Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 815959, 8 pages
http://dx.doi.org/10.1155/2013/815959

Research Article

PUE Attack Detection in CWSN Using Collaboration and Learning Behavior

Javier Blesa, Elena Romero, Alba Rozas, Alvaro Araujo, and Octavio Nieto-Taladriz

Electronic Engineering Department, ETSI Telecomunicación, Universidad Politécnica de Madrid, 28040 Madrid, Spain

Correspondence should be addressed to Javier Blesa; jblesa@die.upm.es

Received 1 March 2013; Accepted 3 June 2013

Academic Editor: S. Khan

Cognitive Wireless Sensor Network (CWSN) is a new paradigm which integrates cognitive features in traditional Wireless Sensor Networks (WSNs) to mitigate important problems such as spectrum occupancy. Security in Cognitive Wireless Sensor Networks is an important problem because these kinds of networks manage critical applications and data. Moreover, the specific constraints of WSN make the problem even more critical. However, effective solutions have not been implemented yet. Among the specific attacks derived from new cognitive features, the one most studied is the Primary User Emulation (PUE) attack. This paper discusses a new approach, based on anomaly behavior detection and collaboration, to detect the PUE attack in CWSN scenarios. A nonparametric CUSUM algorithm, suitable for low resource networks like CWSN, has been used in this work. The algorithm has been tested using a cognitive simulator that brings important results in this area. For example, the result shows that the number of collaborative nodes is the most important parameter in order to improve the PUE attack detection rates. If the 20% of the nodes collaborates, the PUE detection reaches the 98% with less than 1% of false positives.

1. Introduction

One of the fastest growing sectors in recent years has undoubtedly been that of WSNs. WSNs consist of spatially distributed autonomous sensors that monitor a wide range of ambient conditions and cooperate to share data across the network. WSNs are increasingly being introduced into our daily lives. Potential fields of applications can be found, ranging from the military to home control commercially or industrially, to name a few. The emergence of new wireless technologies such as ZigBee and IEEE 802.15.4 has allowed for the development of interoperability among commercial products, which is important for ensuring scalability and low cost. Most WSN solutions operate on unlicensed frequency bands. In general, they use industrial, scientific, and medical (ISM) bands, like the worldwide available 2.4 GHz band. This band is also used by a large number of popular wireless applications, for example, those that work over Wi-Fi or Bluetooth. For this reason, the unlicensed spectrum bands are becoming overcrowded. As a result, coexistence issues on unlicensed bands have been the subject of extensive research, and, in particular, it has been shown that IEEE 802.11 networks can significantly degrade the performance of ZigBee/802.15.4 networks when operating on overlapping frequency bands [1].

The increasing demand for wireless communication presents a challenge to make efficient use of the spectrum. To address this challenge, cognitive radio (CR) has emerged as the key technology, which enables opportunistic access to the spectrum. A CR is an intelligent wireless communication system that is aware of its surrounding environment and adapts its internal parameters to achieve reliable and efficient communication. These new networks have many applications, such as the cognitive use of the TV white space spectrum or making secure calls in emergency situations. In order to create these new applications, CR differentiates between two kinds of users; primary users (PUs) are licensed users, and secondary users (SUs) are those who try to use the same bands when they detect a spectral hole. Adding cognition to the existing WSN infrastructure brings about a lot of benefits. However, cognitive technology will not only provide access to new spectrum bands but will also provide better propagation characteristics. By adaptively changing system parameters like modulation schemes, transmit power, carrier frequency, and constellation size, a wide variety of data rates can be achieved. This will certainly improve power consumption, network life, and reliability in a WSN.

The nature of large, dynamic, adaptive, and Cognitive Wireless Sensor Networks presents significant challenges in designing security schemes. A Cognitive Wireless Sensor Network is a special network that has many constraints and many different features compared to traditional WSNs. While security challenges have been widely tackled in traditional networks, it is a novel area in Cognitive Wireless Sensor Networks. The wireless medium is inherently less secure than the wired one because its broadcast nature makes eavesdropping simple. Any transmission can be easily intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Cognitive features allow for a dynamic reconfiguration to avoid these attacks. However, malicious nodes can use the dynamic reconfiguration to create new attacks such as Primary User Emulation (PUE). PUE is a new attack where a malicious node emulates the behavior of an incumbent node with the purpose of using the radio spectrum for its own interest or denying the access to other nodes.

To avoid these kinds of attacks some approaches have been investigated such as location-based approaches, but other cognitive features such as collaboration and learning have not been sufficiently exploited. We need to take into account that most WSNs have been developed in order to carry out a specific application. As a result, nodes usually have their own behavior pattern. This characteristic gives the network an opportunity to create a node profile for each sensor. These profiles can be created and optimized thanks to cognitive features such as spectrum awareness, learning, and collaboration. In this paper, simulations show how collaboration is essential to improve detection. Moreover, collaboration is the parameter that contributes most efficiently. The node profiles are used to detect anomalies in behavior and, for instance, PUE attacks.

The increasing use of WSN in many critical applications represents an important risk and a motivation for the study of the PUE attack. If a WSN that monitors a factory is attacked, the possibilities of errors in the systems increase. This means loss of money and replacement of machines. Another example is the home security systems. The malicious nodes could send corrupt information in order to hack the access service. If the system can detect the attack, it will omit the information from the attacker.

The organization of this paper is as follows. Section 2 explains the specific characteristics of the CWSN scenarios related to this work. In Section 3, works in security for PUE attacks is reviewed. In Section 4 a brief introduction to the main topics related to behavior learning and security are provided. Then, in Section 5, assumptions taken in account for the simulations are specified. Section 6 explains the general architecture of the system, while Section 7 provides its evaluation. Finally, the conclusions are shown in Section 8.

2. Cognitive Wireless Sensor Networks

A CWSN scenario includes multiple wireless sensor nodes, usually with a specific application. There are some specific characteristics of these CWSNs that imply some changes on how we understand these cognitive networks.

For example, CWSNs usually operate in the ISM bands, where anyone can transmit without license. Because of this feature, the definition of primary users (PUs) and secondary users (SUs) should be different. For this CWSNs definition, the differences between PUs and SUs are based on the priority of their functionality. For example, a fire sensor would be of more priority than a temperature sensor. In our case, an SU only transmits the prepare information when no PU is transmitting.

3. Related Work

According to Section 1 it is very clear that CWSNs face a dangerous problem in security. Several attacks could be adapted from WSNs to the new paradigm of cognitive networks. In the last ten years some researches related to security on CRNs have appeared. They describe specific attacks against these networks, but few countermeasures are proposed.

Most of the studies in security are focused on PUE detection. According to the origin of cognitive radio networks, the efficient use of TV spectrum in the USA and early studies used the location in order to detect malicious attacks. These PUs are TV towers with a precise behavior and location.

In [2] Chen and Park present the first method to detect a PUE attack based on location. The idea of this method is to differentiate the attacker from a licensed user comparing the transmission origin with the previously known PU position.

The same authors use a mechanism based on location in [3]. Moreover, they include some new parameters, such as the signal as power or RF fingerprints, to decide the nature of the signal.

In [4] the authors assume that the attacker is close to the victim and the real PU is much farther from the SUs than the attacker. Moreover, the position of each node, including the attacker, is fixed. Assuming that SUs can learn about the characteristics of the spectrum according to the received power, the authors in [5] follow a similar approach. Although they do not use any location information, they assume a static scenario with the PU much farther away from other possible malicious nodes than the SUs.

More location-based countermeasures can be found in [6, 7]. In the first work, secondary users calculate the estimated position of the PUE and then propagate this knowledge to carry out a coordinate decision. The second work is focused on the algorithm to detect the position of the PUE.

All these countermeasures are only based on the location. This characteristic cannot be used in some CWSN scenarios where both SUs and PUs can be mobile. Therefore, it is very clear that another approach should be adopted.

A few different solutions, not based on location, have been presented. In [8] the authors use the phase noise of a local oscillator as a fingerprint to identify the incumbent signals from the attacking ones.

Finally, in [9] the authors present a differential game approach to mitigate the PUE attack. Based on the assumption that PUE attacker has less energy than the PUs, they look for the optimal sensing strategy of SU. The Nash equilibrium solution is obtained.

Although these two last approaches are valid for mobile PUE attackers in CWSN, the algorithms implemented require relatively high computational resources, which is an impossible requirement in some WSNs.

In this paper, a solution based on the use of node behavior is presented. The cognitive features merged with WSN ones offer the possibility of collecting large amounts of information from the spectrum to model the behavior of each node. The spatial and temporal data redundancy makes it possible to use algorithms to detect changes in the behavior of each node in an unsupervised way.

4. Behavior-Based Systems

Like geolocation countermeasures, defenses based on behavior try to model the PU. The model is used to look for differences between a PU and attackers. For example, in [3] authors use some radio parameters to decide if the transmitter is an incumbent transmitter or an attacker. These parameters are as follows: transmitted power and location. For a typical TV scenario on CR the PU model can be very precise. However, as with geolocation countermeasures, the previous studies do not work with CWSNs. Unfortunately, a model for PU on CWSNs does not exist yet. PUs are usually more unpredictable than in previous scenarios. Moreover, the PU's behavior can be very different depending on the application. However, if we focus our CWSN on limited scenarios, for example, ambient intelligence in a home or a building, the PU is specifically defined. Parameters like power transmission, time occupancy of spectrum, and transmission frequency could be modeled.

Learned behaviors of these parameters allow the system to create some profiles which are compared with periodically acquired measures. It is easy to understand that, when a PUE attack happens, an anomaly in learned parameters can be detected. The intrinsic goals of an attacker make it impossible to have a complete likeness between a PU and a PUE attack. For example, if the goal of a PUE attack is the use of a whole frequency band, it needs to transmit more frequently, with more power and different types of packets than a normal PU.

In [10], the authors use the packet traffic to model the sensor behavior. The packet train size, packet train length, interpacket times, and payload size are used to characterize the packet traffic. They apply these profiles to detect anomalies, such as sinkhole attacks.

In [11], another approximation is taken to monitor the node's behavior. In this work, a group of capable nodes form the attack detection system (ADS) which analyzes the transmitted packets among its neighbors. The reason to limit the ADS to some nodes only is that a continuously monitoring node consumes much more energy than a normal one. Following the same idea, in [12], some monitor nodes sniff the communications in order to detect anomalies. They base their decisions on some principles of WSN such as message symmetry or node similarity.

Finally, in [13] the nodes create neighbor profiles according to the sequence of received packets. The attack is detected using the distance between sequences. The distance is calculated as the number of differences between them.

As a conclusion, the previous works use traffic monitoring to train a behavior model of the network. In this work, we can use other parameters such as power transmission to detect anomalies in CWSN. This is possible thanks to some cognitive features such as spectrum sensing and learning. The advantage of these parameters is that they can be used in more flexible networks or independently of the application. Another advantage over the previous works is the collaboration between nodes. The final decision in the detection of anomalies is collaborative. The more the nodes collaborating in the decisions, the better the PUE detection results. One important reason in order to use collaboration in this scenario is the ignorance of the attacker's position. If the system only uses the information of one or a few nodes, the node profiles might be wrong because of the attenuation or the distance between the SU and the attacker. For example, if an SU is still far from the attacker, it might not receive all the transmitted packets by the attacker. Moreover, the power received could be very variable because of the attenuation. The redundant information, inherent in WSN, and the collaboration in CWSN reduce the possibilities of errors in the sensed information, creating better profiles, and in the final decision. Another motivation for the collaboration is the resource limitation. Nodes of CWSN have to sleep, and their computing resources and energy are limited. During the sleep state, the nodes do not capture information. In these moments, other active nodes can capture information, and the profiles are developed with data from every time.

5. Assumptions and CWSN Scenario

Security is a rarely studied field in cognitive networks, and it is even less studied in CWSNs. But this does not mean that security is not important. On the contrary, security is important in WSNs and so will be in future cognitive applications such as health, home security, or military scenarios. Spectrum sensing is crucial in order to detect malicious behaviors in the transmissions or to analyze suspicious changes in the radio spectrum. The ability to learn and collaboration are also essential for many security algorithms. Finally, adaptation is the base of some countermeasures against jamming or routing attacks.

In our model, a CWSN consists of a set $S = \{s_1, s_2, \dots, s_n\}$ of n cognitive wireless sensor nodes with different roles. Each node can communicate with other nodes within a certain range. In a common CR application, the PUs are usually a TV tower or a base station. In most cases, the SUs know the location and the transmission parameters of PUs, but with CWSNs we cannot assume that. The location and the radio parameters of the nodes are unknown. However, we assume that the nodes have a stationary behavior that allows them to learn from spectrum sensing.

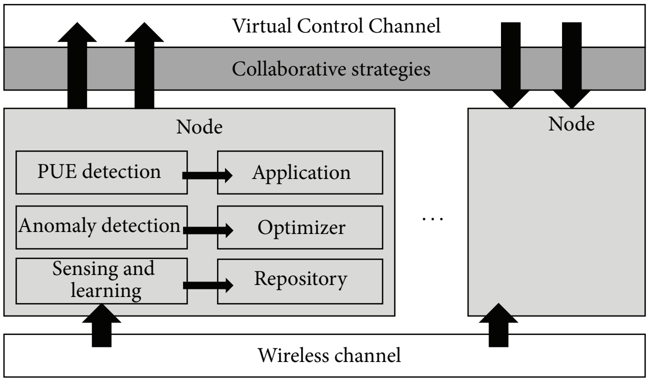


Figure 1: Cognitive features and modules responsible for them.

SUs and PUs act in CWSNs in different ways. While PUs take preference because they are responsible for critical sensors and information, SUs only send the information when the channel is empty or it satisfies some conditions. In a typical CWSN the number of nodes can usually vary between 5 and 200. For our study, we assume that networks with more than 200 nodes are not common.

In our scenario, spectrum sensing is carried out by multiple wireless modules that all nodes in the network have. More specifically, these interfaces work in the ISM bands (2.4 GHz and 868 MHz). All of them can extract information from the environment: received signal power, noise power, or time between packets. The information is processed, stored, and shared according to the implemented algorithm. We further assume the existence of a Virtual Control Channel (VCC) to share this information, with no extra overhead over regular cognitive communications.

Apart from primary and secondary users which form the network, the attackers are the key in security scenarios. The PUE attack in cognitive networks usually belongs to one of these two categories.

(i) *Selfish PUE Attacks*. In this attack, an attacker's objective is to maximize its own spectrum usage.

(ii) *Malicious PUE Attacks*. The objective of this attack is to obstruct secondary user's access to the spectrum.

Our PUE model is captured by the following set of assumptions.

(1) A PUE node is a wireless node with k wireless configurations (where k is the number of wireless configurations at each node NW).

(2) A PUE attacker has similar hardware and radio characteristics to the rest of nodes.

(3) The network does not have any information about the position of the PUE attacker or its strategy.

(4) The PUE attacker and the PUs cannot have exactly the same radio behavior.

As we explain in Section 4 we assume that, regardless of the kind of PUE attack, the malicious node has to change its behavior. If the node continues with the same behavior from the creation of the network and it uses exactly the same radio parameters, attack detection is impossible using either learning behavior or any other method.

6. System Architecture

The system architecture presented in Figure 1 makes use of the collaboration in order to achieve the anomaly detection goal. Its main characteristics are the distributed learning and the collaboration in the final decisions.

6.1. Spectrum Sensing and Learning.

Spectrum sensing is the first module of the entire chain in the system. All the nodes in the system sense the radio spectrum and analyze the data to create a precise enough profile of each node. The spectrum sensing in this system consists of the detection of the signal level in each channel. Each node is aware of the spectrum occupancy in its near range. Moreover, the nodes are able to detect all the valid packets over a reception power threshold. Despite the fact that the packets are usually sent to a specific node, the rest of the nodes in a sensing stage can capture the packets and extract information from them such as the source, the sink, and the time stamp.

Cognitive wireless nodes have some constraints that limit the system when a data base has to be created. For example, low computational resources and low available memory do not allow for the creation of complex detection algorithms or the storage of large data bases.

We propose the nonparametric Cumulative Sum (CUSUM) algorithm [14] for the detection of changes in some key spectrum sensing captured features. The CUSUM is an algorithm used in WSN in order to detect changes in the mean value of a stochastic process. The advantages of this algorithm in CWSN are the low computational requirements and the no assumption of any previous knowledge about the PUE attack. As it has been explained in Section 4, if the scenario is limited, usually the sensor nodes have a stationary behavior. Moreover, the attack happens at unknown time. These are the reasons why the CUSUM algorithm is applicable in this approach.

In this case, some key features, such as the received power, are necessary to model the node behavior. A good approximation is to save the key parameters that define the feature. In this work, the number of measures, the average, and the variance are stored in each node repository. The average "X_n" and the variance "S_n" are calculated using only the previous one's value and the current sample as shown in

$$\overline{X_n} = \frac{1}{n}\sum_{i=1}^{n} x_i = \overline{X_{n-1}\frac{n-1}{n}} + \frac{x_n}{n},$$

$$\overline{S_n^2} = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - \left|X_n\right|^2 = \overline{E_n^2} - \left|X_n\right|^2, \qquad (1)$$

$$\overline{E_n^2} = \overline{E_{n-1}^2\frac{n-1}{n}} + \frac{x_n^2}{n},$$

where $\overline{E_n^2}$ is the average of the squared values. So, each node creates a table with the following data:

$$\left\{\text{Node ID}, n, \overline{X_n}, \overline{E_n^2}\ \overline{S_n^2}, \right\}, \qquad (2)$$

Throughout the learning stage the nodes update and refine these values which will be used as the base in the anomaly detection algorithm.

6.2. Anomaly Detection. When the system has captured enough packets, the node profiles are ready to compare themselves against the new samples. During this step, the optimizer applies the CUSUM algorithm, compares the current samples with the average in the profiles, $\overline{X_n}$, and sends anomaly warnings to the application. The comparison between the samples and the profile is calculated according to the Euclidean distance. If the distance is lower than a number of standard deviations, sample is considered as a normal value. However, if the sample is out of the allowed range, the optimizer sends the anomaly warning to the application level. In this way, the algorithm can be configured with high threshold values, with low false positive rate and slow detection or with low threshold values that imply more false positives but a faster detection.

The application layer is responsible for managing anomaly warnings. Above the application layer, the whole system can be applied for any anomaly detection. In this work, the application filters the warnings and only creates a PUE attack warning when the anomaly continues for a configurable time. If the anomaly behavior in a node exceeds that time, the application marks the node as a possible PUE attacker.

6.3. Collaboration. The previous chapters describe how the nodes in the network can collect information from the spectrum as a key feature in cognitive solutions. The stored information used by an isolated node could be useful for a particular optimization, but if the final goal of the network is a general optimization of a parameter, in this case the security and collaborative strategies are essential. Collaboration strategies are a common solution in other cognitive fields like spectrum sensing and also in security scenarios, such as PUE detection. The next section shows how the introduction of collaborative detection significantly improves results.

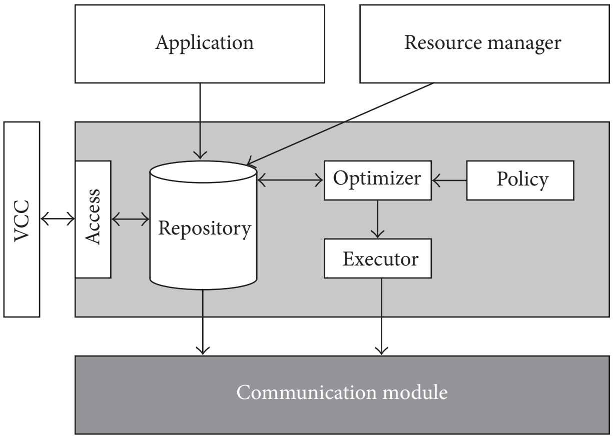


Figure 2: Cognitive radio module structure.

In this work, the SU nodes collaborate by sharing information about the detected anomalies. This information may be characteristic of spectrum sensing or anomalies detected by a single node. When an application marks a node as a possible PUE attacker, it sends a message through the Virtual Control Channel (VCC), a method for sharing information in cognitive networks. Finally, as we will explain later, the VCC allows other nodes to access to almost any information stored in other neighbor nodes.

7. Experimental Results

7.1. Simulation Tools. The proposed countermeasures have been tested on a CWSN simulator [15]. This simulator has been developed over the well-known Castalia simulator. The structure of Castalia has been improved to provide it with cognitive features. The CWSN simulator is responsible for the scenario definition, the simulation of the spectrum state, and the communication between nodes from the physical to the application layer. It supports the cognitive features in the cognitive module, shown in Figure 2, which has the following parts.

(i) *Repository*. It retrieves information about the local and/or remote nodes: information learned, decisions made, or current state. The kind of information stored depends on the context and the requirements of the system.

(ii) *Access*. This module lets a local repository access the repository of remote nodes. At the same time, it exports a subset of the local repository to remote nodes.

(iii) *Policy*. This enforces the requirements for the global system depending on several factors. In this paper, security is the policy to optimize.

(iv) *Optimizer*. This processes the repository information bearing in mind the requirements imposed by the policy module. Decisions regarding the behavior of the local node are the results of processing. They are stored in the repository and evaluated by the executor.

(v) *Executor*. This module performs the decisions made by the optimizer.

Furthermore, it provides the Virtual Control Channel (VCC), a new method for sharing cognitive information among the CR modules of the nodes. CR modules can access exported information from remote repositories through this channel. It allows CR modules to be aware of their surroundings and even of the whole network.

7.2. Simulation Experiments. The attacker is implemented as an SU that changes its behavior in a precise moment acting like a PU. The attacker will try to adapt all radio parameters according to the PU behavior. Some of them, such as modulation, encoding, or carrier frequency, probably will be exactly like those of the PU for two reasons. The attackers and the PUs usually have the same hardware characteristics; therefore the attackers can imitate the PU. The second reason is that the attackers do not need to change these parameters to reach their possible goals: to use more spectrum, to transmit information to other destinations, or to prevent SUs transmissions.

According to this, it is reasonable to restrict the parameters that the attackers will change to transmitted power and occupied spectrum bandwidth. In this work the received power has been used to detect anomalies, like a PUE attack in the network.

Setting this parameter to a similar value to those used by a real PU we can check how precise the algorithm is in detecting this kind of attacks.

In order to test the presented solution, when an attacker changes its behavior, the maximum allowed change in transmitted power is 1 dBm. Even with this small change, the system has demonstrated to be very efficient in detecting anomalies.

Several simulations have been executed in the simulator to extract results and to draw conclusions from the work. The scenarios have some common characteristics.

(i) The scenario area is a 30 m × 30 m square.

(ii) The complete simulation time is 500 seconds.

(iii) The number of nodes in the simulation varies between 50 and 200, including one server, 6 Pus, and a variable number of attackers.

(iv) The learning stage covers the first 60 seconds.

(v) The attacks start at second 100.

(vi) The SUs and PUs send information to the sink.

(vii) However SUs only send the information when the channel is not being used by any PU.

7.3. Results and Discussion. The first figures (Figures 3 and 4) present results about the learning speed of the systems. That means how much time the system needs to converge and to reach acceptable learned values.

The results of a network with 50 nodes are shown in Figures 3 and 4. Figure 3 represents how an SU learns about the power received from other node which has an abnormal operation. The node has a normal behavior during the first 30 transmitted packets. At this time, the attack starts, and the sensing power changes. As we can observe, the average is stable with a few samples. The top limit and the bottom limit form a range where the sensing data is considered normal. When the data is out of the limits, the node interprets it as an anomaly.

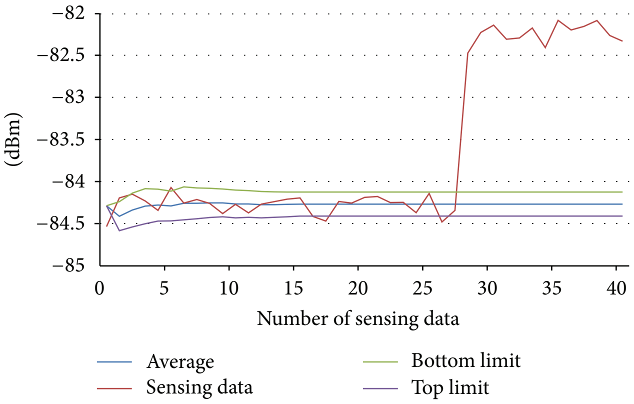


Figure 3: Sensing power and learning average from a PUE attacker node.

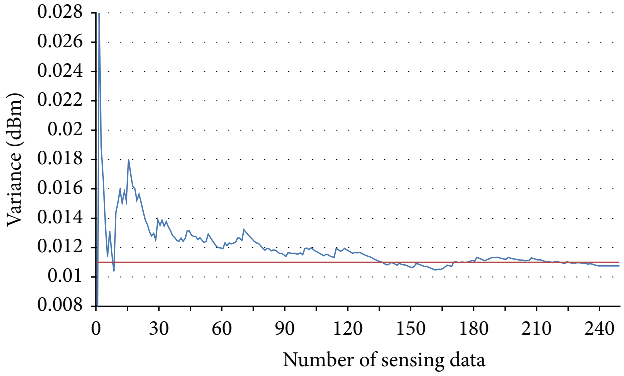


Figure 4: Learning power variance from PUE attacker node.

In the second figure, we can observe how fast the system learns. With few samples, the variance fluctuates but, when the node has more information, the variance stabilizes over 1%. The number of received packets that a node needs to refine the information is showed in the x-axis.

In the next figures (Figures 5, 6, 7, and 8), where the PUE attack scenarios are presented, the false positive parameter is presented. The system has shown very good behavior in detecting the attackers, with a detection rate over 98% in all simulations. However, for some combination of parameters, some normal nodes are detected as attackers. In Figure 5 we can see the results of a simulation with 50 nodes, including 5 PUE attackers, 6 PUs, 1 sink, and 38 SUs. In this situation the decisions taken individually by each node are complemented by the collaboration between nodes. Each line represents a different scenario whit the percentage of SUs that collaborate in the detection changes. The x-axis represents the number of standard deviations that a sensing power measure can deviate

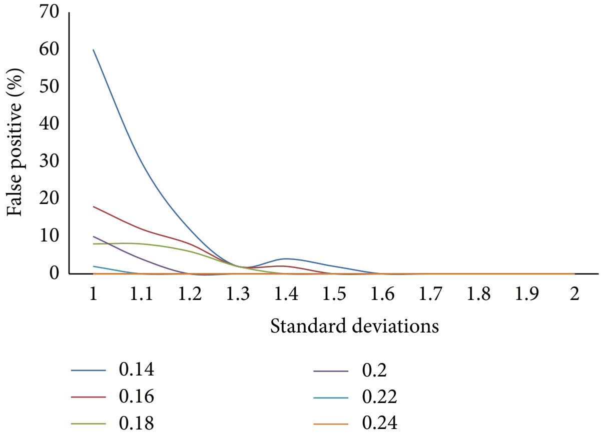


Figure 5: PUE detection results with 50 nodes.

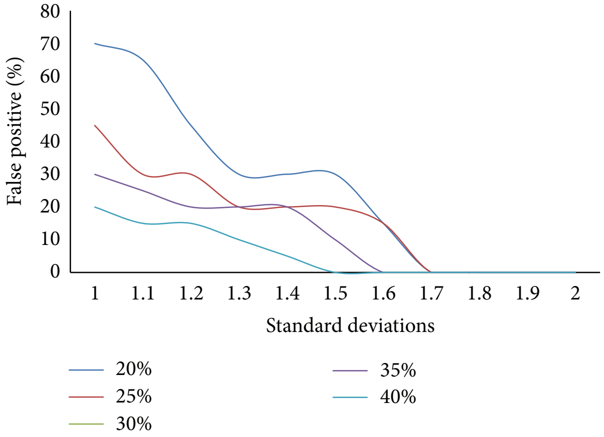


Figure 6: PUE detection results without filtering in the nodes.

from the learning average to be considered as a normal value. Finally, the y-axis represents the false positive percentage.

As we can appreciate, the percentage of collaborative nodes is essential in the PUE detection. For a percentage of around 20% of collaborating nodes the results are very good, with a false positive rate of under 10% with a margin of one standard deviation for anomaly warnings regarding the average in the profile. If we increase the parameter to 1.3, the results are very satisfactory with false positive and false negative rates near 0%.

Figure 6 shows another scenario with worse conditions than the previous one. In this case, the nodes send worse information than in the previous scenario to the other nodes. This is because the node's application does not filter the information received from the optimizer, as Section 6.2 explains, and sends too many anomaly warnings through the VCC. However, if the margin of standard deviations is increased to 1.5 and the number of collaborative nodes is over 30%, the results are good enough.

However, if the collaboration between nodes is eliminated and the filter in the nodes is improved, the system has shown poor results. The system is not capable of discriminating between the PUEs and normal behavior.

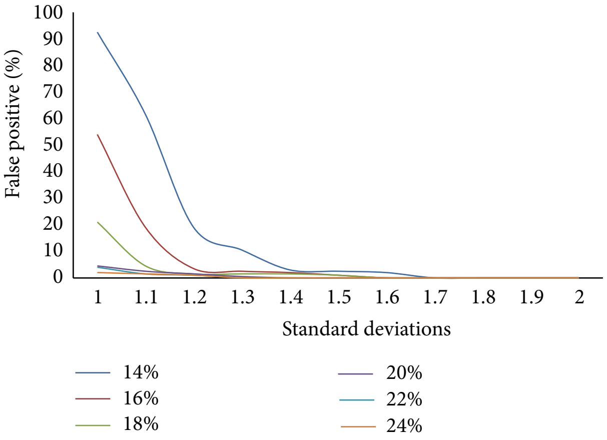


Figure 7: PUE detection results in a network with 200 nodes.

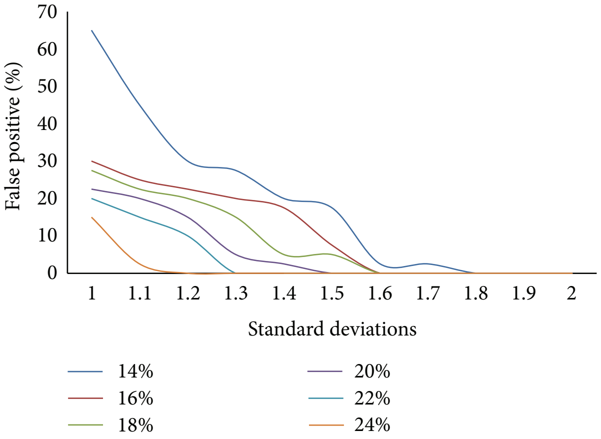


Figure 8: False positives in a multiple PUE attack.

In order to prove the proper working of the system in larger networks, we have simulated a new scenario with 200 nodes. Figure 7 shows that, if the percentage of collaborating nodes is the same, the system keeps differentiating the PUE attack in almost every simulation, but the results become slightly worse. This is because more nodes in the same scenario space can produce more anomalies such as collisions, interference, higher noise level, or retransmissions.

As another interesting result, in Figure 8, the behavior of the system can be observed against a multiple PUE attack, where 10 malicious nodes attack the system after the learning time. In this case, where 25% of the nodes are attackers, the system behavior gets worse. But, even in this case, if the number of collaborative nodes is over 20%, the results are satisfactory.

The results conclude that the most important parameter to improve PUE detection is the number of collaborative nodes. Other parameters, such as the application algorithm or filter and the margin to mark data as anomalous, affect the results but to a lesser extent.

The same analysis has been studied using the bandwidth occupied by the nodes. In this case, the results are not good enough. The reason for the poor results is the behavior of the secondary users. As we have explained before, the secondary nodes only send packets when the channel is free, so the occupied bandwidth has a greater variance than in the power detection-based scenarios. The PUE attack has been impossible to detect with good precision using the occupied bandwidth. This only means that the presented algorithm does not work with our definition of the SUs.

8. Conclusions

In this paper, a new method of detecting PUE attacks on CWSNs has been described based on cognitive features such as sensing, learning, and collaboration. A new simulator has been used to develop the scenarios that prove that collaboration is essential for good anomaly detection. The results have been extracted and presented in the graphics shown in Section 7.3.

Different layers of cognitive architecture implement the tasks to achieve the final objective, PUE detection. Cognitive nodes sense the spectrum and create neighbor profiles in order to model the behavior. The information stored in the repository is used to warn the application about anomalous data. The application is responsible for filtering the information and collaborating with other nodes.

If the collaborative nodes are over 20% of the total, the PUE attack detection has satisfactory results, with a 98% of attacks detected and a false negative rate near 0%, independently of the number of nodes in the scenario.

As the results show, the collaborative systems and the behavior models are valid to detect a PUE attack when there are few PUE attacker nodes compared with the total number of nodes in the network, and we assume that PUE attacker should change its behavior in order to reach the malicious goals.

References

[1] J. Huang, G. Xing, G. Zhou, and R. Zhou, “Beyond co-existence: exploiting WiFi white space for Zigbee performance assurance,” in *Proceedings of the 18th IEEE International Conference on Network Protocols (ICNP ’10)*, pp. 305–314, October 2010.

[2] R. Chen and J.-M. Park, “Ensuring trustworthy spectrum sensing in cognitive radio networks,” in *Proceedings of the 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks (SDR ’06)*, pp. 110–119, September 2006.

[3] R. Chen, J.-M. 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.

[4] 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 IEEE 28th International Performance Computing and Communications Conference (IPCCC ’09)*, pp. 208–215, December 2009.

[5] 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)*, pp. 1–5, June 2009.

[6] Z. Yuan, D. Niyato, H. Li, and Z. Han, “Defense against primary user emulation attacks using belief propagation of location information in cognitive radio networks,” in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC ’11)*, pp. 599–604, March 2011.

[7] L. Huang, L. Xie, H. Yu, W. Wang, and Y. Yao, “Anti-PUE attack based on joint position verification in cognitive radio networks,” in *Proceedings of the International Conference on Communications and Mobile Computing (CMC ’10)*, pp. 169–173, April 2010.

[8] Z. Caidan, W. Wumei, H. Lianfen, and Y. Yan, “Anti-PUE attack base on the transmitter fingerprint identification in cognitive radio,” in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM ’09)*, pp. 1–5, September 2009.

[9] D. Hao and K. Sakurai, “A differential game approach to mitigating primary user emulation attacks in cognitive radio networks,” in *Proceedings of the IEEE 26th International Conference on Advanced Information Networking and Applications (AINA ’12)*, pp. 495–502, March 2012.

[10] Q. Wang, “Packet traffic: a good data source for wireless sensor network modeling and anomaly detection,” *IEEE Network*, vol. 25, no. 3, pp. 15–21, 2011.

[11] L. Yang and H. Kai, “Behavior-based attack detection and reporting in wireless sensor networks,” in *Proceedings of the 3rd International Symposium on Electronic Commerce and Security (ISECS ’10)*, pp. 209–212, July 2010.

[12] F. Wang and J. Gao, “Behavior monitoring framework in large-scale wireless sensor networks,” in *Proceedings of the IEEE 29th International Performance Computing and Communications Conference (IPCCC ’10)*, pp. 138–145, December 2010.

[13] Q. Wang and T. Zhang, “Detecting anomaly node behavior in wireless sensor networks,” in *Proceedings of the 21st International Conference on Advanced Information Networking and ApplicationsWorkshops/Symposia (AINAW ’07)*, pp. 451–456, May 2007.

[14] S. Rajasegarar, C. Leckie, and M. Palaniswami, “Anomaly detection in wireless sensor networks,” *IEEE Wireless Communications*, vol. 15, no. 4, pp. 34–40, 2008.

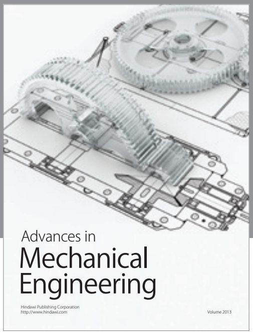
[15] J. Blesa, E. Romero, J. C. Vallejo, D. Villanueva, and A. Araujo, “A cognitive simulator for wireless sensor networks,” in *Proceedings of the 5th Internation Symposium of Ubiquitous Computing and Ambient Intelligence (UCAMI ’11)*, December 2011.

The Scientific World Journal

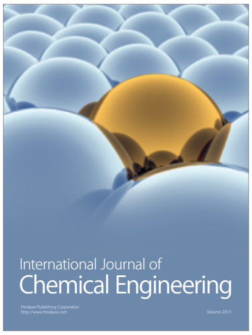
Journal of
Electrical and Computer Engineering

International Journal of
Rotating Machinery

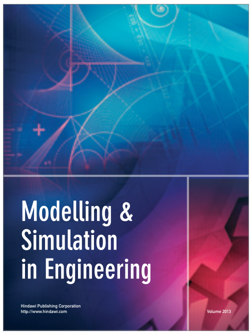
Active and Passive Electronic Components


Advances in
Mechanical Engineering

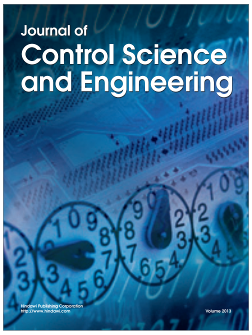
International Journal of
Distributed Sensor Networks

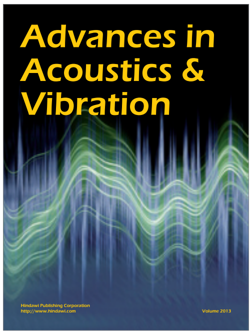

International Journal of
Chemical Engineering

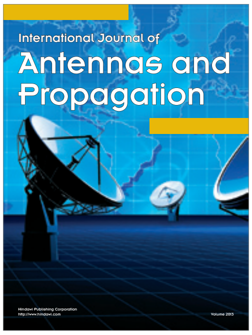
VLSI Design

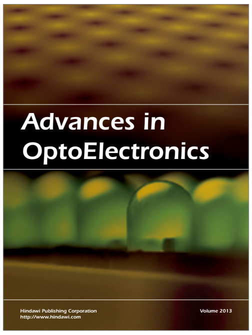

Modelling & Simulation in Engineering

Journal of
Sensors

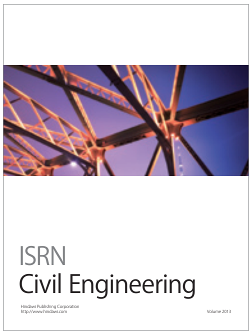

Journal of
Control Science and Engineering

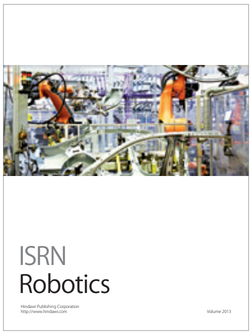

Advances in Acoustics & Vibration

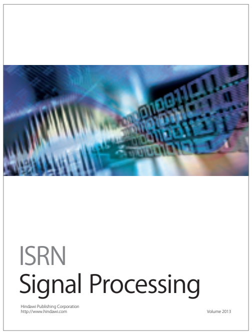

International Journal of
Antennas and Propagation


Advances in OptoElectronics

ISRN
Electronics


ISRN
Civil Engineering


ISRN
Robotics


ISRN
Signal Processing

ISRN
Sensor Networks