Research Article

Primary User Emulation in Cognitive Radio-Enabled WSNs for Structural Health Monitoring: Modeling and Attack Detection

Hassel Aurora Alcala' Garrido,¹ Mario E. Rivero-Angeles ,¹ and Eleazar Aguirre Anaya ²

¹Network and Data Science Laboratory, CIC-Instituto Politecnico Nacional, Mexico City, Mexico

²Cybersecurity Laboratory, CIC-Instituto Politecnico Nacional, Mexico City, Mexico

Correspondence should be addressed to Mario E. Rivero-Angeles; mriveroa@ipn.mx

Received 16 August 2018; Revised 8 January 2019; Accepted 18 February 2019; Published 28 April 2019

Academic Editor: Bruno Andò

Copyright © 2019 Hassel Aurora Alcala' Garrido et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Nowadays, the use of sensor nodes for the IoT is widespread. At the same time, cyberattacks on these systems have become a relevant design consideration in the practical deployment of wireless sensor networks (WSNs). However, there are some types of attacks that have to be prevented or detected as fast as possible, like, for example, attacks that put lives in danger. In this regard, a primary user emulation (PUE) attack in a structural health monitoring (SHM) system falls inside this category since nodes failing to report structural damages may cause a collapse of the building with no warning to people inside it. Building on this, we mathematically model an energy and resource utilization-efficient WSN based on the cognitive radio (CR) technique to monitor the SHM of buildings when a seismic activity occurs, making efficient use of scarce bandwidth when a PUE attack is in progress. The main performance metrics considered in this work are average packet delay and average energy consumption. The proposed model allows an additional tool for the prompt identification of such attacks in order to implement effective countermeasures.

1. Introduction

Recent electronic advances have led to the construction and design of compact-sized, energy-efficient, and low-cost sensor nodes that can communicate wirelessly through relatively long distances. This, in turn, allows the development of wireless sensor networks (WSNs) composed by tens or hundreds of such sensor nodes that have to operate in a cooperative manner in order to efficiently transmit data relative to a certain physical variable of interest monitored in the area where the network is deployed. Furthermore, WSNs are typically powered by batteries which limit the node's lifetime based on the number of packet transmissions and receptions plus the energy consumed by the data processing and storage.

Deployment of sensors in a region may be preplanned or randomly placed in the interest region. Nodes inside a sensor network compete for the shared frequencies for data transmission in order to provide diverse applications for the Internet of things (IoT) where machines, like nodes in a WSN, gather important information about the surroundings [1].

This information is usually regarding special events that occur in the area under observation. The organization of their internal software and hardware must be configured properly in order to work effectively and be able to adapt dynamically to new environments, requirements, and applications [2]. In WSNs, nodes can have atypical behaviors due to faulty circuits or due to environmental factors or even targeted attacks that have to be timely identified to avoid extra energy consumption or prevent relevant data to reach the network operator. Faulty sensors, physical damage to sensor nodes, migration in sensor node position, software bug or hardwired faults, and denial of service attacks are some of the few causes of faults, misbehaviors, and anomalies in sensor networks [3].

In this work, we study the impact of a primary user emulation (PUE) attack in an event-driven WSN [4, 5] where nodes are used to monitor vibrations in buildings or home structures. These nodes are used to send relevant data to a sink node whenever important movement in strategic points of the structure occurs as a result of an earthquake, strong

winds, vibration caused by traffic, or even the natural movement in high buildings. Hence, the WSN is used for structural health monitoring (SHM) applications. As such, in these conditions, many nodes in a reduced area are expected to detect such vibrations generating a high number of simultaneous packet transmissions causing interference to the conventional communication systems in these environments, mainly Wi-Fi networks, hindering the system operation and even preventing user's communications. To address this issue, we propose the use of cognitive radio (CR) technology.

The SHM system is not intended to generate timely alarms in case of seismic activity. Rather, it is designed in order to monitor acceleration and vibration in specific points in the building. This information is gathered during the seismic event and transmitted to a sink node and then from the sink node to a disaster center in order to analyze it in search of possible structural damage. This system is proposed to reduce the time since the event occurs until human intervention in situ is done reviewing, mostly by visual inspection, each building in the affected region. This procedure may take many days or even weeks due to the lack of qualified personnel in medium to large cities. Also, much structural damages cannot be seen in a visual form which presents a great danger for people working or living in such buildings. By implementing sensor nodes inside key points in the structure may reveal possible affectations in a much shorter time in order to perform an in-depth revision to critical buildings, potentially saving many lives.

In general, a PUE attack prevents nodes from communicating and reporting their data during a certain time since a malicious attacker emulates primary user transmissions in such a way as making secondary users to believe that the channel is occupied preventing event reports from the WSN. This attack also consumes the energy of the system much faster than in normal conditions, since nodes are constantly attempting to transmit, listening to the channel in search of transmission opportunities. Furthermore, in SHM applications, such attacks pose a great threat to people's lives by preventing the appropriate reporting of possible structural damage after an earthquake. Building on this, we propose a discrete time Markov chain to study the performance of the system and detect possible PUE attacks. This is done by observing an increase in the energy consumption and reporting delay which can be seen abnormal. As such, the proposed analysis can also be used to detect PUE attacks in other systems.

Cognitive radio capabilities allow an efficient use of radio resources since two different networks use the same physical channels without degrading the performance of the primary system and opportunistically exploiting empty spaces by the secondary network. All secondary users (nodes that do not own the license to use the spectrum but have an agreement with the system that owns it) that have a packet to transmit have to sense the channel in order to detect any activity from primary users and identify the frequencies and channels available to use in an opportunistic manner [6]. In case that primary users are detected in a channel being used by a secondary user, it has to be released in such a way as

to prevent any interference on the primary system. [6, 7]. In licensed bands, users from the primary system (primary users, PUs) have the permission and priority to use the communication resources while nodes in the secondary system (also called SUs) make use of the available resources only when they cause no degradation to the service of PUs [8]. CR capabilities are of particular interest in crowded spectrum bands such as Wi-Fi and cellular networks where fixed spectrum allocation is used [9].

Previous works have focused on SHM by implementing WSNs in the monitored structures [10–17]. However, none of these works considered the impact of a cyberattack and provide analytical tools to detect and prevent them. Also, different approaches for early seismic alarm generation have been proposed, where the objective is to detect as soon as possible an earthquake and generate alarms to prevent the people in a building [18]. Conversely, our focus is on gathering as much information as possible of the seismic activity and effectively convey it to a disaster center in order to identify potential structural damages in buildings and houses.

The structural health monitoring systems have been used before in order to detect and prevent damage in buildings as a result of vibrations that occur in normal (e.g., winds and live loading) or abnormal (e.g., earthquakes) conditions. In these classic SHM systems, coaxial wires have been employed to connect the vibration sensors to data center repositories in order to collect as much information as possible regarding the conditions of the structures and collect such data in weekly or monthly visits by qualified personnel in charge of the *health* of the building. Coaxial wires provide an interference-free communication system, offering reliable data recollection. However, they have to be installed during the construction of the building or through a very costly and labor-intensive procedure after the construction, effectively limiting the number of sensors in site. In old buildings, for instance, additional measures have to be considered to avoid any structural damage in the installation of such cables and data centers. As an alternative to these conventional systems, the use of WSNs provides a low-cost and fast installation alternative to provide SHM. Since sensor nodes are small, they can be installed in many parts of the building without affecting the aesthetics or adding cumbersome equipment in both new and old buildings. As such, a high number of such nodes capable of wirelessly communicating among each other and to a sink node can provide much accurate monitoring of junctions or load points of the structures for local-based damage detection [19].

Security provision in wireless systems is very challenging in general and even harder in new technologies where autonomous nodes perform very complex operations. Specifically, in the case of cognitive radio network, the malicious user can behave like a legitimate user either to capture the communication process or to launch different types of attacks [20]. For example, in [20], the authors show authentication mechanisms to legitimate primary users from the available spectrum usage by means of physical layer network coding techniques. In [21], the authors focus on jamming and blackhole attacks. They propose a mechanism based on a

systematic approach to analyze the impact in the behavior of nodes due to a denial-of-service attack on a mesh network. First, they identify a large number of metrics such as received signal strength indicator (RSSI), transmit/listen time, transmit/listen duty cycle, transmitted/received packets on the network layer, transmitted/received packets on MAC layer, packets with invalid CRC checksum, and energy consumption by radio activities. Then, they consider the intensity of the normal data traffic in a WSN, and the transmission power in order to understand the impact of these factors on the metrics and thus on attack detection. Next, they statistically test these metrics using the cumulative distribution function and perform the Kolmogorov-Smirnov test to assess whether they exhibit significantly different values under attack when compared to those of the baseline operation. However, no cognitive radio is considered. In contrast to [21], we propose a mathematical model as a tool for attack detection instead of practical measurements on the system's performance. The mathematical analysis is more tractable than measuring the system operation in normal conditions. However, for more complex systems, a mathematical analysis is not always possible. Furthermore, we believe that both techniques can work simultaneously in order to strengthen the overall security of the system since these tools are not exclusive. In [22], the authors propose to use the entropy as a parameter to detect denial-of-service attacks on the SIP protocol. The detection method proposes a training period where no attacks are active. In contrast, we propose a mathematical methodology where training is not required since the average packet delay and energy consumption can be known in advance by numerically solving the proposed Markov chain.

Finally in our previous works [23–25], we presented a similar work. However, in [23], we presented only simulation results, while in [24], we considered a continuous process for the primary network and only the cluster formation phase was mathematically modeled. Then, in [25], we developed a discrete model to analytically study the complete cognitive system. However, in none of these previous works the impact of a cyberattack was considered nor any guidelines for the detection and prevention were provided. As such, new Markov chains are developed for both the cluster formation and steady-state phases considering now an attack probability. Also, new numerical results for the average packet delay, average cluster formation, and average energy consumption are obtained in order to investigate the impact of an attack on the WSN.

Based on the aforementioned investigations, the following considerations are taken into account for the detection and performance evaluation of the impact of a PUE attack in SHM environments:

- (i) Considering the advantages of a clustered architecture [13], a cluster topology is proposed and the network is evaluated in terms of average cluster formation (CF) time and average power consumption at the cluster formation phase. Also, the impact of the cyberattack is studied based on the increase energy consumption and average reporting delay

for the entire seismic event reporting, which occurs after clusters are already formed, also called the steady-state phase

- (ii) A WSN with CR capability can work as a mechanism to use efficiently the radio spectrum resources in a wireless medium so that energy consumption and channel occupancy can be reduced
- (iii) A PUE attack where a malicious node prevents the whole network from communication either at the cluster formation phase or at the steady-state phase is considered. In this regard, we consider that multiple sensor networks are deployed in buildings, where each network is composed of multiple sensor nodes that can directly communicate among them. Also, we consider that these multiple networks can be placed far apart of each other and do not interfere among them. We propose a mathematical model to study the impact of the attack based on the probability that it is in progress at each time slot
- (iv) Some of the requirements of this work are similar to [18]
- (v) Specifically, the performance evaluation of a system for reporting data vibration of a building and the objective of the WSN is to transmit the building's acceleration or vibration readings to a base station (BS) to evaluate possible damage to the infrastructure; therefore, a long time delay can be supported due to a cluster topology. In addition, a mathematical model to evaluate the performance of the system is proposed, while [18] focuses on a practical system implementation to obtain these metrics. Additionally, [18] does not consider the operation under a cyberattack

The rest of the paper is organized as follows: first, Section 2 presents the system operation, Section 3 describes the cyberattack modeled and considered in this work, Section 4 develops the analysis of the WSN with a cybernetic attack, and in Section 5, we show some relevant numerical results and finally our main conclusions.

2. System Operation

In this section, we specify the main variables and system operation of the cognitive radio system using the cellular network as the primary system and the WSN for SHM as the secondary system under a PUE cyberattack.

2.1. Secondary Network: WSN. We consider a cluster-based and event-driven WSN. Clustering has been used to reduce energy consumption [26, 27]. In such architectures, nodes are classified either as cluster members (CMs) or cluster heads (CHs). The latter is in charge of gathering information from its members and then relaying such data to the sink node. The former is charged only with the gathering of information tasks and relaying such data to their CH. This effectively reduces long range transmissions since

CMs perform short-range transmissions to their CH. The CHs, however, have to make long range transmissions to the sink node that can be placed outside the network. As such, it is important to change the role of CHs and CMs in order to prevent premature energy depletion. Note that the use of the cellular system's frequencies by the WSN does not imply transmissions to the base stations of the cellular network. Instead, secondary nodes transmit to the sink nodes inside the monitored structures (short-range and local transmissions) using the cellular frequencies and then the sink node transmits the data to the disaster center control by any other possible means (fiber optics, microwaves, satellite systems, or others).

In high residence or commercial buildings, there are well-known load columns and junctions where multiple sensors are required in order to have an accurate structure monitoring, while some other parts of the building's structure offer no real utility in terms of structural damage control. As such, many sensors can be placed in these strategic points and around them, allowing direct communication among these sensor nodes separated by long empty spaces (where no sensors are placed). Building from this, a structural health monitoring network can be composed of many individual sensor networks that can be considered independent and there is no interference among them. We focus our study on one of such isolated networks since we assume that they are all statistically similar in terms of the number of nodes and monitoring area. In order to form the clusters in one of these independent networks, all nodes have to transmit a short packet using the slotted NP-CSMA (nonpersistent carrier sense multiple access) protocol [28, 29] where nodes (re)transmit according to a geometric backoff with parameter τ . As studied in [30], the transmission probability τ has to be carefully selected in order to ensure an appropriate system performance. After all nodes have successfully transmitted and the sink node has the information regarding all active nodes, CMs can transmit according to a specific schedule to their respective CH using a TDMA (time division multiple access) protocol. This phase is also called the steady-state phase.

In the steady-state phase, we assume N_{CM} nodes per cluster in average. Also, we consider that each cluster member transmits packets of P bits at a data rate of R (bits/sec). From this, it is easy to see that the time required to transmit a data packet is $T = (P/R)$ sec. As such time slots of T seconds are considered and the average frame duration is given by $(N_{CM} + 1)T$ [29]. As for the energy consumption in the system, we make the following assumptions: as described in [26], the energy consumed in the transmission of a packet can be described as follows:

$$E_{Tx}(k, d) = E_{elec} * k + \epsilon_{amp} * k * d^2, \quad (1)$$

where $E_{elec} = 50$ nJ/bit is the energy consumed by the electronic systems of the node, k is the number of bits of the packet, $\epsilon_{amp} = 100$ pJ/bit/m² is the energy consumed by the amplification circuits in charge of the transmission (the receiver node does not use these circuits), and d is the distance between the transmitter and the intended receiver.

On the other hand, the energy consumed by the reception of a packet is given as follows:

$$E_{Tx}(k, d) = E_{elec} * k. \quad (2)$$

Building from this, the energy consumed by the transmission of the control packet in the cluster formation phase is given by $E_{tx}^{CF}(16, 50) = 8.8[\mu J]$ considering that a 2-byte packet is used and the sink node is found at most at 50 meters from any node in a given section of the building. Also, energy consumed by the reception of a control packet in the cluster formation phase is given by $E_{rx}^{CF} = 0.8[\mu J]$. Hence, normalizing by E_{tx}^{CF} , i.e., considering that E_{tx}^{CF} is one energy unit, it is easy to see that $E_{rx}^{CF} = 0.09 * E_{tx}^{CF}$. To simplify the analysis, we approximate it as $E_{rx}^{CF} \approx 0.1 * E_{tx}^{CF}$. For the steady-state phase, the energy consumed by the transmission of a cluster member to its cluster head can be calculated as $E_{tx}^S(24, 40) = 5.04[\mu J]$ considering a lower distance and higher number of bits per packet, while the energy consumed by the reception of such packet is given by $E_{rx}^S = 1.2[\mu J]$.

These energy units correspond to $E_{tx}^S = 0.57 * E_{tx}^{CF}$ and $E_{rx}^S = 0.13 * E_{tx}^{CF}$ which we approximate to $E_{tx}^S \approx 0.5 * E_{tx}^{CF}$ and $E_{rx}^S \approx 0.1 * E_{tx}^{CF}$. Finally, the energy consumed to transmit an aggregated packet from the cluster head to the sink node can be calculated as $E_{tx}^{sink}(52, 50) = 13.75[\mu J]$ considering again that the distance from any node to the sink is at most 50 meters and an aggregated packet is longer than a regular data packet. As such, $E_{tx}^{sink} = 1.56 * E_{tx}^{CF}$ which we approximate to $E_{tx}^{sink} \approx 1.5 * E_{tx}^{CF}$.

From this and as in [9], we can normalize the energy consumption using energy units, where a packet transmission in the CF phase is $E_{tx}^{CF} = 1$ energy units, a control packet received in this same phase is $E_{rx}^{CF} = 0.1$ energy units, a packet transmitted in the steady state is $E_{tx}^S = 0.5$ energy units, a packet received in the same phase is $E_{rx}^S = 0.1$ energy units, and a packet transmitted from the cluster heads to the sink node is $E_{tx}^{sink} = 1.5$ energy units. From this, it is evident that nodes acting as CHs consume more energy than nodes acting as members since the former have to be active during the complete round in the steady state receiving data from its members and conveying such data to the sink node. Also, it can be seen that energy consumption for packet reception consumes low energy units since it basically depends on the packet length but not on the distance between transmitter and receiver. Then energy consumption is lower in the CF phase than in the SS phase since in the former, packets are mainly control packets with no information other than the ID of the nodes. Finally, the transmission from CHs to the sink nodes is highly costly since transmissions are performed over a high distance range.

2.2. Primary Network: Cellular System. A blocked customers cleared (BCC) system is considered where users arrive to the system according to a Poisson process. Voice channels are assigned randomly to incoming users only if empty channels exist. Otherwise, the user is blocked and has to retry access in a future time. We consider a system with S channels.

Hence, at most, S simultaneous voice call can be active in a given time. In order to mathematically study the complete system, we use the discrete model of this continuous process as in [31], where the probability that n packets arrive in the period of $(t - T_{\text{slot}}, t)$ can be written as follows:

$$P_A(n) = P\{N(t - T_{\text{slot}}, t) = n\} = \frac{(\lambda T_{\text{slot}})^n e^{-\lambda T_{\text{slot}}}}{n!}. \quad (3)$$

Average service time is assumed to be exponentially distributed with mean $1/\mu$. In [25], it was shown that the probability that a user leaves the system in a particular time slot can be approximated by a geometric distribution with parameter as follows:

$$P_s = 1 - e^{-\mu T_{\text{slot}}}. \quad (4)$$

From this, the probability that j users abandon the system in the n^{th} time slot can be written as follows:

$$P(U_n = j) = \binom{n}{j} P_s^j (1 - P_s)^{n-j}. \quad (5)$$

Now, an approximation to simplify the mathematical model is presented, where we assume that the time slot duration is sufficiently small compared to the average interarrival time such that in a given time slot, one or no arrival occurs, but the probability that two or more arrivals happen in the same time slot is almost zero, as in [32]. Building from this, we can express the arrival probability per time slot as follows:

$$P\{N(t - T_{\text{slot}}, t) = 1\} = P_a = (\lambda T_{\text{slot}}) e^{-(\lambda T_{\text{slot}})}. \quad (6)$$

The same assumptions are made for the average service time similar to [33], i.e., the probability that two or more users leave the system in the same time slot when $T_{\text{slot}} \ll (1/\mu)$ is very low. Hence, the departure probability per time slot is described as follows:

$$P_s^{(n)} = P(U_n = 1) = n P_s (1 - P_s)^{(n-1)}. \quad (7)$$

We focus our study on the GSM-based systems, such as GPRS or EDGE, where a TDMA protocol is used for voice and packet data transmissions. In these systems, the frame with duration of 120 milliseconds is divided into eight time slots of approximately 15 milliseconds each. We consider M time slots for packet data transmission for the secondary network. It is important to note that we use the exponential distribution assumption only to calculate the appropriate values of λ and μ to guarantee an adequate blocking probability. However, the proposed mathematical model is not restricted to an exponential distribution. In fact, it considers a geometrical distribution after discretizing the continuous exponential process. As such, a heavy tail distribution can also be discretized into a geometrical distribution in order to calculate the system variables for other types of traffic different from voice services. Note that the Markov chains described in Section 4 only require the values of P_a and P_s .

FIGURE 1: Average cluster formation time.

and no exponential process is present in these chains. Building on this, we believe that the proposed method is general for any continuous distribution on the arrival and departure of the primary users. Figure 1 presents the average cluster formation time for different values of P_a and P_s . It can be seen that as the arrival (departure) probability increases (decreases), there are more users in the primary system increasing the average cluster formation time, and for arrival/departure processes different from the exponential one, a match between the parameters of such processes (λ and μ in case of the exponential distribution) to the values of P_a and P_s has to be found.

2.3. Cognitive Radio Network. Based on the operation of the secondary network, described above, any transmission of the control packet in the cluster formation phase or in the steady state has to be done after scanning the channel for any primary node transmission. Specifically, nodes in attempting a transmission, first listen to the channel, scanning any activity by means of the received power. If the received power is sufficiently high, the nodes infer that a primary node is active in that slot. Otherwise, the nodes infer that the slot is empty. This procedure is repeated at the beginning of each time slot. It is important to mention that, when a secondary node finds the time slot occupied, it stops listening to the channel for the rest of the time slot in order to save energy.

3. PUE Cybernetic Attack

There are many cyberattacks in the IoT systems, including WSNs with cognitive radio capabilities. In [34], the authors identify vulnerabilities and categorize into three classes:

(1) Attacks on spectrum sensing

- (i) *Distortion of Spectrum Availability.* In this case, infected nodes can broadcast false information regarding the availability of resources, effectively preventing access to idle channels
- (ii) *Primary User Emulation (PUE) Attacks.* In this case, infected nodes behave as a PU, while SUs only detect the transmission of a legal PU with no authentication process

(2) Attacks on the channel negotiation process

- (i) *Backoff Manipulation Attack (BMA)*. In this case, infected nodes choose smaller values of backoff periods in order to gain preference access to the channels
- (ii) *Multireservation Attacks (MRA)*. In this case, infected CR nodes make multiple channel reservations to gain access to the available resources, while regular nodes only place single reservations

(3) Denial-of-service (DoS) attacks

- (i) *Control Channel Saturation*. In this case, infected nodes transmit diverse control packets to pass as legal transmissions, effectively restricting access to legal users since their control packets cannot be successfully received
- (ii) *Control Channel Jamming*. In this case, infected nodes jam the control channels to avoid successful negotiations for legal users

In all these cases, the secondary network is affected in two major ways: their reports cannot be efficiently conveyed to the base station and the energy consumption is increased since SUs continually look for empty spaces for transmission opportunities or many packet collisions occur in the control channel which entails transmission, reception, and signal processing tasks. In this work, we consider a PUE attack since it is a type of attack that does not require great technical abilities from the part of the attacker as we consider a cellular system as a primary system. Indeed, the operation of cellular systems is well known. Furthermore, making use of cellular equipment is straightforward. As such, it can be performed without the need for specialized equipment and it could be considered as an attack that can occur in any network since the cellular network is not required to authenticate such transmissions.

In the majority of attacks, the systems deplete their energy and their reporting capabilities are seriously reduced. When the WSN is deployed for monitoring applications, such as commerce, public spaces, or home surveillance, the impact of such attacks is mainly economic and personal security. However, these PUE attacks in SHM applications carry a much heavier burden since the network fails to inform about possible structural damage in buildings where dozens of people habit or work, putting those lives in grave danger.

Building from this, we consider a PUE attack with the following characteristics: a malicious node or nodes emulate primary users transmissions causing secondary nodes (nodes form the WSN) to account for the primary channels as busy, effectively preventing any transmission in such channels. In order to reduce the detection of the attack, malicious nodes only transmit in a time slot basis with probability P_{attack} . Hence, the probability of having consecutive unusable slots decreases with time. Since nodes are grouped inside the building, we assume that all secondary nodes are affected by the transmission of the malicious nodes.

In the following sections, we provide a mathematical model that captures the system operation under such PUE attacks. Based on the performance of the system, we propose an attack detection mechanism.

4. Mathematical Analysis

A main assumption of this work is that voice channels of the primary system are randomly assigned. As such, when i PUs are active, all channels have the same probability $P_{oc}(i) = i/S$ to be occupied. In low traffic conditions, this assumption may not hold when the channels are sequentially assigned to incoming PUs.

For the secondary system, in the cluster formation phase, multiple packet transmissions in idle time slots generate collisions that prevent successful data decoding. As such, two or more transmissions in the same slot require the retransmission of the packets involved in such collision. Building on this, the success transmission probability can be calculated as follows:

$$P_{\text{suc}}(k) = \binom{k}{1} \tau (1 - \tau)^{k-1} = k\tau(1 - \tau)^{k-1}, \quad (8)$$

where τ is the transmission probability per node in each time slot.

As mentioned above, we focus on a PUE attack. In particular, when a malicious node emulates a primary user transmission in a given time slot with probability P_{attack} , all nodes in the system assume that the channel is busy and does not transmit.

4.1. Cluster Formation Phase. This phase is initiated when sensor nodes detect an abnormal vibration value as a result of an earthquake, strong winds, or load balancing forces in the structure among other phenomena. At this point, all the nodes in each independent sensor network attempt a control packet transmission to the sink node in order to become either a cluster head or cluster member. In more detail, secondary nodes scan the activity in each channel, and if no PUs are detected or no attack is present, they transmit their control packet with probability τ and defer their transmission with probability $1 - \tau$. When all nodes have successfully transmitted their packet, we assume that this phase is finished. At this point, all nodes are aware of the cluster they are assigned to and the roles inside it. In this regard, the first N_{CH} nodes that successfully transmit their packet become cluster heads, while the rest of the nodes become a cluster member of the nearest CH. In [35], we evaluated the performance of such CH selection (first come-first chosen) to other clustering schemes such as those using *intelligent algorithms* like k -means and fuzzy C -means. Although the intelligent approaches, in general, render better results (CHs are better placed in the system), they also convey higher cluster formation times and energy consumption due to the intrinsic computing tasks required to operate. Additionally, for medium-low sensor networks (less than 100 nodes), the performance of the proposed first come-first chosen approach is

FIGURE 2: Markov chain in the CF phase with CR capabilities.

very similar to the intelligent approaches. For dense sensor networks (more than 100 nodes), the gain of using such intelligent approaches is more important.

We propose a discrete time Markov chain to model such a system as shown in Figure 2, where i is the number of ongoing voice calls in the primary system, and k is the number of secondary nodes that still have not successfully transmitted their control packet.

Building on this, the valid state space of the Markov chain is $(0 \leq k \leq N)$ and $(0 \leq i \leq S)$. The transition probabilities are now described in detail.

- (i) P_1 is the probability that a new voice call is generated in the PS and no voice user leaves the system and a successful control packet is transmitted in the secondary system after the time slot was detected as idle and no attack is present. Then,

$$P_1 = P_a P_{\text{suc}}(k)(1 - P_{\text{OC}}(i))(1 - P_{\text{attack}}). \quad (9)$$

- (ii) P_2 is the probability that no new voice calls are generated in the PS and no voice user leaves the system and a successful control packet is transmitted in the secondary system after the time slot was detected as idle and no attack is present. Then,

$$P_2 = (1 - P_a) \left(1 - P_S^{(i)}\right) (1 - P_{\text{OC}}(i)) P_{\text{suc}}(k) (1 - P_{\text{attack}}). \quad (10)$$

- (iii) P_3 is the probability that no new voice calls are generated in the PS and a single-voice user leaves the system and a successful control packet is transmitted in the secondary system after the time slot was detected as idle and no attack is present. Then,

$$P_3 = (1 - P_a) P_S^{(i)} P_{\text{suc}}(k) (1 - P_{\text{OC}}(i)) (1 - P_{\text{attack}}). \quad (11)$$

- (iv) P_4 is the probability that no new voice calls are generated in the PS and no voice user leaves the system and there are no successful control packet transmissions in the secondary system either because a

collision occurred or there are no packet transmissions or the slot was occupied by a PU or a malicious node is present. Then,

$$P_4 = [P_{\text{OC}}(i) + \{(1 - P_{\text{suc}}(k))(1 - P_{\text{OC}}(i))\} + P_{\text{attack}}](1 - P_a) \left(1 - P_S^{(i)}\right). \quad (12)$$

- (v) P_5 is the probability that no new voice calls are generated in the PS and a single-voice user leaves the system and there are no successful control packet transmissions in the secondary system either because a collision occurred or there are no packet transmissions or the slot was occupied by a PU or a malicious node is present. Then,

$$P_5 = [P_{\text{OC}}(i) + \{(1 - P_{\text{suc}}(k))(1 - P_{\text{OC}}(i))\} + P_{\text{attack}}] P_S^{(i)}. \quad (13)$$

- (vi) P_6 is the probability that a new voice call is generated in the PS and no voice user leaves the system and there are no successful control packet transmissions in the secondary system either because a collision occurred or there are no packet transmissions or the slot was occupied by a PU or a malicious node is present. Then,

$$P_6 = [P_{\text{OC}}(i) + \{(1 - P_{\text{suc}}(k))(1 - P_{\text{OC}}(i))\} + P_{\text{attack}}] P_a, \quad (14)$$

where P_a and $P_S^{(i)}$ are described by (6) and (7), respectively.

The average absorption time beginning in state (i, N) , for $0 \leq i \leq S$, until the Markov chain reaches the absorbent state $(j, 0)$, for $0 \leq j \leq S$, corresponds to the average cluster formation delay and it is numerically evaluated.

Similarly, the average energy consumption in the cluster formation phase is numerically evaluated from the initial state (i, N) , for $0 \leq i \leq S$, until the Markov Chain reaches the absorbent state $(j, 0)$, for $0 \leq j \leq S$. In each state, secondary nodes scan any PU activity in the time slot before attempting a transmission. This is done by listening for a small time at the beginning of the slot. During this small time interval, if a PU is detected, secondary nodes go to the sleep mode and each secondary node consumes $E_{\text{Rx}}^{\text{Det}}$ which corresponds to a small fraction of the energy consumed when a packet is received. Indeed, the reception and activity detection operations are similar except that activity detection is made for a small amount of time. Otherwise, they attempt a control packet transmission. As such, when there are k secondary nodes still active in the cluster formation phase and i PUs with an ongoing call, the energy consumption depends on the following:

- (1) *Slot Occupied*. When the time slot is being used by a primary user or when a PUE attack is in progress, then nodes in the secondary nodes differ their

transmissions and the energy consumption in the time slot is given as follows:

$$EC_{OC}(k) = kE_{Rx}^{Det}. \quad (15)$$

(2) *Slot Available*. When the time slot is not being used by a PU or there is not a PUE attack in progress, then the power consumption in this case is as follows:

(i) When a time slot is idle and there is not a PUE attack in progress, but the transmission is unsuccessful due to packet collisions or no packet transmissions, the energy consumption is given as follows:

$$EC_{fail}(k) = \sum_{j=0, j \neq 1}^k [jE_{tx}^{CF} + (k-j)E_{rx}^{CF}], \quad (16)$$

due to j transmissions and the energy consumption due to the $k-j$ packet receptions by the rest of the nodes.

(ii) When a successful transmission occurs because the channel is not being used by a PU and there is not a PUE attack in progress, then the energy consumption in that time slot is as follows:

$$EC_{succ}(k) = [E_{tx}^{CF} + (k-1)E_{rx}^{CF}], \quad (17)$$

due to the single transmission and $k-1$ packet receptions.

Building on this, when k secondary nodes are active in the cluster formation phase, average energy consumption is calculated by means of numerically solving the Markov chain with the following rewards: in case of a nonidle slot, $r_{OC} = kE_{Rx}^{Det}$; in case of a successful transmission, $r_{succ} = EC_{succ}(k)$; in case of collisions or no transmissions in the secondary system, $r_{fail} = EC_{fail}(k)$.

4.2. Steady-State Phase. It is assumed that all sensor nodes store the seismic event in a buffer from the beginning to the end of the event. Note that data packets cannot be transmitted during the CF phase. As such, data transmission begins at the steady state, when clusters are already formed. At this point, CHs know the ID of their cluster members and an orderly, collision-free, TDMA-based schedule is conveyed in each cluster. Each node in the cluster waits for the transmission of the previous node in the schedule which can take a number of slots in case that a PU is active or a cyberattack is present. Packet transmissions are finished after all nodes have transmitted their data packets regarding the particular event, i.e., after the N_{eq} packets that recorded the activity inside the structure during the complete event.

Figure 3 presents the DTMC that models the activity in the steady-state phase when i voice channels are used in the primary system and there are x ($0 \leq x \leq N_{eq}$) packets waiting for a transmission opportunity.

FIGURE 3: Markov chain for the SS phase with CR capabilities.

(i) P_1 is the probability that no voice user enters into the primary system and a voice user leaves the system and a secondary node detects an idle time slot and no cyberattack is present. Then,

$$P_1 = (1 - P_a)P_S^{(i)}(1 - P_{OC}(i))(1 - P_{attack}). \quad (18)$$

(ii) P_2 is the probability that no voice user enters into the primary system and no voice users leave the system and a secondary node detects an idle time slot and no cyberattack is present. Then,

$$P_2 = (1 - P_a)(1 - P_S^{(i)})(1 - P_{OC}(i))(1 - P_{attack}). \quad (19)$$

(iii) P_3 is the probability that a single-voice user enters into the primary system and no voice users leave the system and a secondary node detects an idle time slot and no cyberattack is present. Then,

$$P_3 = P_a(1 - P_S^{(i)})(1 - P_{OC}(i))(1 - P_{attack}). \quad (20)$$

(iv) P_4 is the probability that no voice user enters into the primary system and no voice users leave the system and a secondary node detects the time slot as occupied or a cyberattack is present. Then,

$$P_4 = (1 - P_a)(1 - P_S^{(i)})[P_{OC}(i) + P_{attack}]. \quad (21)$$

(v) P_5 is the probability that no voice user enters into the primary system and a single-voice user leaves the system and a secondary node detects the time slot as occupied or a cyberattack is present. Then,

$$P_5 = (1 - P_a)P_S^{(i)}[P_{OC}(i) + P_{attack}]. \quad (22)$$

(vi) P_6 is the probability that a single-voice user enters into the primary system and no voice users leave

the system and a secondary node detects the time slot as occupied or a cyberattack is present. Then,

$$P_6 = P_a \left(1 - P_s^{(i)}\right) [P_{OC}(i) + P_{attack}]. \quad (23)$$

To calculate the average reporting time and average energy consumption in the steady-state phase, consider the following details: (a) the sensor network has N nodes, (b) ten percent of those nodes are selected as cluster heads, and then $N_{CH} = 0.1 N$, and (c) consequently, $N - N_{CH}$ nodes are cluster members. From this, we consider the case where CHs are evenly distributed in the monitored area. Hence, the average cluster member per cluster is $N_{CM} = (N/N_{CH})$. Since we assign the CH role to the first N_{CH} nodes that successfully transmit their control packet, this even CH distribution is not always achieved. However, this is a common issue among clustering algorithms such as LEACH [26]. Furthermore, in [36] we show that for $N \leq 100$, performance of the proposed *first arrive-first chosen* approach is similar to LEACH. In order to provide an event CH distribution and avoid long transmissions inside the clusters, require more computing operations that consume more energy and time to form the clusters. We consider this issue to fall outside the scope of this work, and we leave this research area open for a future work.

The previous assumptions entail an average frame size per cluster of the following:

$$T_{frame} = N_{CM} T_{slot}. \quad (24)$$

If the event has a duration time of T_{eq} seconds, then the average number of frames required to convey the information of such event is calculated as follows:

$$n_f = \frac{T_{eq}}{T_{frame}}, \quad (25)$$

and the number of total packets to report the event is $N_{eq} = N * n_f$. From this, the average time slots required by all nodes to transmit their data, D_{SS} , can be calculated as the absorption time of the previously described Markov chain beginning at state (i, N_{eq}) , for $0 \leq i \leq S$ until the state $(i, 0)$ is reached.

Similarly, a reward Markov chain is proposed to evaluate the average energy consumption in this steady state by considering the following rewards: (a) $r_{tx} = E_{Tx}^{SS} + E_{Rx}^{SS}$ energy units when a successful transmission occurs and it considers both the data packet transmission and reception in case of an idle or nonattacked slot, (b) $r_{OC} = E_{Rx}^{Det}$ energy units for an occupied or attacked slot, and (c) E_{Tx}^{Sink} energy units at the end of each frame for the aggregated data form the CH to the sink.

5. Cyberattack Detection Procedure

We now propose a procedure to detect PUE cyberattacks. Our hypothesis is that any PUE attack would invariably

increment both reporting time and energy consumption in the network. However, for low attack probabilities, such increment would be rather low and hard to detect, while for high attack probabilities, the average reporting time would be more visible and easy to detect. Building from this, we propose the following detection mechanism:

- (i) Quantify the number of times that the reporting time was higher than the mean reporting time plus the variance, for a given value of P_a and P_s . These suspiciously large reporting times can be a result of the intrinsic random nature of primary users or it can be the result of a cyberattack. As such, the probability that a reporting time is suspicious is called $P_{sus} = P_f/n$, where P_f is the number of times that the reporting time was higher than the mean plus the standard deviation and n the number of reporting events
- (ii) If P_{sus} is higher than a certain threshold, the system raises a flag that an attack is probably underway. Conversely, if P_{sus} is lower than the threshold, the unusually high reporting time may be attributed to the randomness of the system's users

We then evaluate the cyberattack detection probability for different values of the attack probability and the threshold to see the effectiveness of the proposed method.

Note that in order to have an accurate estimate of P_{sus} , a high number of vibration reports have to be done. Since buildings and high structures experience a continuous number of vibrations due to winds, low-intensity earthquakes, and other physical phenomena, we believe that in a short period, the SHM system would have attained this high number of reports to efficiently detect an ongoing cyberattack. In the numerical section, we evaluate this effectiveness.

6. Numerical Results

In this section, numerical results are presented to quantitatively evaluate the performance of the CR network for different traffic loads. We study both the cluster formation phase and steady state in terms of average packet delay and average energy consumption. Based on our previous works [23, 24], we set that the value of $\tau = 0.1$ gives the best performance results.

In Figures 4–6, we show the average CF time for different numbers of nodes in the network and offered traffic load of 3, 30, and 60 Erlangs, respectively, and different attack intensity, P_{attack} , considering a transmission probability of $\tau = 0.1$. As expected, when P_{attack} and the offered traffic increase, also the cluster formation time increases. This is because the probability of finding empty slots is low when primary channels are more likely to be used by PUs or a PUE attack is in progress. In Table 1, we present the average reporting time for the Mexico City seism, i.e., the average time that the system requires to send all the gathered information during the seism event to the sink node. Again, as the traffic load increases or the intensity of the attack increases, the nodes in the secondary network finds

FIGURE 4: CF time with an offered traffic of 3 Erlangs.

FIGURE 5: CF time with an offered traffic of 30 Erlangs.

FIGURE 6: CF time with an offered traffic of 60 Erlangs.

increasingly hard transmission opportunities, increasing the average reporting delay.

As a relevant result, we can see that even in the worst possible conditions, when traffic load is extremely high in the cellular network (which is expected after or during a seism event) and for a very intensive attack ($P_{\text{attack}} = 0.9$), the WSN is still capable of conveying the complete information regarding the earthquake to the sink node, although this is done in a much higher time than in normal conditions (traffic load of 3 Erlangs that entails a blocking probability of 0.1 and no attack). These results are very encouraging for the use of WSNs for the SHM in IoT applications.

6.1. Attack Detection Mechanism. From the figures above, we propose an attack detection mechanism as follows. When the system is not attacked, the average cluster formation

TABLE 1: Reporting time for Mexico City seism.

	3 Erlangs	30 Erlangs	60 Erlangs
$P_{\text{attack}} = 0$	17,051.89 slots 4.2 min	209,851.3 slots 52.4 min	439,370.25 slots 109.8 min
$P_{\text{attack}} = 0.1$	17,504.89 slots 4.3762 min	213,178 slots 53.2945 min	565,627 slots 141.4067 min
$P_{\text{attack}} = 0.2$	18,007 slots 4.5018 min	235,125 slots 58.7812 min	670,791 slots 167.6977 min
$P_{\text{attack}} = 0.3$	18,816 slots 4.7040 min	381,490 slots 95.3725 min	780,456 slots 195.1140 min
$P_{\text{attack}} = 0.4$	19,659 slots 4.9147 min	432,720 slots 108.18 min	804,637 slots 201.1593 min
$P_{\text{attack}} = 0.5$	21,073 slots 5.2682 min	493,570 slots 123.3925 min	945,980 slots 236.4950 min
$P_{\text{attack}} = 0.6$	23,042 slots 5.7605 min	527,950 slots 131.9875 min	1,028,486 slots 257.1215 min
$P_{\text{attack}} = 0.7$	26,415 slots 6.6037 min	539,920 slots 134.98 min	1,065,963 slots 266.4907 min
$P_{\text{attack}} = 0.8$	33,635 slots 8.4087 min	664,850 slots 166.2125 min	1,246,940 slots 311.735 min
$P_{\text{attack}} = 0.9$	52,361 slots 13.0902 min	982,581 slots 245.6453 min	1,927,340 slots 481.8350 min

time accounts for the required time to form the clusters including possible collisions and empty slots. It is clear then, that as the attack probability increases, nodes in the system detect more slots as occupied and hence cannot be used. This increases the cluster formation time to abnormal values. From this perspective, it is possible to detect a possible attack observing the increase in cluster formation time. For instance, consider the case where an attacker selects an attack probability of 0.4, when $N = 20$ and traffic load in the primary system is 60 Erlangs. In this case, we can see a 225% increase in the average cluster formation delay (from 2313.15 time slots when $P_{\text{attack}} = 0$ to 7524.7 time slots when $P_{\text{attack}} = 0.4$). Clearly, there is an important increase which can be detected relatively easy.

This detection method allows the network administrator to detect a possible cyberattack in order to take the appropriate counterattack actions. For instance, the electromagnetic source of the attack can be traced or the system can migrate to a different frequency of the cellular system.

The attack can also be detected by the performance of the system in the steady state as presented in Table 1. We can see that if the attack occurs with $P_{\text{attack}} = 0.5$ and 60 Erlangs in the primary network, the system suffers a 115% increase in the average seism reporting time (from 109.8 minutes when $P_{\text{attack}} = 0$ to 236.4950 minutes when $P_{\text{attack}} = 0.5$) which is a considerable increment and easily detectable.

It is important to note that if the attacker wants to remain undetected, a low P_{attack} can be used in such a way as to slightly increase cluster formation time. In such conditions, the attack would be harder to be detected. For instance, if the attacker uses $P_{\text{attack}} = 0.1$ for a system with a traffic load of 30 Erlangs in the primary network and 10 nodes, then the increase in cluster formation time would only be 66% (from 314.827 time slots when $P_{\text{attack}} = 0$ to 523.01 time slots

FIGURE 7: Histograms for average reporting times under stealthy attack ($P_{\text{attack}} < 0.4$). FIGURE 8: Histograms for average reporting times under mild attack ($0.4 \leq P_{\text{attack}} \leq 0.7$).

FIGURE 9: Histograms for average reporting times under strong attack ($P_{\text{attack}} > 0.7$).

when $P_{\text{attack}} = 0.1$). This increase would be much harder to detect. However, the impact of the attack is also less important, since nodes can still send the gathered information in a reasonable amount of time and the energy consumption is barely increased. However, even if the attacker chooses a low-intensity attack, the impact on the average packet delay is still nonnegligible. From this, we conclude that the mathematical tool developed in this work can be used as an attack detection mechanism that does not require constant measurements of diverse parameters in the system which could be time consuming. Building on this, we obtained the histograms of the average reporting delay under different attack conditions, ranging from a stealthy attack ($P_{\text{attack}} < 0.4$) to a mild attack ($0.4 \leq P_{\text{attack}} \leq 0.7$) to a strong attack ($P_{\text{attack}} > 0.7$) in Figures 7–9, respectively. In these results, the figures of the left show an augmented part of the reporting delay higher than the mean plus the standard variation, i.e., it corresponds to P_f described in Section 5. The figures on the right correspond to the complete histogram of the reporting times, clearly indicating the mean, with the red vertical line, and the mean plus the standard deviation, with the vertical blue line. Also, we present the histogram when no attack is present ($P_{\text{attack}} = 0$). From these results, it is clear

that even a stealthy attack has a big impact on the distribution of the reporting times, increasing the number of times that the reporting time is higher than the mean plus the standard deviation, actively increasing the suspicious probability.

From these results, we can establish an adequate threshold to detect an ongoing attack. Specifically, the suspicious probability, P_{sus} , increases to 0.99 whenever an attack is underway, while it is lower than 0.3 when no attack is present due to the inherent randomness in the system. As such, compared to the results presented in [22], where detection probabilities are higher than 93.4%, using our methodology described in Section 5, we achieve a detection probability of 0.99 as seen in Figure 10. Indeed, the probability to detect an ongoing attack is the probability that the suspicious probability is higher than 0.3.

Also, it is important to remark that such PUE attacks not only prevent the appropriate data reporting to occur in a timely manner but the most important effect of the attack is the energy depletion that it causes in the system. Note that average energy consumption is greatly increased as the attack probability increases. This would consume the energy much faster leading the network to be disabled in a short amount of time, preventing further reporting epochs.

FIGURE 10: Suspicious probability P_{sus}^* .

7. Conclusions

In this work, we study, analyze, mathematically model, and evaluate the performance of a SHM system-based event-driven WSNs when a PUE attack occurs. The proposed analysis allows to capture the effect of such attack for different conditions of the system. From the numerical results, we propose an attack detection method based on the energy consumption and cluster formation and reporting delay caused by such attacks. When the attack happens with a high intensity (high probability of attack), the network administrator can detect it much easier than when the attacker chooses a low-intensity attack. A low-intensity attack allows the attacker to remain undetected longer times but the attack would have less effect on the performance of the system.

In future works, we are considering to expand the mathematical model to include other types of cyberattacks, for instance, a local PUE attack, where only a certain number of nodes inside the attack region are affected instead of the complete system. This type of attack is typical in multihop networks and new communication protocols and cluster head selection schemes have to be developed as well as a new mathematical model has to be considered in such scenarios. Also, the case where a malicious node or a hacked node transmits with a higher probability than other neighbor nodes, causing many collisions in the cluster formation phase. It is important to model these types of attacks in order to have a mathematical tool to detect a higher energy consumption or packet delay, leading to the suspicion that an attack is in progress.

Data Availability

Data supporting the results in a published article are available at our databases including, where applicable, hyperlinks to publicly archived datasets analyzed or generated during the study.

Conflicts of Interest

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

References

- [1] S. Dhanoriya and M. Pandey, "A survey on wireless sensor networks: faults, misbehaviour and protection against them," in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, Delhi, India, 2017.
- [2] G. Pradnya and M. Anjali, "A survey of architecture and node deployment in wireless sensor network," in *2008 First International Conference on the Applications of Digital Information and Web Technologies (ICADIWT)*, pp. 426–430, Ostrava, Czech Republic, August 2008.
- [3] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.
- [4] T. Arampatzis, J. Lygeros, and S. Manesis, "A survey of applications of wireless sensors and wireless sensor networks," in *Proceedings of the 2005 IEEE International Symposium on, Mediterranean Conference on Control and Automation Intelligent Control, 2005*, pp. 719–724, Limassol, Cyprus, 2005.
- [5] H. Shu and Q. Liang, "Fundamental performance analysis of event detection in wireless sensor networks," in *IEEE Wireless Communications and Networking Conference, 2006. WCNC 2006*, pp. 2187–2192, Las Vegas, NV, USA, 2006.
- [6] V. Ramani and S. K. Sharma, "Cognitive radios: a survey on spectrum sensing, security and spectrum handoff," *China Communications*, vol. 14, no. 11, pp. 185–208, 2017.
- [7] J. Xue, Z. Feng, and K. Chen, "Beijing spectrum survey for cognitive radio applications," in *2013 IEEE 78th Vehicular Technology Conference (VTC Fall)*, Las Vegas, NV, USA, 2013.
- [8] O. B. Akan, O. B. Karli, and O. Ergul, "Cognitive radio sensor networks," *IEEE Network*, vol. 23, no. 4, pp. 34–40, 2009.
- [9] B. Mercier, V. Fodor, R. Thobaben et al., *Sensor Networks for Cognitive Radio: Theory and System Design*, ICT MobileSummit, 2008.
- [10] X. Hu, B. Wang, and H. Ji, "A wireless sensor network-based structural health monitoring system for highway bridges," *Computer, Aided Civil and Infrastructure Engineering*, vol. 28, no. 3, pp. 193–209, 2013.
- [11] X. Liu, J. Cao, W.-Z. Song, P. Guo, and Z. He, "Distributed sensing for high-quality structural health monitoring using WSNs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 3, pp. 738–747, 2015.
- [12] M. Zakirul, A. Bhuiyan, G. Wang, J. Cao, and J. Wu, "Energy and bandwidth-efficient wireless sensor networks for monitoring high-frequency events," in *2013 IEEE International Conference on Sensing, Communications and Networking (SECON)*, pp. 194–202, New Orleans, LA, USA, 2013.
- [13] S. Singh, W. K. G. Seah, and B. Ng, "Cluster-centric medium access control for WSNs in structural health monitoring," in *2015 13th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, pp. 275–282, Mumbai, India, 2015.
- [14] T. Torfs, T. Sterken, S. Brebels et al., "Low power wireless sensor network for building monitoring," *IEEE Sensors Journal*, vol. 13, no. 3, pp. 909–915, 2013.
- [15] M. Z. A. Bhuiyan, G. Wang, J. Cao, and J. Wu, "Deploying wireless sensor networks with fault-tolerance for structural health monitoring," *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 382–395, 2015.

- [16] M. Z. A. Bhuiyan, G. Wang, J. Wu, J. Cao, X. Liu, and T. Wang, "Dependable structural health monitoring using wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 14, no. 4, pp. 363–376, 2017.
- [17] Z. Zou, Y. Bao, F. Deng, and H. Li, "An approach of reliable data transmission with random redundancy for wireless sensors in structural health monitoring," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 809–818, 2015.
- [18] Q. Zheng, X. Fei, T. Tang et al., "A hybrid dynamic traffic-adaptive MAC protocol for wireless sensor networks," in *15th International Conference on Advanced Communication Technology, (ICACT) 2013*, pp. 574–578, PyeongChang, South Korea, 2013.
- [19] J. P. Lynch and K. J. Loh, "A summary review of wireless sensors and sensor networks for structural health monitoring," *The Shock and Vibration Digest*, vol. 38, no. 2, pp. 91–128, 2006.
- [20] J. Gope, P. Dutta, S. Bhadra et al., "Analytical study of primary user emulation attack detection techniques in cognitive radio Adhoc network," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 392–395, New York, NY, USA, 2017.
- [21] M. Riecker, D. Thies, and M. Hollick, "Measuring the impact of denial-of-service attacks on wireless sensor networks," in *39th Annual IEEE Conference on Local Computer Networks*, pp. 296–304, Edmonton, Canada, 2014.
- [22] R. H. M. Zargar and M. H. Y. Moghaddam, "SIP flooding attacks detection and prevention using Shannon, Renyi and Tsallis entropy," *International Journal of Hybrid Information Technology*, vol. 7, no. 5, pp. 257–272, 2014.
- [23] H. A. A. Garrido, M. E. Rivero-Angeles, and I. Y. O. Flores, "Performance analysis of a wireless sensor network for seism reporting in an overlay cognitive radio system," in *2016 30th international conference on advanced information networking and applications workshops (WAINA)*, pp. 565–570, Crans-Montana, Switzerland, 2016.
- [24] H. A. A. Garrido, M. E. Rivero-Angeles, I. Y. O. Flores, E. A. Anaya, and F. J. Rivero-Angeles, "Performance analysis of a wireless sensor network with cognitive radio capabilities for structural health monitoring," *Journal of Ad Hoc and Sensor Wireless Networks*, vol. 39, no. 1-4, pp. 97–122, 2017.
- [25] H. A. A. Garrido, M. E. Rivero-Angeles, E. A. Anaya, F. A. Cruz-Perez, S. L. Castellanos-Lopez, and G. Hernandez-Valdez, "Performance analysis of a wireless sensor network with cognitive radio capabilities in structural health monitoring applications: a discrete model," *International Journal of Distributed Sensor Networks*, vol. 14, no. 5, 2018.
- [26] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, 2002.
- [27] G. Hou, K. W. Tang, and E. Noel, "Implementation and analysis of the LEACH protocol on the TinyOS platform," in *2013 International Conference on ICT Convergence (ICTC)*, pp. 918–923, Jeju, South Korea, 2013.
- [28] J. Galtier, "Analysis of the slotted non-persistent CSMA protocol with Poissonian packet size using a semi-Markov graph representation," in *2006 International Conference on Transparent Optical Networks*, pp. 258–262, Nottingham, England, 2006.
- [29] R. Rom and M. Sidi, *Multiple Access Protocols: Performance and Analysis*, Springer, 1989.
- [30] N. Bouabdallah, M. E. Rivero-Angeles, and B. Sericola, "Continuous monitoring using event-driven reporting for cluster-based wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3460–3479, 2009.
- [31] D. Niyato and E. Hossain, "A novel analytical framework for integrated cross-layer study of call-level and packet-level QoS in wireless mobile multimedia networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 3, pp. 322–335, 2007.
- [32] A. Y. Veretennikov, "On mixing rate and convergence to stationary regime in discrete time Erlang problem," *Automation and Remote Control*, vol. 70, no. 12, pp. 1992–2002, 2009.
- [33] Q. Bi, S. Vitebsky, Y. Yang, Y. Yuan, and Q. Zhang, "Performance and capacity of cellular OFDMA systems with voice-over-IP traffic," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 6, pp. 3641–3652, 2008.
- [34] Y. Zhang and L. Lazos, "Vulnerabilities of cognitive radio MAC protocols and countermeasures," *IEEE Network*, vol. 27, no. 3, pp. 40–45, 2013.
- [35] E. R. Montiel, M. E. Rivero-Angeles, G. Rubino, H. Molina-Lozano, R. Menchaca-Mendez, and R. M. Mendez, "Performance analysis of cluster formation in wireless sensor networks," *Sensors*, vol. 17, no. 12, article 2902, 2017.
- [36] E. R. Montiel, M. E. Rivero-Angeles, I. V. Jimenez, and H. M. Lozano, "Impact of the error sensing probability in wide coverage areas of clustered-based wireless sensor networks," *Revista Facultad de Ingeniería Universidad de Antioquia*, no. 79, pp. 63–74, 2016.