication is often used in both types of networks (e.g., [34]) when data from a large and/or harsh area have to be sensed. Information flows from a sensor to a sink through multiple intermediate sensors that route packets according to an appropriate routing algorithm (e.g., RPL [35]). In a number of contributions, the network is split into several clusters and decisions are taken by the cluster heads in order to minimize sensors communication overhead and save energy, prolonging network's lifetime.

In both types of networks, network topology is highly dynamic and unpredictable without any central management. This is the case when sensors are deployed in harsh and volatile environments (e.g., [36, 37]). In such cases, adversaries can more easily attack and compromise the WSN.

4.2. Common Attacks against WSNs and CWSNs. The above common characteristics of WSNs and CWSNs make them vulnerable to a number of security threats. A diverse range of vulnerabilities are exploited by adversaries who can have several incentives, for example, network disruption, information theft, and so forth. In general, there are two types of attackers [38]: (i) external attackers that are not authorized participants of the sensor network and (ii) internal attackers that have compromised a legitimate sensor and use it to launch attacks in the network. Furthermore, attackers can be classified into passive and active. Passive attackers monitor network traffic without interfering with it. Their aim is to eavesdrop on the exchanged information and to acquire private data or to infer about information-sensitive applications that execute in the sensors (e.g., [2]). Active attackers disrupt network operation by launching several types of attacks that cause DoS (denial of service) in the WSN.

A severe DoS attack is jamming at the physical layer of the network. An adversary by creating interference, mainly through energy emission in the neighboring channels of the channel used by the sensor network [39], substantially increases the noise such that potential receivers become completely unavailable to receive and decode any information. This results in packet loss and further retransmissions by the senders that potentially lead to energy waste in the sensor network.

Jamming attacks can also be launched at the link layer. Here, an attacker can violate several characteristics of the communication protocol and cause packet collisions, exhausting sensors' resources. The authors in [40] show how a single adversary can cause severe performance degradation by violating several rules of the link layer protocol (back-off mechanism). Another popular attack is the Sybil attack where an adversary maliciously uses the identities of a number of sensors. This is achieved either by learning other sensors' identities or by fabricating new ones [41]. Furthermore, other types of attacks such as MAC spoofing [42] and ACK attacks [43] can cause confusion and packet loss in the network.

A major challenge in a WSN is maximizing its network lifetime by choosing the appropriate mode of communication. Single-hop communication, where the sensors communicate directly to a sink, is the flavour mode when the number of the sensors and the communication radius are small [44]. On the other hand, when the number of sensors is large (a typical case when a large area has to be covered by sensors) multihop communication is the most appropriate mode that saves sensors' energy, prolonging network's lifetime. In the multihop scenario, sensors have a dual role: they sense the environment and they also route the packets of their neighbors towards the sink (and vice versa). Packet forwarding and optimal path selection are performed by following an appropriate routing protocol. Adversaries can exploit several vulnerabilities and launch attacks against multihop sensor networks. Various attacks have been reported in the literature.

(i) *Selective Forwarding Attack.* Attackers drop the packets they have to route, randomly or selectively based on some rules (e.g., packets that originate from a specific sensor).

(ii) *Sinkhole Attack.* An attacker by broadcasting fake information makes the legitimate nodes believe that the attacker is attractive according to the routing protocol. If this attack is successful, neighboring sensors will forward their packets to the attacker that is then free to alter or steal information or drop the packets.

(iii) *Wormhole Attack.* This attack is performed by a number of colluding adversaries that forward packets between them through a direct long-distance and low-latency communication link (wormhole link). With this attack, legitimate sensors at a specific area of the network believe that they are close neighbors with sensors of another area that is however far away. This illusion creates confusion and affects routing within the network.

Except the above attacks that exploit several vulnerabilities in different layers of the communication stack, there is a special type of attack that aims to infer about information-sensitive application that executes in the sensors. Suppose that there is an on-body sensor network (e.g., [45]) consisting of a number of sensors that record high-sensitivity data such as the heart rate and oxygen saturation. Usually these applications transmit the sensed data to a sink in a periodic fashion [46]. Recent works [2, 46] have shown that adversaries can infer about these applications by passively monitoring the network traffic and detecting its periodic components that can finally reveal the potential medical applications. This becomes feasible using the appropriate signal processing techniques (e.g., the Lomb-Scargle periodogram) that discover traffic's periodic components even if it is encrypted.

5. Specific Attacks against CWSNs

As described in the previous section, WSNs and CWSNs have a number of common features and hence some common vulnerabilities that can be exploited by potential adversaries.

Nevertheless, CWSNs have two unique characteristics (that WSNs do not have) due to their cognitive nature [47].

(i) *Cognitive Capability.* It allows sensors to sense the environment for white spaces. Then, through a spectrum management process they decide upon which band to use for transmission and how to estimate the related-to-transmission physical layer parameters (frequency, modulation type, power, etc.). The cognitive cycle consists of several mechanisms: (i) radio environment, (ii) spectrum sensing, (iii) spectrum analysis, and (iv) spectrum decision.

(ii) *Reconfigurability.* It allows sensors to change on the fly their physical layer parameters and adapt to their environment. As sensors in CWSNs opportunistically use the fallow bands, they have to be flexible and vacate a band if a primary transmission is detected.

These unique characteristics make CWSNs vulnerable to a number of novel attacks. One of the most destructive attacks is called *primary user emulation attack* (PUEA). In this attack, an adversary mimics a primary user (PU) by transmitting fake incumbent signals [48]. Legitimate sensors will immediately evacuate the specific (under attack) frequency band, seeking for an alternative band to operate. Adversaries launching this attack can be of two types: (i) greedy sensors that emit the fake incumbent signals in order to make legitimate sensors evacuate the band in order to acquire its exclusive use and (ii) malicious sensors that aim to cause a DoS attack making sensors hop from band to band. Regardless of the type of the adversary, the PUEA attack can cause severe network disruption and a huge energy waste to the legitimate sensors. Figure 1 [47] shows that the PUEA attack affects all parts of the cognitive cycle.

As mentioned before, spectrum sensing is a fundamental operation and is one of the most challenging issues of the cognitive cycle. Spectrum sensing is the task of obtaining awareness about the spectrum usage and the possible presence of primary users [49]. During this operation, there is always the risk for the cognitive sensors not to correctly decode and hence detect the primary signals because of the shadow fading and hidden node effects. If this happens, harmful interference will be created to the primary transmitters. Collaborative spectrum sensing has been proposed as a solution to this problem [50]. In collaborative spectrum sensing, all sensors perform spectrum sensing and report their findings to a fusion centre (FC). The FC after performing a spectrum analysis procedure based on the sensors' reporting decides if a spectrum handoff has to be performed and at which frequency band. In a CWSN, the sink or the cluster heads (if the sensor network uses clusters) can have the role of the FC. However, if the network is not partitioned into clusters or the sink is far away from the majority of the sensors, this centralized scheme is not feasible. In such cases, distributed sensing can take place, where each sensor based on its own spectrum observation and the observations shared by its neighboring sensors makes its own spectrum decisions [51].

Adversaries can exploit the above mechanisms and affect FC's decision (or their neighbors' decision in distributed sensing) by sending false observations regarding spectrum usage. This attack is called *spectrum sensing data falsification* attack (SSDF). SSDF attackers can report that a specific band is vacant when it is not or that is occupied by primary signals when it is not. In the first case, harmful interference to the primary users will be created, while in the latter legitimate sensors will keep performing costly (in terms of energy) spectrum handoffs. Attackers can have different motives: (i) they can be greedy users that continuously report that a specific band is occupied in order to acquire its exclusive use and (ii) they can be malicious nodes that, by sending false observations, aim to create interference to primary transmitters or create a DoS attack on the network due to the continuous spectrum handoff of the legitimate sensors. SSDF attacks can also be initiated by unintentionally misbehaving sensors that report false observations because some parts of their software or hardware components are malfunctioning. This type of attack can substantially degrade network's performance as the authors in [52] show. Regarding the cognitive cycle, the SSDF attack affects the spectrum analysis and spectrum decision operations (Figure 1).

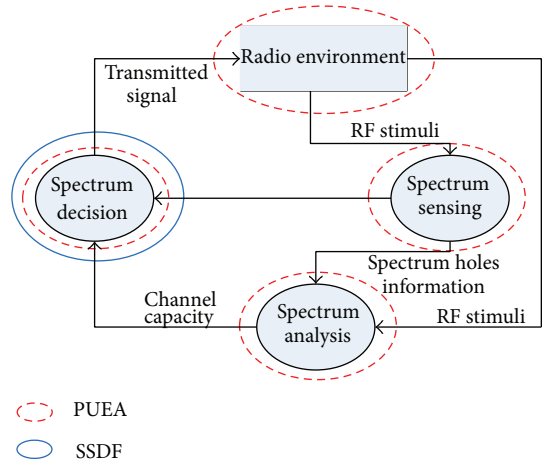

Figure 1: The cognitive cycle [47].

6. Security, Privacy, and Reliability Mechanisms for CWSNs

6.1. Security. Securing a WSN is of paramount importance, and for this reason a large number of contributions exist in the literature for the detection and mitigation of attacks against this type of networks. Depending on the attack type, different strategies and algorithms are followed.

6.1.1. Physical Layer Attack Detection. As mentioned in Section 4.2, jamming at the physical layer can cause disruptive DoS attacks in a WSN. The detection techniques try to (almost) instantly detect that a jamming attack is taking place by considering various metrics. The authors in [53] use the signal-to-interference-plus-noise ratio (SINR) as the metric that can signal the jamming attack. The recorded SINR values are fed to a cumulative-sum algorithm that

is able to detect abrupt changes that are caused by the attacker's presence. The performance of this anomaly-based detection algorithm is augmented if several monitors are used in a collaborative intrusion detection scheme. In [54], the definition of several types of attackers is given, and jamming detection is performed by using multiple if-else statements considering as metrics the *packet delivery ratio*, the *bad packet ratio*, and the *energy consumption amount*. In [55], a distributed anomaly detection algorithm is presented based on simple thresholds and a method for combining measurements using Pearson's product moment correlation coefficient. RF jamming attacks are the focus of [56] where the proposed algorithm applies high order crossings, a spectral dissemination technique that distinguishes normal scenarios from two types of defined attackers. The detection algorithm is based on thresholds considering the signal strength and location information. The authors in [57] propose DEEJAM, a defensive mechanism that uses an IEEE 802.15.4-based hardware. Here, the proposed algorithm hides messages from a jammer, evades its search, and reduces the impact of the corrupted messages.

6.1.2. Link Layer Attack Detection. Contributions that study the detection of attacks at the link layer include [40]. Here, an anomaly-based algorithm is presented considering the ratio of the corrupted packets over the correctly decoded packets as the metric that reveals jamming when the attacker's energy is emitted on the same channel. In [58], the authors explore energy-efficient attacks targeting three WSN protocols: (i) S-MAC, (ii) B-MAC, and (iii) L-MAC. As a countermeasure they suggest the use of shorter data packets for the L-MAC and high duty cycle for the S-MAC. Link layer misbehaviour in [59] is detected by applying a nonparametric cumulative-sum algorithm considering the expected back-off value of the honest participants. MAC address spoofing detection in WSN is studied in [60]. In that work, an approach based on the Gaussian mixture models that considers RSS (received-signal-strength) profiles is used to detect if a MAC address is spoofed. RSS is a metric that is hard to forge arbitrarily, and it highly depends on the transmitter's location. The authors in [42] propose an algorithm that leverages the sequence number field carried by the data packets. This algorithm records the sequence number of each received frame and that of the last frame coming from the same source node. When the gap between the current sequence number and the last recorded one is within a specific range, it is considered as abnormal. For each abnormal frame, a verification process follows to declare the specific frame as normal or spoofed.

Regarding the Sybil attack detection, the algorithm in [61] uses the ratios of the RSSI (received-signal-strength indicator) recorded in a number of sensor monitors when a packet is transmitted within their communication range. If these ratios are very close to the ratios computed when a packet with a different identity is used, the corresponding transmitter is flagged as a Sybil attacker. In [62], the detection algorithm exploits the characteristic that every Sybil (forged) sensor has the same set of neighbors as they are created by the same adversary. It detects the Sybil attack by comparing the information collected from neighboring sensors (contained in small messages). In [63], Sybil attacks are detected by exploiting the spatial variability of radio channels in environments with rich scattering. An enhanced physical layer authentication scheme is used for both wideband and narrowband wireless systems.

6.1.3. Network Layer Attack Detection. As described in Section 4.2, a large number of vulnerabilities of the routing protocols can be exploited in sensor networks. Different countermeasures have been proposed for the detection of these attacks. In [64], a lightweight scheme uses a multihop acknowledgment technique to launch alarms when responses from intermediate sensors are missing. Each time a sensor receives a data packet, it sends an ACK to the sensor that handled the packet in the previous hop. If a sensor receives less than a number of ACK packets within a specified time, it suspects that the previous report it forwarded has been dropped by a malicious sensor. If this is the case, it sends an alarm packet to the sink, reporting its next-hop sensor as a potential malicious sensor. The sink after it receives all alarm packets infers about the malicious sensors. The authors in [65] propose a centralized scheme with the use of support vector machines (SVMs). A 2D SVM is initially trained when no attacker is present, using the hop count and the measured bandwidth at the sink as features. At run time, the detection algorithm based on the SVM executes at the sink. A different approach is followed in [66] where each sensor observes the behavior of its neighbors recording the number of packets they forward, along with the source address of the originating sensor. Based on these observations, it updates a trust metric for each of its neighbors that reveals the potential attackers. After a sensor has been labelled as an attacker, the routing tables are modified in order to isolate that sensor from the network.

For the detection of the sinkhole attacks, a distributed detection scheme is presented in [67]. Every sensor S_i is set in promiscuous mode and records the route update packets transmitted by its neighbors. Furthermore, two rules have been defined that if violated, an alert message is broadcasted: (i) if sender's ID matches S_i's ID and (ii) if sender's ID does not belong to the known IDs of S_i's neighbors. This detection scheme also employs a collaborative detection algorithm that reveals the potential attacker based on an intersection computation of the information carried by the alert messages. Ngai et al. [68] propose a detection algorithm that consists of two steps: (i) it locates a list of suspected sensors by checking data consistency based on the information sensors report to the sink and (ii) it labels a sensor as an attacker by analyzing the network flow information (represented by directed edges between communicating sensors). The authors in [69] show that shortest-path routing protocols select a series of paths whose length exhibits a log-normal distribution. Based on this observation, they propose an anomaly detection algorithm by deriving tolerance limits from the log-normal distribution of path lengths when no attacker is present.

Regarding the wormhole detection, the scheme proposed in [70] considers the round-trip time (RTT) between an originating sensor and its destination. RTT depends on how far the intermediate sensors are located. If a wormhole attack is in progress, RTT can significantly increase, as packets are replicated in a different part of the network from colluding attackers. In [71], a localized scheme based on connectivity graphs is proposed. It seeks for *forbidden substructures* in the connectivity graphs that should not be present under normal circumstances. The authors in [72] propose a distributed detection algorithm that detects wormhole attacks based on the distortions these attacks create in the network. This scheme uses a hop counting technique as a probe procedure, reconstructing local maps for each sensor, and then a diameter feature that depends on the number of neighboring nodes, for anomaly detection.

6.1.4. Detection of Attacks That Exploit Vulnerabilities of the Cognitive Nature of CWSNs. A possible framework for securing cognitive radio networks has been proposed in [73] and can easily be extended to secure CWSNs. This framework attempts to identify the mechanisms that can mitigate the specific attacks on cognitive radio networks. As discussed in Section 5, there are two major types of attacks that can be launched against CWSNs: (i) PUEAs and (ii) SSDF attacks. Regarding the detection of the PUEAs, there are a large number of significant contributions that split into two main categories: (i) location-based and (ii) non-location-based contributions. Location-based contributions assume that the locations of the primary transmitters are known a priori.

The work in [48] considers both the location information of the primary transmitter and the RSS values collected by a separate sensor network each time a primary transmission is taking place. Based on the RSS measurements the location of the transmitter is estimated, and if it is different than the (already) known location of the legitimate primary transmitter, an alarm is triggered. Jin et al. [74] developed an algorithm that considers the received power measured at the radio interfaces of the secondary users (SUs) in a specific band. Then, by using Fenton's approximation and Wald's sequential probability radio test, they decide on the corresponding hypothesis about the presence or not of a PUEA attacker. The received power is also considered in [75] where the authors propose a variance method to detect the attack. This scheme first estimates the variance of the received power from the primary transmitter, and then it determines whether a received signal is from the primary transmitter or from an attacker.

In non-location-based algorithms like in [76], the locations of the primary transmitters are not required to be known. The authors state that the channel impulse response can be revealed if a primary transmitter has moved to a different location. Their approach uses a *helper node* (HN) that is located very close to a primary transmitter in a fixed location. This node is used as a bridge between the SUs and the primary transmitter by allowing SUs to verify cryptographic signatures by HN's signals and then obtain HN's link signals in order to verify primary transmitter's signals. The authors show that, by using the first and second multipath components measured at HN, they can verify if the transmitted signal belongs to the legitimate primary user or it is fake. The scheme presented in [77] uses a public key cryptography mechanism where a primary transmitter integrates its transmitted data with cryptographic signatures. Each SU that detects a primary signal attempts to verify its integrated signatures. If verification fails, the signal is characterized as fake.

Regarding the SSDF attack detection, in [52] a centralized algorithm calculates the trust values of SUs based on their past record. Additionally, consistency checks are performed because the trust values can become unstable if an attacker is present or there is not enough information. If the consistency value and the trust value of an SU drop below a specific threshold, the specific SU is characterized as an attacker. Rawat et al. [78] propose a centralized scheme that computes a reputation metric for each SU based on SU's past observation, and the decision is made by the FC during that round of observations. If there is a decision mismatch, SU's reputation metric is increased by one, and if it becomes larger than a predefined threshold, SU is labelled as an attacker. Reputation metrics are also used by other similar contributions like in [79, 80].

6.2. Privacy. Although security attacks in WSNs have been very extensively researched until now, "privacy" attacks are a not so common research topic. Most works until now have focused mainly on protecting the location privacy of the sensor nodes, while others focus on protecting the traffic of the data that are transmitted by the nodes. However, when sensors are enhanced with CR technology, the traditional WSN privacy attacks still exist, with the addition of other attacks for eavesdropping on the sensing data (in collaborative spectrum sensing) and the context of the exchanged sensor data, for impersonating the PU and against the anonymity of a sensor node. In this section the common attacks against privacy on CWSN are described, together with the existing mechanisms for mitigating these attacks.

6.2.1. CR Location Privacy. Location privacy is a major research topic in cognitive WSNs due to the fact that the spectrum opportunities (namely, the unoccupied spectrum frequencies or the white spaces) are heavily depending on the location of both the sensor nodes and the PUs. The received PU signal at the sensor nodes is highly related to the distance between the sensor nodes and a malicious user can identify the sensor node location using geolocation mechanisms. Furthermore, in participatory sensing [81] the data from the sensor nodes are usually tagged with location and the time.

According to [82], the respective location privacy attacks can be either external (combined with eavesdropping) or internal. An external attacker can intercept the spectrum sensing reports that are exchanged throughout the CWSN by eavesdropping on the communication of the sensor nodes either with each other or with the FC (in case of a centralized spectrum sensing system). That way, the attacker is able to

know the received PU signals of all sensor nodes and by correlating the data with its own sensing reports, he is able to identify the location of the sensor nodes. An internal attacker can be either another node participating in the collaborative sensing or the fusion center (or an attacker impersonating the fusion center). That way the attacker seems to be a legitimate node that receives the sensing reports from all other nodes and can easily compromise their location by correlating the data with his physical location. An internal attacker can also exploit the results of the aggregated sensing reports that are being transmitted by the FC. That way, comparing the reports before and after the inclusion of a new node in the network, it is easy to identify its location.

Mitigation. For preserving the privacy of cognitive sensor nodes, in [82] a combination of techniques for cryptography and sensing data randomization has been proposed. The first technique uses the concept of secrets [83] and each sensor encrypts its sensing data in such a way that the FC should get all reports in order to be able to decrypt the aggregated sensing report. That way, when a malicious user intercepts the reports from a specific sensor or from all sensors in an area, he will not be able to decrypt these reports, hence the sensors' locations cannot be estimated.

Another proposal [82] for protecting the location of cognitive sensors includes the transmission of dummy sensing reports from one of the legitimate nodes or the fusion center when a new node is joining or leaving the network. Although this can degrade the performance of collaborative sensing, an appropriate selection of the dummy report and its weight on the overall sensing aggregation can have a minimal impact, without affecting significantly the sensing result.

Proposals for ensuring location privacy in participatory sensing include the anonymization of sensing reports using the principle of k-anonymity [84–87], which assumes that at least k users are located at the same area, and thus they tag their sensing reports with an area "ID" and not with their actual location information. That way, if an attacker eavesdrops on the reports of the sensor nodes, only an abstract view of the general area of the users could be extracted and not an actual location. However, the performance of such a sensing system is heavily depending on the size of the area, because a small area can result in an optimum sensing result but can also give enough information to the attacker to identify the location of the sensor nodes. On the other hand, a large area may preserve the nodes' location information but can degrade significantly the performance of the participatory sensing system.

6.2.2. Sensed Data Privacy. Like traditional WSNs, CWSNs are deployed for getting automated measurements and transmitting them to an application server for processing. This information may be sensitive in some applications and must be protected from unauthorized access and use. For example, hijacking the information sent by sensors measuring the energy consumption of devices in a household may reveal the presence/absence of the habitants, which could be utilized by burglars. Respective attacks against the sensor data include eavesdropping, impersonation, and traffic analysis [88].

Eavesdropping (or passive monitoring) is a very common attack on WSNs, under which an attacker is listening to the communication channel of the sensor nodes and intercepts their data. In this attack, the malicious node is hidden from the sensor nodes because it does not communicate directly with them. Under the impersonation attack, the malicious node impersonates either a legitimate node or the FC and gets the data directly from the legitimate sensor nodes. This attack can be the first point to launch other attacks changing the data and transmitting false data to the other nodes. The traffic analysis is used by attackers to extract the context of data that are transferred by the sensors and is achieved by analysing the traffic patterns from eavesdropping on the wireless links. Using the traffic analysis attack, a malicious node can also identify some nodes that have a special role in the CWSN (i.e., who has the role of the FC).

Mitigation. Targeting avoidance of the disclosure of the sensed data to unauthorized recipients, several proposals have been made in the literature, which mainly focus on anonymity schemes or on information flooding. Using anonymization, the data sent by a legitimate node do not contain personal information that can be used to track back the measurements to the originating sensor node [89]. In [90], a framework for context-aware privacy of sensor data is proposed, which includes a two-step process of (i) identifying which data will be shared and (ii) obfuscating the data before transmitting them. Although most previous anonymization proposals were focused on protecting sensor location information [82, 91], they can be relatively easily adapted to the sensed data that the nodes are transmitting. Information flooding is another technique that can be used to protect the data privacy in CWSNs, as proposed in [92], which discusses the fact that probabilistic flooding can give good protection to the node information while being energy efficient.

7. Conclusion

WSNs and CWSNs are two similar sensor network types with quite a few common features. Recently there has been an explosion of Smart City applications for providing advanced ICT-based services to citizens with the use of enhanced WSN networks. For the realization of such applications a plethora of sensing and actuating devices are usually installed either in a city area or within buildings. In this context, the WSNs will be playing a significant role in the everyday life of people, and thus their security is of great importance. This explosion in the number of wireless sensing and actuating devices in city areas together with the continuous installation of many (public and private) wireless access networks in these areas has resulted in congestion in the unlicensed spectrum bands (ISM bands around 2.4 GHz) that are used for both WSNs and Wi-Fi. For mitigating the congestion effects on the WSN networks, there are proposals to equip the latter with CR technology forming the CWSNs, which on the one hand

Table 1: Attacks against CWSNs.

Type of attack	OSI layer	Characteristic	Common with WSN
Jamming	Physical layer	DoS attack creating interference, increasing packet loss and collisions	Yes
Back-off attack	Link layer	An attacker causes severe performance degradation by minimizing the CWmin and thus his back-off period	Yes
Sybil attack	Cross layer	Stealing sensors identities, that is, MAC address, IP address, and so forth	Yes
MAC spoofing	Link layer	Alternating a MAC address on a network interface can help an unauthorized intruder enter a secure network	Yes
Selective forwarding attack	Network layer	Attackers drop packets they have to route	Yes
Sinkhole attack	Network layer	Attacker broadcasts false routing related information so that neighbouring nodes send them their packets and steals information or drops them	Yes
Wormhole attack	Network layer	Adversaries exchange packets through a long-distance and low-latency links affecting routing making legitimate sensors believe that they are neighbours with sensors of another area	Yes
PUEA	Physical layer	Adversaries mimic PU so that hey exploit unused frequencies that the other nodes assume as occupied by the PU	No
SSDF attack	Physical layer	Attackers provide false information regarding spectrum occupancy	No
Location privacy attacks	Physical layer	Attackers intercept signals and sensing reports so that with data correlation they can identify the sensor location	No
Sensed data privacy attacks	Physical/link layer	Attackers eavesdrop the channel and analyse the traffic to intercept the sensed data that are transmitted by the sensors	Yes

solves several issues of traditional WSNs security-wise but on the other introduces new security threats.

Securing WSNs and CWSNs is of key importance, and a large pool of contributions from the literature for the detection and mitigation of attacks against these networks has been presented in this paper. Furthermore, an overview of the most common attacks against CWSN is presented in Table 1. Depending on the attack type, different strategies and algorithms are followed. Exploiting the CR features of CWSN enables two major classes of attacks that can be launched against them: (i) PUEAs and (ii) SSDF attacks. Regarding the detection of the PUEAs a significant number of contributions exist which can be broken into two categories: (i) location-based and (ii) non-location-based contributions. For the former the key challenge is the detection of the attacker's location, an issue that is open in many other problems of wireless networking. The SSDF attack detection in the literature presented here is primarily based on the notions of reputation and trust, given the collaborative nature of the proposed solutions. Regarding privacy, the most common attacks are those against identifying the location of the cognitive sensors node and those against intercepting the sensing data.

Although much research has been done in the literature regarding the security of the CWSNs, there are still several challenges and open research issues remaining. One of the most important challenges is related to introducing trust within the CWSN architecture. Although several attempts for mitigating SSDF attacks are introducing reputation mechanisms for the cognitive nodes, these can be considered as an "add-on" feature, while a trust framework embedded within the cognitive nodes not only addresses the SSDF attacks but also ensures the complete trustworthy operation (starting from the sensed data and going all the way up to ensuring the trustworthiness of the applications that run on the nodes) of the cognitive nodes. Another open challenge is related to designing lightweight cryptographic algorithms that could run on the very resource-limited cognitive sensor nodes, focusing on private-key cryptography, efficient key distribution schemes for symmetric key cryptography, and efficient key management protocols for public key cryptography. Regarding routing, in CWSNs there is a need for further research on secure routing schemes taking into account the spectrum assigned to each one of the intermediate nodes, as well as the mobility of the nodes and the potential scalability and efficiency issues. Moreover, in data aggregation mechanisms there is a need for further research on enhancing the data aggregation and securing it against malicious cognitive users, introducing trust and security metrics. Other open research issues regarding security in CWSNs that need to be addressed in future research include the use of geolocation information for improving security, that is, in PUEA attacks, the investigation of intelligent physical layer security mechanisms that exploit CR characteristics, the development of distributed mechanisms against SSDF attacks, and the design of efficient cooperative mechanisms against malicious nodes and intruders.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The research leading to these results has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under Grant Agreements nos. 609094 and 612361.

References

[1] A. Liotta, D. Geelen, G. Kempen, and F. Hoogstraten, "A survey on networks for smart-metering systems," *International Journal of Pervasive Computing and Communications*, vol. 8, pp. 23–52, 2012.

[2] A. Fragkiadakis and I. Askoxylakis, "Malicious traffic analysis in wireless sensor networks using advanced signal processing techniques," in *Proceedings of the 14th International Symposium and Workshops on aWorld of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, pp. 1–6, 2013.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, no. 4, pp. 393–422, 2002.

[4] S. DUST, "SMART DUST Autonomous sensing and communication in a cubic millimeter," http://robotics.eecs.berkeley.edu/~pister/SmartDust/.

[5] M. Winkler, M. Street, K. D. Tuchs, and K. Wrona, "Wireless sensor networks for military purposes," in *Autonomous Sensor Networks*, vol. 13 of *Springer Series on Chemical Sensors and Biosensors*, pp. 365–394, 2013.

[6] Y. Xiaoqing, W. Pute, W. Hana, and Z. Zhanga, "A survey on wireless sensor network infrastructure for agriculture," *Computer Standards and Interfaces*, vol. 35, no. 1, pp. 59–64, 2013.

[7] J. Ko, C. Lu, M. B. Srivastava, J. A. Stankovic, A. Terzis, and M. Welsh, "Wireless sensor networks for healthcare," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1947–1960, 2010.

[8] A. Pascale, M. Nicoli, F. Deflorio, B. Dalla Chiara, and U. Spagnolini, "Wireless sensor networks for traffic management and road safety," *IET Intelligent Transport Systems*, vol. 6, no. 1, pp. 67–77, 2012.

[9] E. A. Fan Zhang, "A batteryless 19uw mics/ism-band energy harvesting body area sensor node soc," in *Proceedings of the Solid-State Circuits Conference Digest of Technical Papers (ISSCC '12)*, 2012.

[10] B. Buchli, F. Sutton, and J. Beutel, "Gps-equipped wireless sensor network node for high-accuracy positioning applications," in *Wireless Sensor Networks*, vol. 7158 of *Lecture Notes in Computer Science*, Springer, Berlin, Germany, 2012.

[11] P. Santi, "Topology control in wireless ad hoc and sensor networks," *ACM Computing Surveys*, vol. 37, no. 2, pp. 164–194, 2005.

[12] G. Wittenburg, "Cooperative event detection in wireless sensor networks," *Communications Magazine*, vol. 50, no. 12, 2012.

[13] R. P. Khedo and A. Mungur, "A wireless sensor network air pollution monitoring system," *International Journal of Wireless and Mobile Networks*, vol. 2, no. 2, 2012.

[14] A. Antonopoulos and C. Verikoukis, "Network-coding-based cooperative ARQ medium access control protocol for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2012, Article ID 601321, 2012.

[15] J. A. S. G. Zhou and S. H. Son, "Crowded spectrum in wireless sensor networks," in *Proceedings of the 3rd Workshop on Embedded Networked Sensors*, 2006.

[16] G. Anastasi, M. Conti, M. Di Francesco, and A. Passarella, "Energy conservation in wireless sensor networks: a survey," *Ad Hoc Networks*, vol. 7, no. 3, pp. 537–568, 2009.

[17] T. F. Abdelzaher, S. Prabh, and R. Kiran, "On real-time capacity limits of multihop wireless sensor networks," in *Proceedings of the 25th IEEE International Real-Time Systems Symposium (RTSS '04)*, pp. 359–370, December 2004.

[18] K. Iwanicki and M. Van Steen, "On hierarchical routing in wireless sensor networks," in *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN '09)*, pp. 133–144, April 2009.

[19] J. Zhang, L. Shan, H. Hu, and Y. Yang, "Mobile cellular networks and wireless sensor networks: toward convergence," *IEEE Communications Magazine*, vol. 50, no. 3, pp. 164–169, 2012.

[20] I. F. Akyildiz, W. Lee, and K. R. Chowdhury, "CRAHNs: cognitive radio ad hoc networks," *Ad Hoc Networks*, vol. 7, no. 5, pp. 810–836, 2009.

[21] S. Haykin, "Cognitive radio: brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[22] S. Huang, X. Liu, and Z. Ding, "Opportunistic spectrum access in cognitive radio networks," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications*, pp. 2101–2109, April 2008.

[23] O. S. A. Lindgren and A. Doria, "Probabilistic routing in intermittently connected networks," *SIGMOBILE Mobile Computing Communications Review*, vol. 23, no. 2, 2003.

[24] I. F. Akyildiz, W. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[25] O. B. Akan, O. B. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE Network*, vol. 23, no. 4, pp. 34–40, 2009.

[26] S. Maleki, A. Pandharipande, and G. Leus, "Energy-efficient distributed spectrum sensing for cognitive sensor networks," *IEEE Sensors Journal*, vol. 11, no. 3, pp. 565–573, 2011.

[27] E. Tragos, S. Zeadally, A. Fragkiadakis, and V. Siris, "Spectrum assignment in cognitive radio networks: a comprehensive survey," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1108–1135, 2013.

[28] J. A. Han, W. S. Jeon, and D. G. Jeong, "Energy-efficient channel management scheme for cognitive radio sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 4, pp. 1905–1910, 2011.

[29] Y. Xu, C. Wu, C. He, and L. Jiang, "A cluster-based energy efficient mac protocol for multi-hop cognitive radio sensor networks," in *Proceedings of the Global Communications Conference (GLOBECOM '12)*, 2012.

[30] A. S. Zahmati and X. Fernando, "Application-specific spectrum sensing method for cognitive sensor networks," *IET Wireless Sensor Systems*, vol. 3, no. 3, pp. 193–204, 2013.

[31] E. Tragos and V. Angelakis, "Cognitive radio inspired m2m communications," in *Proceedings of the 16th International Symposium on Wireless Personal Multimedia Communications (WPMC '13)*, pp. 1–5, June 2013.

[32] B. Otal, C. Verikoukis, and L. Alonso, "Efficient power management based on a distributed queuing MAC for wireless sensor networks," in *Proceedings of the IEEE 65th Vehicular Technology Conference (VTC '07)*, pp. 105–109, April 2007.

[33] J. Alonso-Zarate, E. Stavrou, A. Stamou, P. Angelidis, L. Alonso, and C. Verikoukis, "Energy-efficiency evaluation of a medium access control protocol for cooperative ARQ," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, June 2011.

[34] N. Gazoni, V. Angelakis, V. A. Siris, and B. Raffaele, "A framework for opportunistic routing in multi-hop wireless networks," in *Proceedings of the 7th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN '10)*, pp. 50–57, October 2010.

[35] U. Herberg and T. Clausen, "A comparative performance study of the routing protocols LOAD and RPL with bi-directional traffic in low-power and lossy networks (LLN)," in *Proceedings of the 8th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks (PE-WASUN '11)*, pp. 73–80, November 2011.

[36] G. Werner-Allen, K. Lorincz, M. Welsh et al., "Deploying a wireless sensor network on an active volcano," *IEEE Internet Computing*, vol. 10, no. 2, pp. 18–25, 2006.

[37] V. Bychkovsky, K. Chen, M. Goraczko et al., "The CarTel mobile sensor computing system," in *Proceedings of the 4th International Conference on Embedded Networked Sensor Systems (SenSys '06)*, pp. 383–384, November 2006.

[38] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 52–73, 2009.

[39] A. G. Fragkiadakis, V. A. Siris, and A. P. Traganitis, "Effective and robust detection of jamming attacks," in *Proceedings of the Future Network and Mobile Summit*, June 2010.

[40] A. Fragkiadakis, E. Tragos, T. Tryfonas, and I. Askoxylakis, "Design and performance evaluation of a lightweight wireless early warning intrusion detection prototype," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, article 37, pp. 1–18, 2012.

[41] C. E. Loo, M. Y. Ng, C. Leckie, and M. Palaniswami, "Intrusion detection for routing attacks in sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2, no. 4, pp. 313–332, 2006.

[42] F. Guo and T. Chiueh, "Sequence number-based mac address spoof detection," in *Proceedings of the 8th international conference on Recent Advances in Intrusion Detection (RAID '05)*, pp. 1–20, 2005.

[43] Y. Xiao, S. Sethi, H. Chen, and B. Sun, "Security services and enhancements in the IEEE 802.15.4 wireless sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference(GLOBECOM '05)*, pp. 1796–1800, December 2005.

[44] J. F. Shi, X. X. Zhong, and S. Chen, "Study on communication mode of wireless sensor networks based on effective result," *Journal of Physics: Conference Series*, vol. 48, no. 1, article 245, pp. 1317–1321, 2006.

[45] B. Otal, L. Alonso, and C. Verikoukis, "Highly reliable energy-saving mac for wireless body sensor networks in healthcare systems," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 553–565, 2009.

[46] L. Buttyan and T. Holczerr, "Traffic analysis attacks and countermeasures in wireless body area sensor networks," in *proceedings of the International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMom '12)*, pp. 1–6, 2012.

[47] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. 15, pp. 428–445, 2013.

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

[49] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[50] S. Zarrin and T. J. Lim, "Cooperative quickest spectrum sensing in cognitive radios with unknown parameters," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '09)*, December 2009.

[51] Z. Tian, E. Blasch, W. Li, G. Chen, and X. Li, "Performance evaluation of distributed compressed wideband sensing for cognitive radio networks," in *Proceedings of the 11th International Conference on Information Fusion (FUSION '08)*, July 2008.

[52] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proceedings of the 43rd Annual Conference on Information Sciences and Systems (CISS '09)*, pp. 130–134, March 2009.

[53] A. Fragkiadakis, V. Siris, N. Petroulakis, and A. Traganitis, "Anomaly-based intrusion detection of jamming attacks, local versus collaborative detection," *Wireless Communications and Mobile Computing*, 2013.

[54] M. Cakiroglou and T. Ozcerit, "Jamming detection mechanisms for wireless sensor networks," Proceedings of the 3rd International Conference on Scalable Information Systems, 2008.

[55] A. Sheth, C. Doerr, D. Grunwald, R. Han, and D. Sicker, "MOJO: a distributed physical anomaly detection system for 802.11 WLANs," in *Proceedings of the 4th International Conference on Mobile Systems, Applications and Services*, pp. 191–204, June 2006.

[56] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 46–57, May 2005.

[57] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proceedings of the 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07)*, pp. 60–69, June 2007.

[58] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Transactions on Sensor Networks*, vol. 5, no. 1, article 6, 2009.

[59] A. A. Cárdenas, S. Radosavac, and J. S. Baras, "Evaluation of detection algorithms for MAC layer misbehavior: theory and experiments," *IEEE/ACM Transactions on Networking*, vol. 17, no. 2, pp. 605–617, 2009.

[60] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proceedings of the 27th IEEE Communications Society Conference on Computer Communications (INFOCOM '08)*, pp. 2441–2449, April 2008.

[61] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '06)*, pp. 564–568, June 2006.

[62] K. Ssu, W. Wang, and W. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042–3056, 2009.

[63] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-based detection of sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp. 492–503, 2009.

[64] B. Yu and B. Xiao, "Detecting selective forwarding attacks in wireless sensor networks," in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (IPDPS '06)*, pp. 1–8, 2006.

[65] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Şekerciğlu, "Detecting selective forwarding attacks in wireless sensor networks using support vector machines," in *Proceedings of the International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '07)*, pp. 335–340, December 2007.

[66] Y. Cho and G. Qu, "Detection and prevention of selective forwarding-based denial-of-service attacks in wsns," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 205920, 16 pages, 2013.

[67] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Algorithmic Aspects of Wireless Sensor Networks*, pp. 150–161, 2008.

[68] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2353–2364, 2007.

[69] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-count monitoring: detecting sinkhole attacks in wireless sensor networks," in *Proceedings of the 15th IEEE International Conference on Networks (ICON '07)*, pp. 176–181, November 2007.

[70] Z. Tun and A. Maw, "Wormhole attack detection in wireless sensor networks," in *Proceedings of the World Academy of Science, Engineering and Technology*, pp. 545–550, 2008.

[71] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proceedings of the 26th IEEE International Conference on Computer Communications*, pp. 107–115, May 2007.

[72] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Detecting wormhole attacks in wireless sensor networks," *IFIP International Federation for Information Processing*, vol. 253, pp. 267–279, 2007.

[73] A. Mihovska, R. Prasad, E. Tragos, and V. Angelakis, "Design considerations for a cognitive radio trust and security framework," in *Proceedings of the IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD '12)*, pp. 156–158, September 2012.

[74] Z. Jin, S. Anand, and K. P. Subbalakshmi, "Detecting primary user emulation attacks in dynamic spectrum access networks," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, June 2009.

[75] Z. Chen, T. Cooklev, C. Chen, and C. Pomalaza-Ráez, "Modeling primary user emulation attacks and defenses in cognitive radio networks," in *Proceedings of the 28th International Performance Computing and Communications Conference (IPCCC '09)*, pp. 208–215, December 2009.

[76] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in *Proceedings of the 31st IEEE Symposium on Security and Privacy (SP '10)*, pp. 286–301, May 2010.

[77] C. N. Mathur and K. P. Subbalakshmi, "Digital signatures for centralized DSA networks," in *Proceedings of the 4th Annual IEEE Consumer Communications and Networking Conference (CCNC '07)*, pp. 1037–1041, January 2007.

[78] A. S. Rawat, P. Anand, H. Chen, and P. K. Varshney, "Countering Byzantine attacks in cognitive radio networks," in *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '10)*, pp. 3098–3101, March 2010.

[79] R. Chen, J. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proceedings of the 27th Conference on Computer Communications (INFOCOM '08)*, pp. 1876–1884, 2008.

[80] E. Noon and H. Li, "Defending against hit-and-run attackers in collaborative spectrum sensing of cognitive radio networks: a point system," in *Proceedings of the 71st Vehicular Technology Conference (VTC '10)*, May 2010.

[81] J. Burke, D. Estrin, M. Hansen et al., "Participatory sensing," in *Proceedings of the Workshop on World-Sensor-Web (WSW '06), 2006*, pp. 117–134.

[82] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Communications*, vol. 19, no. 6, pp. 106–112, 2012.

[83] E. Shi, R. Chow, T. H. Hubert Chan, D. Song, and E. Rieffel, "Privacy-preserving aggregation of time-series data," in *Proceedings of the NDSS Symposium*, 2011.

[84] K. L. Huang, S. S. Kanhere, and W. Hu, "Towards privacy-sensitive participatory sensing," in *Proceedings of the 7th Annual IEEE International Conference on Pervasive Computing and Communications (PerCom '09)*, March 2009.

[85] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "AnonySense: privacy-aware people-centric sensing," in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, pp. 211–224, ACM, New York, NY, USA, June 2008.

[86] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "Anonysense: opportunistic and privacy-preserving context collection," in *Proceedings of the 6th International Conference on Pervasive Computing*, pp. 280–297, Springer, Berlin, Germany, 2008.

[87] L. Sweeney, "K-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 5, pp. 557–570, 2002.

[88] J. Sen, "Security and privacy challenges in cognitive wireless sensor networks," in *Cognitive Radio Technology Applications for Wireless and Mobile Ad Hoc Networks*, N. Meghanathan and Y. B. Reddy, Eds., pp. 194–232, IGI-Global, Hershey, Pa, USA, 2013.

[89] Y. Ouyang, Z. Le, Y. Xu et al., "Providing anonymity in wireless sensor networks," in *Proceedings of the IEEE International Conference on Pervasive Services (ICPS '07)*, pp. 145–148, July 2007.

[90] S. Chakraborty, K. R. Raghavan, M. P. Johnson, and M. B. Srivastava, "A framework for context-aware privacy of sensor data on mobile systems," in *Proceedings of the 14th Workshop on Mobile Computing Systems and Applications*, pp. 11:1–11:6, ACM, New York, NY, USA, 2013.

[91] M. Gruteser and D. Grunwald, "Anonymous usage of locationbased services through spatial and temporal cloaking," in *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, pp. 31–42, ACM, New York, NY, USA, 2003.

[92] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04)*, pp. 88–93, October 2004.