computers

MDPI

Review

Cognitive Radio for Smart Grid with Security Considerations

Khaled Shuaib [1,*], Ezedin Barka [1], Nedaa Al Hussien [1], Mohammed Abdel-Hafez [2] and Mahmoud Alahmad [3]

[1] College of Information Technology, United Arab Emirates University, Al Ain, P.O. Box 15551, UAE; ebarka@uaeu.ac.ae (E.B.); nedaa_yousef@uaeu.ac.ae (N.A.H.)
[2] College of Engineering, United Arab Emirates University, Al Ain, P.O. Box 15551, UAE; mhafez@uaeu.ac.ae
[3] College of Engineering, University of Nebraska-Lincoln, Omaha, NE 68182, USA; malahmad2@unl.edu
* Correspondence: k.shuaib@uaeu.ac.ae; Tel.: +971-3-7135551

Academic Editor: Thomas Strang
Received: 29 January 2016; Accepted: 25 April 2016; Published: 28 April 2016

Abstract: In this paper, we investigate how Cognitive Radio as a means of communication can be utilized to serve a smart grid deployment end to end, from a home area network to power generation. We show how Cognitive Radio can be mapped to integrate the possible different communication networks within a smart grid large scale deployment. In addition, various applications in smart grid are defined and discussed showing how Cognitive Radio can be used to fulfill their communication requirements. Moreover, information security issues pertained to the use of Cognitive Radio in a smart grid environment at different levels and layers are discussed and mitigation techniques are suggested. Finally, the well-known Role-Based Access Control (RBAC) is integrated with the Cognitive Radio part of a smart grid communication network to protect against unauthorized access to customer's data and to the network at large.

Keywords: cognitive radio; information security; smart grid; role-based access control

1. Introduction

The current electrical power grid is a centrally controlled network that is located over a large geographic area with an enormous number of systems and devices, starting from the power generation plant all the way to the customer side. This traditional power grid faces many challenges such as rising energy demand, aging infrastructure, reliability and security issues [1]. Moreover, there is an increasingly growing attention on integrating renewable energy resources with the existing fuel-based power generation for both economic and environmental concerns. This issue raises the need for the traditional power grid to cope with these challenges and evolve toward intelligence in power generation, transmission, distribution, and billing. This can be achieved by moving to the next-generation power grid, which is known as smart grid.

Smart grid is a two-way communication enabled power grid, in which electrical power generation is integrated with emerging technologies such as wireless communication, pervasive computing, and adaptive control to substantially improve the efficiency, reliability and sustainability. Significant benefits are achieved from adopting smart grid networks including: economic benefits (reducing generation and distribution cost, managing consumption and bill pricing, controlling grid failure and power outage), and environmental benefits (saving energy through demand response management, integrating renewable/distributed energy resources) [2].

Starting from power generation systems (traditional and/or renewable) through transmission/distribution systems to customers (industrial, commercial and/or residential), smart grid combines all these sub-networks within one intelligent network with bidirectional flow of electricity and information.

Smart meters, sensors, intelligent appliances, and electric vehicles are all connected to smart grid to provide real-time information that is critical for demand response control and grid management. Figure 1 depicts a simplified smart grid conceptual model paradigm as envisioned by NIST.

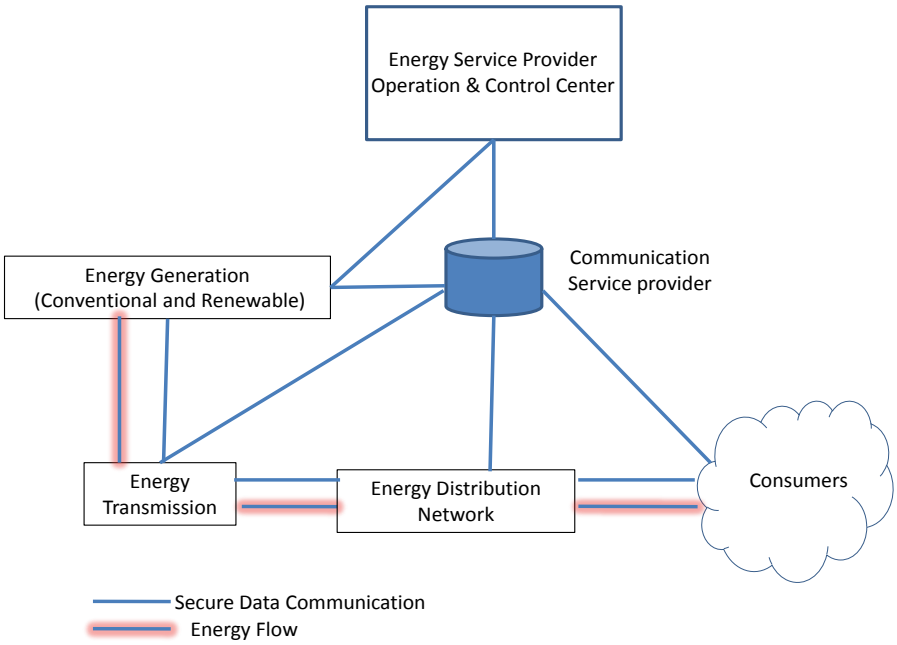

Figure 1. Smart Grid Conceptual Model.

One of the cornerstones of smart grid networks is establishing a reliable communication infrastructure that can accommodate current and future applications. The nature of some smart grid applications and services, where real-time information and critical monitoring and controlling data need to be exchanged with minimal delay, imposes stringent requirements on the communication infrastructure. Communication infrastructure in smart grid carries heterogeneous data and connects all elements, which are located over a large geographical area. Different communication technologies can be used in smart grid including power line communication (PLC), fiber optics, and wireless communication over both the licensed and unlicensed spectrum bands.

Using a certain communication technology depends on the type of data and the available resources. For example, fiber optics are used in communication within the core network that connects head offices and substations, providing high data rates and minimal latency required critical data communication. In distribution networks, technologies such as cellular, PLC and WiFi communication networks are commonly used to connect automation and control devices.

As smart grid networks evolve, more applications and services are introduced imposing an increasing demand for the RF spectrum in use to cover the large scale geographical area. This calls for a scalable communication infrastructure that can cope with the needed requirements while providing reliable services. However, the RF spectrum is a limited natural resource, which is characterized by static frequency allocation schemes. In static frequency allocation, frequency bands are assigned to licensed networks and users on long-term basis within a certain geographical area. Though measurements indicate that these bands are unused by the licensed users for significant periods of time, resulting in spectrum under-utilization [3,4].

There are many challenges related to the design of a communication infrastructure for smart grid which include:

Limited bandwidth: The amount of data acquired from smart meters and sensors has grown dramatically, from 10,780 Tbytes in 2010 to 75,200 Tbytes in 2015 [1]. This increases the burden on the existing communication infrastructure as more bandwidth is required for reliable communication.

Energy sources: Integrating distributed energy sources (e.g., solar and wind power) as part of traditional power generation is a unique characteristic of the smart grid. However, these sources have essential differences in price and availability. Therefore, balancing the usage of the different energy sources is very important for power grid stability, availability and operation cost.

Traffic variability: There is a vast amount of real-time data in a smart grid deployment which might vary rapidly during the day. Therefore, higher data rates and more reliable communication services are required during peak hours.

Interoperability: Different communication technologies are used as part of the communication infrastructure within smart grid for reliable data flow over the generation, transmission, distribution and customers' networks. One of the main challenges is to ensure interoperability between these different communication technologies.

Quality of service (QoS): Different categories of data have different QoS priorities in terms of transmission latency, reliability, bandwidth and security [1]. Information regarding the operational state of devices such as load, faults and power quality should flow over the communication infrastructure accurately with high priority. However, a lower priority can be assigned to traffic carrying periodic pricing data used to calculate the electric usage monthly bill.

Security: In smart grid, computer networks are used to monitor and control the power infrastructures. This exposes smart grid to certain attacks such as Denial of Service (DoS), data insertion/falsification, access and authorization violation [5].

In this work, we explore the utilization of Cognitive Radio (CR) as a technology to overcome some of the above challenges and discuss any introduced additional constraints or concerns. According to the FCC (Federal Communication Commission); "Cognitive radio is a system that senses its operational electromagnetic environment and can dynamically and autonomously adjust its radio operating parameters to modify system operation, such as maximize throughput, mitigate interference, facilitate interoperability, access secondary markets" [6]. As a promising technology, cognitive radio allows unlicensed (secondary) users to access the licensed spectrum opportunistically without causing harmful interferences to the licensed (primary) users, as shown in Figure 2.

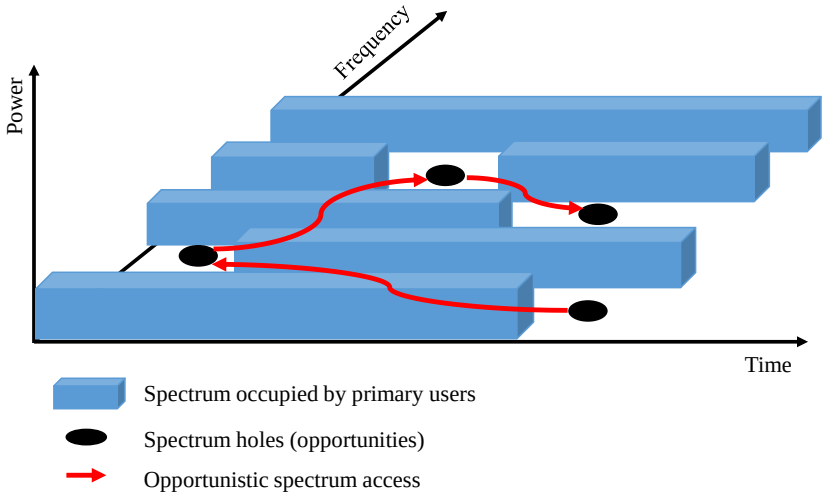

Figure 2. Opportunistic Spectrum Access in Cognitive Radio.

The utilization of cognitive radio for smart grid can take several directions depending on the location of the network and the type of needed services. For example, cognitive radio can be used as stand-alone radio to provide broadband access in areas where spectrum density is low and there is available spectrum holes (opportunities), such as rural areas. However, it can be used as a secondary link for sending non-critical data in areas where the spectrum is densely occupied, or as backup link in the case of emergency and network failure [7]. Although using CR communication in smart grid

networks is not unique as a strategy, its importance can be derived from several factors showing it to be an effective choice. For example, using CR allows for an integrated communication solution to be used across the large scale smart grid communication network while utilizing existing resources. Another advantage of using CR in smart grid is related to the possibility of providing different end to end QoS to different applications based on their needs. Pervasiveness is another feature providing the different users of smart grid with anytime, anywhere connectivity to fulfill their needs. Further motivations behind the use of CR in smart grid are outlined in the next section.

Our contribution in this paper is to investigate using cognitive radio as a communication technology in smart grid, identify and discuss relevant security issues, and integrate the Role-Based Access Control Model (RBAC) [8] into the environment in order to control access to the network, thus, protects both users' and utility companies' data from improper disclosure. The rest of the paper is organized as follows: an overview of cognitive radio paradigm in smart grid is provided in Section 2. We present a list of vulnerabilities and potential security attacks related to using cognitive radio for smart grid communication along with their mitigation techniques in Section 3. In Section 4, we introduce an access control mechanism based on the well-known Role-Based Access Control Model to manage, securely, the communication within smart grid. Section 5 presents security analysis for the proposed access control mechanism and Section 6 concludes the paper.

2. Cognitive Radio for Smart Grid Networks

The Communication infrastructure in smart grid is required to perform three fundamental functions: sensing, transmission and control. Smart grid is usually deployed over a large geographical area, where the communication infrastructure has to cover the entire area and connect a large number of nodes. A cognitive radio based multi-layer communication infrastructure is proposed in [1] to ensure reliable communication within smart grid. This multi-layer structure consists of three main layers (areas): the home area network (HAN), the neighborhood area network (NAN) and the wide area network (WAN).

Home area networks (HANs) are consumer networks that connect, and communicate with various "home/premises" smart devices to collect real-time energy consumption data. One of those devices with a special importance is the smart meter that plays a major role in the smart grid paradigm. Smart meters are part of this network. Smart meters are the basic components used to collect and deliver power consumption information to remote utilities much more effectively than the conventional meters. Smart meters measure the load profile and demand, store historical information and act as a meter or as a meter/gateway. Using smart meters will also help utility companies monitor the peak load through consumer participation and control electricity consumption. In addition to consumers' premises, smart meters can be deployed as part of the distribution power network and primary and secondary power stations for an end to end command and control. Outside the HAN, a neighborhood area network (NAN) connect multiple HANs to local access points, and wide area network (WAN) controls communication between multiple NANs and the utility control center to achieve energy efficiency and demand/response management.

2.1. Motivations

Several motivations drive using cognitive radio for communication in smart grid networks. Some of these motivations are summarized as follows:

- Smart meters within the HAN usually operate in the 2.4 GHz license-free industrial, scientific and medical (ISM) frequency band for economic reasons. However, there is a number of radio technologies operating in this band (e.g., Bluetooth, Zigbee, U-LTE and WiFi) resulting in significant interference to each other. This imposes significant challenges to the HAN and threatens the reliable data communication within smart grid. Therefore, the need for cognitive radio technology in HANs is vital to reduce interference between these technologies using intelligent transmission scheduling and power coordination techniques.

- The available spectrum for wireless technologies is limited and underutilized due to the static frequency allocation schemes. Therefore, using cognitive radio in smart grid increases spectrum utilization and results in more capacity to support increasing traffic growth.
- The proposed multi-layer communication architecture for the smart grid is essentially a heterogeneous network that needs to communicate over three networks: HAN, NAN and WAN. Therefore, cognitive radio would be a good fit to ensure coverage and convergence of the whole smart grid, where smart grid components need to be equipped with cognitive radio functionalities.
- Cognitive radio can utilize white spaces within the local TV band spectrum for low-latency communications, which improves the overall performance of the smart grid network.
- Smart grid network is usually a large scale network that is distributed over a large geographic area. Hence, multiple communication networks can coexist within a single smart grid, and using cognitive radio guarantees fair spectrum sharing among those networks.
- Using cognitive radio capabilities allow smart grid applications and services to use different spectrum regulations that may exist within this large scale network while achieving the desired QoSs. Using cognitive radio functionalities, data transmission can be scheduled to achieve differential QoS based on the priority of the transmitted data [9], where data priority is defined according to the role and location of the smart grid user.
- Cognitive radio offers a cost-effective solution to extend the coverage area of the whole smart grid without the need to install more switches and routers, in the wired communication case, or wireless access points and base stations, in the wireless communication case. This can be achieved by using cognitive radio-based standards such as IEEE 802.22 [7,10]. Furthermore, Operating cost of the cognitive network is optimized under real-time pricing where macrocell and femtocell base stations adjust their power consumption based on electricity prices [11].
- Cognitive radio provides an energy-efficient technology for data communication in smart grid, with optimum data transmission duration and high average data throughput [12].

Cognitive radio in HAN operates in the license-free band to coordinate the heterogeneous wireless technologies. While in NAN and WAN cognitive communication operates in licensed bands to utilize unoccupied spectrum opportunities. In the next section we explore various communication technologies pertained CR in more details.

2.2. IEEE Standards Related to CR

There are several IEEE standard developments, which are related to the adoption of CR communications as a technology. In this paper, we discuss three of these IEEE standards.

IEEE 802.22: The IEEE 802.22 standard is developed to define the air interface in wireless regional area networks (WRAN) to access available TV white spaces using cognitive radio as a technology. It benefits from the good propagation characteristics of TV channels, operating in the VHF and UHF spectrum regions, to provide a broadband access for rural and regional areas with an extended coverage area (33–100 km) [7].

The IEEE 802.22 standard operates as a point-to-multipoint (P2MP) network, where a base station (BS) and a number of customer premises equipment (CPE) form a cell. The BS controls the medium access of all CPEs, transmits data to the CPEs in the downlink, and receives data from the CPEs in the uplink. To ensure reliable communication and prevent harmful interference to the primary users (PUs), spectrum sensing is performed. There are two methods considered for spectrum sensing. In the first method, the BS transmits location information via a GPS device to a centralized database, which has information about the PU activity in the different TV channels, and the database replies back with the available TV channels within the coverage area of the BS. In the second method, the BS locally determines the availability of free TV channels based on its sensing information or sensing information received from the CPEs. The CPEs perform distributed sensing and then periodically send

sensing information to the BS, which gathers the information and makes a decision whether to keep communication in the current channel or move to another available channel.

The IEEE 802.22 PHY layer employs orthogonal frequency division multiple access (OFDMA) modulation scheme for transmission in the uplink and downlink, to efficiently adjust and allocate the available bandwidth. With OFDMA the BS can smoothly change the operating channel, when claimed by the primary user, to another free channel without affecting communication with the CPEs. The MAC layer adopts cognitive radio and performs two types of spectrum sensing: fast and fine sensing. In fast sensing, both CPEs and BS perform sensing quickly (at a speed under 1 ms per channel) to exploit the changes in spectrum occupancy and decide if transmission needs to be moved to another channel. Then, the BS initiates fine sensing based on the results of the fast sensing stage, in which sensing takes longer time (about 25 ms per channel). Simple sensing techniques such as energy detection are used in fast sensing, while more accurate sensing techniques such as matched-filter detection and cyclostationary-feature detection are employed in fine sensing [7].

IEEE 802.19.1 Standard: The IEEE 802.19.1 was developed for "TV White Space Coexistence Methods" [13,14]. This standard defines three mainly needed mechanisms for achieving coexistence between different CR systems operating within the TV white space frequency bands. One is the discovery of systems that need to coexist with each other. This is achieved by employing a logical entity called a coexistence discovery and information server (CDIS) which uses certain parameters to discover radio systems, which can be considered as neighbors, *i.e.*, interference between them is possible, within the TV white space radio system. These parameters include .the locations of the white space radio systems and their radiated power characteristics.

Second is the modification of operating parameters of these systems to achieve better performance. This can be done through two services provided by the standard: information service and management service. The information service relies on neighbor discovery parameter information, which is periodically provided to the white space radio system to autonomously update its operating parameters. As for the management service, the coexistence system manages the operating parameters of a white space radio system through an employed logical entity called a coexistence manager, which collects registration information from the CDIS serving the neighboring various radio systems in addition to information on the available frequency bands. These information are then evaluated and coexistence decisions are made.

Third is the providing of a unified interface between the different types of radio systems and a coexistence system. This service is achieved through defining a logical entity called a coexistence enabler to provide a unified interface between a white space radio system and the IEEE 802.19.1 coexistence system. However, the standard only defines an abstract notion of this interface and leaves its implementation up to the individual manufacturers.

IEEE 802.11af Standard: The IEEE 802.11af standard provides a framework to incorporate the different operating parameters of licensed and unlicensed devises operating within the white space radio system [15]. This is mainly concerned with preventing unlicensed devices from interfering with existing licensed devices operating within the same band simultaneously. To enable and manage spectrum sharing in the white space TV band a geo-location database containing a full knowledge of licensed and unlicensed usage of the band can be implemented through two approaches: open and closed-loop systems. The IEEE 802.11af standard provides a common framework for architecture, communication and a control structure that allows standardization across these two approaches.

2.3. Cognitive Radio-Based Communication Infrastructure

In general, there are three CR communication paradigms that can be used in smart grid environment: Interweave CR communication, Underlay CR communication, and Overlay CR communication. In the interweave paradigm, the secondary user can access a certain frequency band as long as no primary user's activity is detected. However, once a primary user's activity is sensed, the secondary user has to vacate the band. In the underlay paradigm, secondary users transmit

with low power, below the noise threshold of the primary user communication, to avoid interfering with the primary user transmission. The underlay and interweave CR-based SG communication paradigms can be used for data communication within a HAN due to low data rates and short communication ranges. On the other hand, overlay CR-based SG communication utilizes code books and messages to identify the primary users, thus mitigating any interference. A CR user can transmit at any power and the interference to non-cognitive users can be offset by relaying the non-cognitive users' messages. These methods satisfy reliability, security and high data rates, and thus are suited for NANs and WANs [16]. In the following subsections, a cognitive radio-based multilayer architecture for smart grid communication is explored and discussed.

2.3.1. Home Area Networks (HANs)

HAN includes smart meters, sensors, actuators, home appliances, in-home displays, energy management systems, and electric dashboards. It establishes two-way communication links between these components to deliver real-time power data and load information from customer's side to the utility control center. It also manages receiving dynamic electricity pricing information and demand response in the reverse direction. Data exchanged over the HAN can be used for different purposes such as power measurements, peak demand management, pricing, power supply/demand balancing, and energy consumption management.

As shown in Figure 3, communication within the HAN is performed using a star topology. Where data is sent to the HAN cognitive gateway (HGW), which acts as an access point or an interface between the HAN and the NAN, using different wireless technologies (e.g., WiFi, Bluetooth, and Zigbee) or wired technologies (e.g., power line communications).

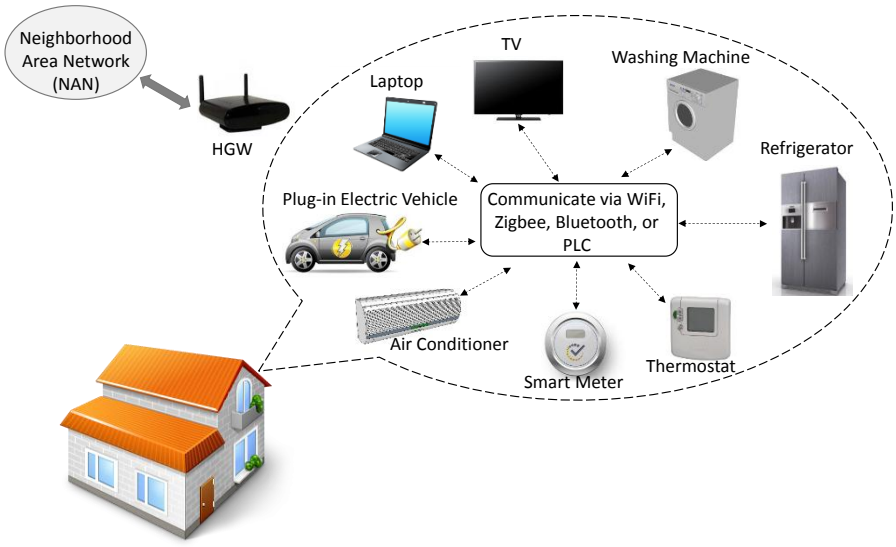

Figure 3. Home Area Network (HAN) Architecture.

Cognitive Radio in HANs:

HAN is basically a heterogeneous network that comprises different communication technologies. Moreover, reliable and flexible communication is required to accommodate the increasing number of devices joining a HAN and to manage communication between multiple HANs and a NAN. To achieve this, the HGW should have self-configuration and cognitive capabilities to adjust its operating parameters according to the surrounding radio environment. Using cognitive radio capabilities, the HGW can sense the spectrum and opportunistically access unused frequency bands, under certain interference constraints, in order to establish communication between the HAN and the external NAN. Moreover, the HGW manages communication within the HAN in the licensed-free spectrum, it assigns

frequency channel and network address to the devices joining the HAN, coordinates communication between devices, and manages spectrum sharing among smart meters.

2.3.2. Neighborhood Area Networks (NANs)

A NAN is the intermediate layer that connects multiple HANs to the WAN of the utility company. Load information and energy consumption data measured by smart meters are collected and sent via HGWs to the NAN and then to the utility control center. Communication within the NAN is organized using the NAN cognitive gateway (NGW), where the NGW connects multiple HGWs together as shown in Figure 4.

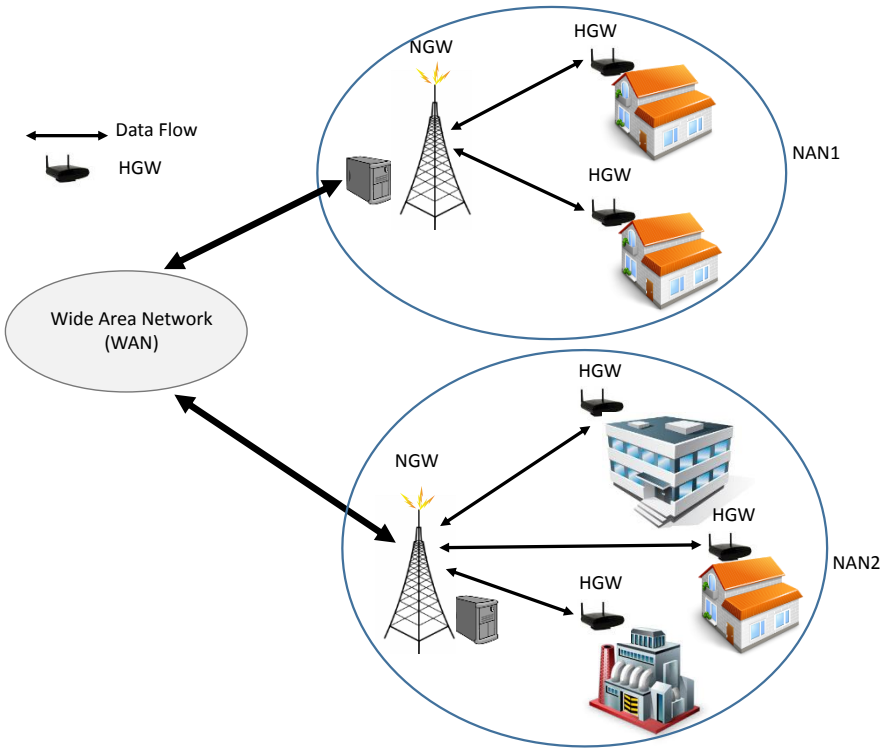

Figure 4. Neighborhood Area Network (NAN) Architecture.

Cognitive Radio in NANs:

Within the NAN, HGWs act as cognitive nodes that communicate with the NGW over the licensed spectrum using cognitive radio technology, where the NGW is used as cognitive radio access point to transfer data and distribute the spectrum between multiple HGWs. However, communication between HGWs and NGWs over the licensed band might be insufficient to accommodate the increasingly growing traffic and satisfy the QoS requirements within the smart grid. Therefore, a novel hybrid dynamic spectrum access (H-DSA) paradigm has been proposed [1]. In H-DSA, HGWs communicate with NGWs over the licensed band to ensure QoS of data communication, while unlicensed access is used to improve capacity and throughput. In the unlicensed access, both HGWs and NGWs are considered as secondary users and can access the unoccupied spectrum opportunistically. This paradigm provides cost-effective and reliable communication for smart grid.

TV white space (TVWS) can also be used for communication between HGWs and NGW within the NAN. However, interference between multiple NANs that coexist within the same geographical area should be taken into consideration. The authors in [17] proposed to allow the HGW to sense the TVWS channel declared available from incumbents by the White Space Database (WSDB) to discover the presence of an interfering NAN. If the sensing result declares the TVWS channel as idle, the HGW can

transmit over that channel. Otherwise, the HGW uses the unlicensed channel. The sensing duration is designed to maximize the achievable data rate, by explicitly accounting for the accuracy/overhead trade-off and the co-located NANs traffic patterns.

2.3.3. Wide Area Networks (WANs)

A WAN in the cognitive radio-based communication infrastructure in smart grid manages communication between multiple NANs and the utility control center as shown in Figure 5. In the WAN, each NGW acts as a cognitive node with the capability to communicate with the utility control center over the unused licensed spectrum via a CR base station [1]. In addition to the utility control center, a spectrum database exists to manage the sharing of spectrum resources between multiple NANs.

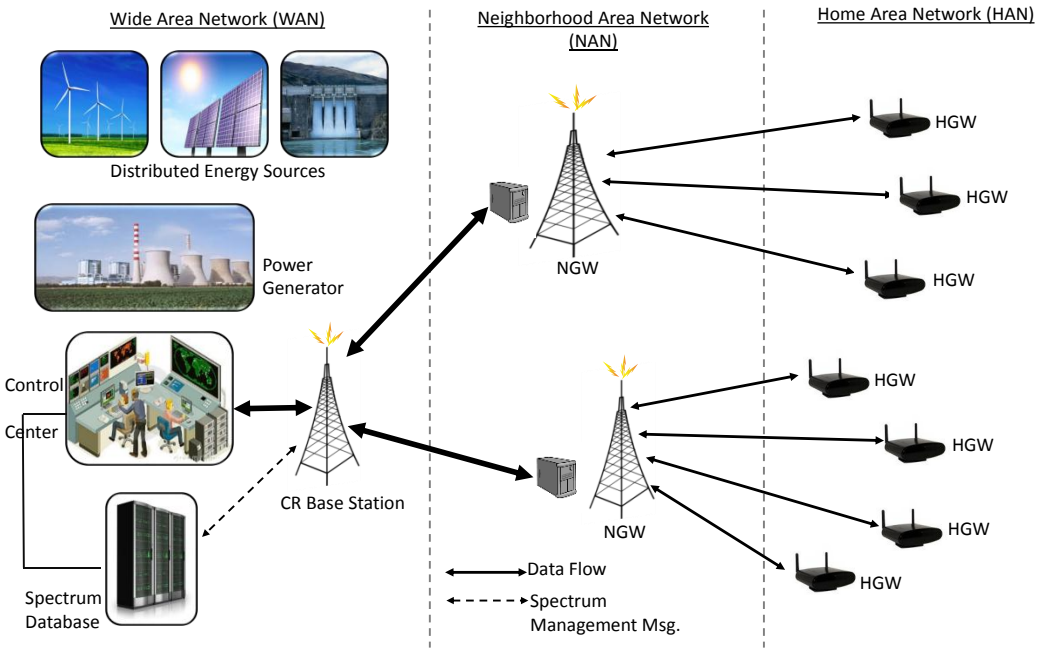

Figure 5. Wide Area Network (WAN) Architecture.

Cognitive Radio in WANs:

The CR base station manages communication between multiple NGWs. Both licensed and unlicensed spectrum access can be used for communication, where the spectrum database (broker) is responsible for scheduling and switching between these two modes without affecting the service. Moreover, if multiple NANs are distributed over a large geographic area within a WAN, they can share the same frequency bands without causing interference to each other.

2.4. Cognitive Radio Applications for Smart Grid Networks

2.4.1. Advanced Metering Infrastructure (AMI)

Advanced metering infrastructure (AMI) represents the entire measurement and collection system including: smart meters at the customer side, communication network between customers and service provider, and data management systems [18]. The amount of data generated and exchanged within the smart grid is enormous and the need for reliable and secure communication infrastructure is crucial. However, the presence of different communication technologies within smart grid makes it difficult to build an end to end reliable communication infrastructure. For example, as mentioned earlier, smart meters within the HAN communicate over the unlicensed ISM band, where interference is a significant

issue that might affect the reliability of the communication backbone. Moreover, exchanging data between access points and electric utility over the licensed band adds extra cost in establishing a communication infrastructure for the smart grid. Therefore, using cognitive radio functionalities in opportunistic spectrum access and spectrum sharing helps utilize the unused licensed spectrum to achieve efficient data communication over the smart grid. CR enabled smart meters will be able to sense the spectrum for channel availability to better utilize the available spectrum. The communication overhead associated with such sensing will depends on several factors, such as the frequency of sensing, availability of channels and the number of licensed users within the operational cell. Data transmission can be scheduled using different channel selection mechanisms to guarantee the reliability and energy efficiency. For example, data transmitted over the smart grid can be classified into two categories: delay-sensitive data and non-delay-sensitive data. Using channel selection mechanisms such as the one proposed in [19], delay-sensitive data is transmitted over reliable channel while non-delay-sensitive data is transmitted over high SNR channel at a higher data rate.

2.4.2. Distributed Power Generation

The integration of traditional power sources and renewable energy sources is a special feature of smart grid. In addition to generating clean energy, the use of renewable energy sources reduces the burden on the increasingly overloaded traditional power sources. This helps in balancing the overall power demand in smart grid. However, traditional and renewable power sources have differences in price and availability. This raises the need for reliable communication and coordination to balance their usage and monitor their operation for efficiency and safety purposes. To achieve this, wireless networks can be used to provide cost-effective communication infrastructure for smart grid. However, the performance of any wireless networks can be affected by many factors such as interference, physical obstacles, network contention, and node failure. Therefore, using CR can be suitable to increase communication reliability and efficiency using opportunistic spectrum access techniques while taking into consideration acceptable communication overhead by dynamically adjusting the sensing parameters based on performance indicators of the overall system.

2.4.3. Smart Grid Monitoring

Monitoring the operation of all smart grid components including generation utilities, transmission lines, and the distribution utility is very important to ensure the consistency of high-level performance, reliability, and efficiency of such systems. It is also vital to ensure effective and reliable demand response management (DRM). Smart grid monitoring can be performed over licensed or unlicensed frequency spectrum. While using the unlicensed spectrum can be efficient in terms of cost and installation, it suffers from crowdedness interference. Moreover, the fact that smart grid is a large-scale network makes it difficult to build a sensor network that can monitor the grid reliably due to electromagnetic interference, maintenance, shadowing and fading issues [20]. Therefore, using cognitive radio functionalities, such as spectrum sensing and opportunistic dynamic spectrum access, helps achieve a reliable monitoring operation with high efficiency and minimal cost.

Monitoring the CR communication channels in smart grid produces an additional overhead resulting from spectrum sensing. To deal with this extra traffic load, several algorithms have been proposed. These algorithms aim to design an optimal sensing time while ensuring a reliable sensing process. In [21], a two-way cognitive-switching procedure was proposed. A cost function, which takes into account both the sensing-accuracy improvement gained and the transmission capacity degradation induced due to increasing sensing time, is evaluated and an optimum sensing time is derived. In [22], a joint optimization algorithm for sensing time and transmission time was also derived. A sensing-performance tradeoff between better control performance and lower communication cost was achieved by calculating the optimal sensing time value under the constraint that the licensed primary user is sufficiently protected [23]. In addition, different spectrum sharing techniques have been proposed to better utilize the licensed spectrum and ensure reliable communication between

smart grid components. Some spectrum sharing techniques utilize the spectrum either in the space or time dimension where more efficient ones utilize the spectrum in dimensions such as the joint spatial and temporal spectrum sharing technique [24].

2.4.4. Electric Vehicles (G2V and V2G)

Growing environmental concerns motivated the work toward an economic and environment-friendly replacement for the conventional fuel-operated vehicles. Therefore, electric vehicles (EV) started to emerge the market as the future generation of transportation systems. Two types of vehicles fall under the category of electric vehicles: fully electric vehicles and plug-in hybrid electric vehicles (PHEVs). EVs are integrated into smart grid in two paradigms, Grid-to-Vehicle (G2V) and Vehicle-to-Grid (V2G).

In a G2V paradigm, EVs get their electricity supply from external power source within the smart grid, where EVs batteries are charged upon request. The major concern in this paradigm, although it is theoretically simple, is the additional load imposed on the grid during charging times. The penetration of EVs within the grid affects load balancing and peak-demand management. In [25], the authors presented a case study on the effect of PHEVs penetration on the existing distribution systems in the Pacific Northwest. The study has shown that the existing distribution infrastructure is capable of supporting 50% penetration of PHEVs with the 120 V smart-charging profile, which is approximately 21.6% of the light duty vehicle (LDV) fleet. However, this exceeds the capacity of the existing generation infrastructure that can support approximately 18% of the LDV fleet.

High penetration of EVs in addition to uncoordinated charging result in major challenges in smart grid such as; overloading, power outages, and degradation in grid performance. To overcome these challenges, large-scale EVs behavior should be analyzed using different methods such as queuing theory. Charging stations are assumed to work as a queue serving arriving EVs. Using queuing theory many parameters affecting EVs charging process can be analyzed such as; EVs arrival rate, queue length, EV waiting time in the queue to be served, and number of EVs being served. Moreover, the number of available charging stations, and their state (empty or full) can be predicted.

The second paradigm is V2G, where EVs are used to store and supply electric power to the grid. This paradigm is motivated by the fact that the car in US is driven one hour a day on average [26]. Therefore, EVs can communicate and deliver power when they are parked and connected to the grid. This can help in balancing load throughout the grid during peak times. However, proper and effective operation of V2G is subject to uncertainty as it depends on the availability of EVs plugged into the grid. Moreover, EVs can communicate with each other within a V2V paradigm using vehicular ad hoc networks (VANET) technology, where they can exchange information about the location and availability of charging stations. In addition, they can share their experience about the quality of service provided by charging stations in terms of charging time and waiting time.

Up to this end, it is obvious that EVs need reliable communication links with the generation and distribution infrastructures in smart grid to ensure effective demand/supply operation and charging coordination. For example, an EV has to communicate with the grid and send a charging request to acquire power supply for charging its battery in the G2V paradigm. Therefore, information about available charging stations, their locations, and the amount of time that the EV needs to wait before being served has to be available for the EV sending the charging request. Moreover, in the V2G paradigm, the grid has to communicate with EVs to check their availability within a certain location, or the time at which they will be available to supply the grid with electricity. This implies that smart grid certain entities and EVs need to communicate reliably and continuously exchanging information. However, dedicating certain frequency bands to accommodate communication between EVs and smart grid entities is inefficient especially when considering the cost of frequency spectrum licenses and the growing number of EVs over time. Therefore, cognitive radio as a technology can be considered as an effective communication alternative for this application, where opportunistic spectrum access can be used to manage EVs and grid communication by utilizing unused frequency bands. Besides, using

cognitive radio makes the smart grid adaptive to an increasing number of EVs, helps balance the load, and utilizes the available power resources through proper allocation of EVs charging requests.

3. Security Issues Related to Cognitive Radio in Smart Grid Networks

Data exchanged within smart grid networks is valuable and confidential for both customers and utility companies, as it carries critical information such as energy consumption, active appliances, customer's name/address, and payment information. Therefore, any communication infrastructure designed for smart grid should emphasize security to guarantee reliable and efficient performance. Following are the main security requirements that need to be considered when designing a security framework for smart grid communication infrastructure.

Privacy: As mentioned earlier, information related to consumers is private and needs to remain confidential when transmitted over the smart grid network. To achieve this, every smart meter, gateway, and server within the smart grid has to implement some measures to ensure confidentiality. Smart meters within the HAN are authenticated by the HAN cognitive gateway (HGW) and HGWs are authenticated by the utility company. This hierarchal approach provides a scalable solution that ensures the provision of secure communication within the smart grid [27].

Integrity: Integrity refers to the protection against unauthorized modification of data while it is in transit. In smart grid, the integrity of data exchanged over its networks can be subject to many attacks such as data falsification [28], data injection [29], message replay, and message delay [30]. These attacks can negatively affect a smart grid operation given the amount of data and the sensitivity of information being transmitted over the grid.

Availability: Availability refers to adequate system resources being always available when needed. A malicious user can target smart grid availability by connecting to communication channels within the grid and initiating DoS attacks. This results in delaying/blocking data from authorized users and corrupting communication between smart grid components. Therefore, violating availability in smart grid communication networks dramatically degrades the overall performance of the grid [31].

Authentication: Authentication refers to determining the identity of any subject (user, process or device) trying to join the smart grid network, and verifying provided credentials against information stored in a database.

Authorization: Authorization controls the access to smart grid and prevents illegitimate users from acquiring data or issuing commands to the control system. Achieving other security objectives such as, privacy and integrity mostly depends on the authorization stage.

In addition to the general security requirements mentioned above, using cognitive radio as a technology for communication in smart grid introduces its own vulnerabilities and security concerns as with all other wireless communication technologies. Moreover, the fact that cognitive radio dynamically adjusts its parameters according to the surrounding radio environment creates new opportunities for more attacks. In this paper, we focus on security attacks in cognitive radio networks and their impact on the operation of the cognitive radio-based communication infrastructure when applied in a smart grid network.

To better understand and analyze the possible attacks on the cognitive radio network, we first introduce the main functionalities of such network.

Four main cognitive functionalities are performed to set up communication in a cognitive radio network. As shown in Figure 6, these functionalities are spectrum sensing, spectrum management, spectrum sharing, and spectrum mobility [32]. Spectrum sensing is performed to exploit spectrum holes (opportunities) for unlicensed access, and spectrum management is executed to utilize these opportunities without causing interference to the primary user. Moreover, spectrum sharing allows the secondary user to share the spectrum with the primary user and other secondary users, where the IEEE 802.22, IEEE 802.19.1 and 802.11af standards are developed to manage this functionality. Finally, spectrum mobility allows secondary users to move to another empty frequency band after vacating the current band for the primary user.

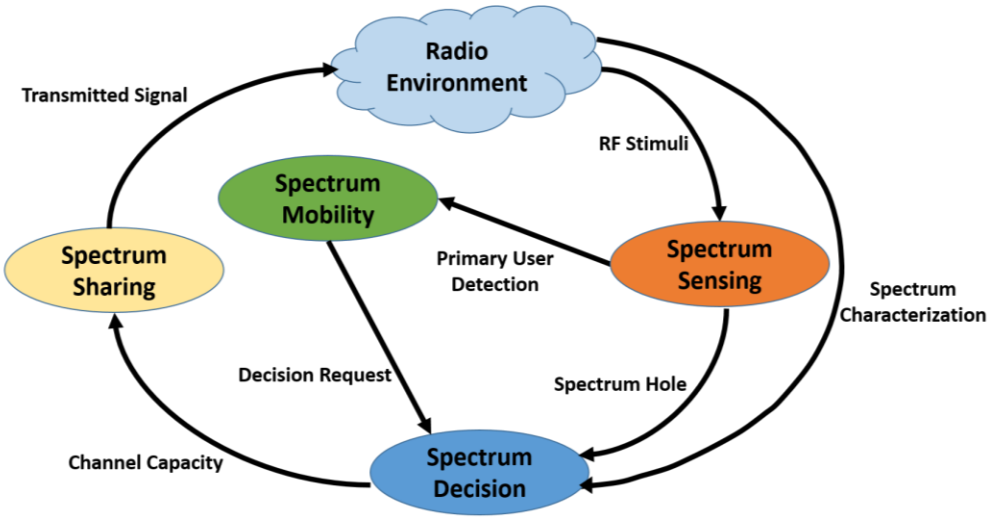

Figure 6. Cognitive Radio Cycle.

The operation of these functionalities and hence the performance of the whole cognitive radio network can be affected by security attacks. Two types of cognitive radio can be identified to be affected by security attacks: policy radio and learning radio [33,34]. Policy radio has a reasoning engine that determines the status of a frequency band based on the current activity of the primary user. Therefore, the effect of the attack disappears whenever the attacker leaves the channel. On the other hand, learning radio has a reasoning and learning engine that uses both the current and past information of the primary user activity to predict the status of a frequency band. Hence, resulting in a long-term effect of the security attack on the cognitive radio network.

Moreover, cognitive radio networks can operate in two modes; non-collaborative and collaborative. In the non-collaborative mode, one secondary user senses the channel and decides whether it is occupied by the primary user or not. While in the collaborative mode, multiple secondary users sense the channel and exchange their information with each other, in the case of distributed spectrum sensing, or send their information to a spectrum manager (fusion center), in the case of centralized spectrum sensing, to decide upon the status of the channel. Collaborative sensing is used to achieve higher sensing accuracy by overcoming some sensing issues such as; hidden primary user problem, multipath fading, and shadowing. However, collaborative sensing can be highly affected by possible security attacks as the attacker may send false data to the fusion center and affect the final decision regarding the primary user's presence [35].

In the case of smart grid networks, security attacks can affect the reliability and efficiency of the cognitive radio-based communication infrastructure by reducing the overall throughput of the network. For example, if the attack is performed within a NAN, where cognitive radio is used to organize communication and allocate available spectrum opportunities between multiple HGWs, an attacker might disrupt communication between the NGW and the HGWs. In addition, an attack can be launched within a WAN, where a CR base station is used to manage communication between multiple NGWs and the utility company control center. In this case, the attacker can fool the CR base station and the spectrum broker to consider him as a primary user, resulting in reduction in spectrum opportunities available for the NGWs to communicate with the control center. Figure 7 shows an example of security attack within cognitive radio-based communication infrastructure in both a NAN and a WAN.

The following subsections describe the different security attacks against cognitive radio-based communications and provide proper mitigation mechanisms to defend against these attacks.

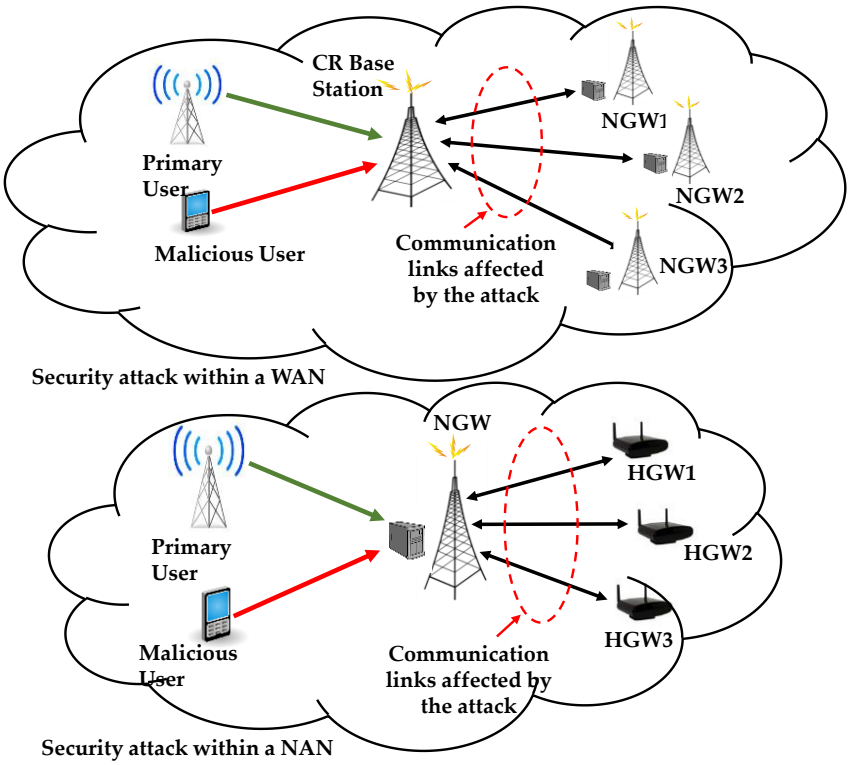

Figure 7. Example of Security Attack in a Cognitive Radio-Based Communication Infrastructure.

3.1. Primary User Emulation (PUE)

One of the main features of cognitive radio networks is the ability to distinguish between the primary user and the secondary user. Different spectrum sensing techniques can be used to detect the primary user such as energy detection, matched filter detection, and cyclostationary-feature detection. Once the primary user is detected, the secondary user has to vacate the channel and search for another free channel to access.

In a primary user emulation (PUE) attack [36], a malicious user may modify his signal to emulate the primary user signal. In this case, other secondary users will sense the frequency band and falsely decide on it being occupied by a primary user. The PUE attack is performed for either selfish purposes or malicious purposes. In the selfish PUE attack, the attacker's intention is to access the available spectrum opportunities without sharing them with other secondary users. While in the malicious PUE attack, the attacker aims to disrupt the communication of other legitimate secondary users, by preventing them from accessing available spectrum opportunities, and cause a denial of service situation.

Mitigation Techniques for Primary User Emulation Attack:

The key concept for defending against the PUE attack is identifying whether the transmitter is a licensed primary user or an attacker. Taking into consideration that the location of the primary user is known to the cognitive radio network, matching the location of the transmitter with the location of the primary user allows detection of the attacker. From this perspective, the authors in [37] proposed a trust based algorithm dependent on the location awareness and distance between the users. Given that the location of the primary user is known to the secondary users, the distance to both the primary user and the user emulating the primary user are calculated based on the received signal strength. Based on the results, the trustworthiness of both users is determined and the users are classified as either legitimate or malicious.

In [38], the authors proposed a transmitter verification scheme called localization based defense (LocDef). This scheme utilizes the underlying wireless sensor network to collect data about the received signal strength (RSS) across the cognitive radio network. Based on the strong correlation between the RSS and the distance between transmitter and receiver, the collected data is smoothed and the location of the transmitter is identified.

3.2. Jamming

In jamming, a malicious user transmits over the licensed channel to make it unavailable for both the primary user and the secondary users; resulting in a denial of service situation. The jammer can transmit over the channel continuously to force other secondary users take a false decision, or he may jam the common control channel (CCC) used to exchange sensing information and disrupt the overall communication within the cognitive radio network. This kind of jamming can easily be applied within a HAN thus denying proper communication between the HGW, smart meters, and home appliances.

There are four types of jammers: constant jammer, deceptive jammer, random jammer, and reactive jammer [39]. The constant jammer continuously transmits random bits without waiting for the channel to be idle and regardless of the MAC-layer protocols. Therefore, with this constant transmission performed by the jammer, other secondary users will always make false decisions about the sensed channel and will not be able to access it. Examples of a constant jammer are a waveform generator or a normal wireless device. The deceptive jammer continuously transmits regular packets with zero inter-departure time between transmissions. It forces other users to stay in the receiving mode whether they have data to transmit or not, as they are deceived by the constant stream of transmissions. The random jammer switches between jamming and sleeping modes. For example, it may jam for t_j time slots and then sleeps for t_s time slots in order to save its energy. In addition, during jamming periods it may act as a constant or as a deceptive jammer. On the other hand, the reactive jammer is different from the three types of jammers mentioned above in the sense that it remains quiet as long as the channel is idle and jams the channel whenever it detects communication. From the jammer's point of view, this type of jamming is inefficient in terms of energy consumption, as the jammer needs to sense the channel all the time to capture any activity. However, it is hard to detect the reactive jammer since jamming is not performed continuously.

Mitigation Techniques for Jamming:

Before discussing jamming mitigation, it is important to discuss jamming detection. Different techniques exist to detect a jammer. In [39], a jamming detection technique, known as Signal Strength Consistency Check, is proposed. This check is based on the signal strength (SS) and the packet delivery ratio (PDR). The PDR can be measured either at the transmitter side, as the number of acknowledgements received from the receiver; or on the receiver side, as the number of packets that pass the CRC check with respect to the number of packets received. When no packets are received, the PDR will be zero. In jamming-free wireless network, a certain node will measure high SS and high PDR from its close neighboring nodes. However, under jamming attacks, this node will measure high SS and low PDR at the same time. Another test that can be performed to detect jamming is the Location Consistency Check. This check is based on the location of the nodes, where the location can be acquired using GPS. Under normal conditions, any node should measure high PDR value from its close neighbors. However, when this node captures low PDR from a neighboring node, this means that the neighboring node is under a jamming attack.

Defending against jamming attacks is the next step after detecting such attacks. In [40], two approaches to defend against jamming have been proposed; channel surfing, and spatial retreats. In the channel surfing approach, both the transmitter and the receiver move their communication to another channel once jamming is detected on the current channel. Channel surfing can be performed physically using frequency hopping, under the assumption that the jammer can jam only one channel at a time and does not have an access to the authentication key. The second approach is the spatial retreats,

where the nodes move their location outside the interference range of the jammer. However, some coordination between moving nodes should exist to guarantee that they stay within the communication range of each other and escape from the jammer at the same time. This technique is effective in the case of wireless networks with mobile nodes. In a smart grid network, this can be best seen to be applied in the previously discussed applications of V2G, G2V and V2V communication.

3.3. Objective Function Attack

The main feature of cognitive radio is its ability to sense the surrounding radio environment and adjust its radio parameters accordingly. These parameters include; power, bandwidth, center frequency, modulation type, coding rate, channel access protocol, frame size, and encryption type. By solving the objective function, these parameters can be defined in order to achieve certain transmission requirements such as a high level of security, and a high data rate. In the objective function attack, the attacker manipulates the parameters, which he can control and change the sensing results. The authors in [33] discussed an objective function attack example, where the following objective function is considered with w_i as weights, p as power, r as transmission rate, and s as security.

$$f = w_1 p + w_2 r + w_3 s \tag{1}$$

Cognitive radio solves the objective function to minimize power consumption p, maximize transmission rate r, and maximize security level s. However, if the attacker aims to lower security level s, then whenever the cognitive radio system tries to send data at high security level, the attacker will jam the channel resulting in lower transmission rate and hence lower objective function. Therefore, the cognitive radio system will readjust its parameters and send high security data at lower security level.

Mitigation Techniques for Objective Function Attack:

A simple solution to defend against the objective function attack has been proposed in [41]. It is based on defining a threshold for every adjustable radio parameter, and if any parameter does not meet the threshold, communication will stop. Another solution to overcome this attack is proposed in [42] using the neighborhood majority voting approach. In this approach, each secondary user collects sensing reports from its immediate neighbors and performs a spatial correlation test to decide the legality of its neighbors. The results are broadcasted to the neighboring nodes, and if a node receives more than half of its neighbor votes announcing it as a suspicious node, then this node will be considered as a malicious node. In a smart grid network, this can be applied in a NAN where collaborative communication can be utilized between HGWs when communicating with a NGA.

3.4. Byzantine Attack

The Byzantine attack, also known as spectrum sensing data falsification (SSDF), happens when an attacker sends false spectrum sensing data and results in wrong sensing decision. By sending false data, to the fusion center in the case of centralized collaborative sensing or to other secondary users in the case of distributed collaborative sensing, legitimate secondary users will either be denied from accessing a free channel or admitted to a busy channel causing interference to the primary user. The severity of this attack is higher in the case of distributed sensing, as sensing information propagates among secondary users faster. While in centralized sensing, the fusion center can control and detect false data by comparing sensing information from different secondary users.

Mitigation Techniques for Byzantine Attack:

A mitigation technique to detect malicious nodes based on a trust approach and pre-filtering techniques is proposed in [43]. Malicious nodes are classified into two types: "Always Yes" and "Always No". An "Always Yes" node sends positive sensing data all the time indicating that the primary user is present; hence it increases the probability of false detection. While an "Always No"

node always advertises that the primary user is absent, resulting in reduction in the probability of detection. The pre-filtering stage can identify and remove malicious nodes by assigning trust values to each node, based on the data received from all nodes, followed by a data quantization step. A fast and easy technique for identifying a malicious node is proposed in [44], where the byzantine attacker can be detected by counting the number of mismatches between its local decisions and the global decision at the fusion center over a certain time window. This technique proves to be effective for detecting byzantine attackers over a short time period.

3.5. Control Channel Saturation

Any secondary user should finish channel negotiation and reserve a channel during the control phase, where negotiation is performed over a Common Control Channel (CCC), in order to be able to communicate and send data during the data transmission phase. However, the common control channel can accommodate a limited number of contending secondary users at the same time. In a control channel saturation attack, a malicious user may utilize this feature and saturate the control channel by sending a large number of packets. Therefore, causing a DoS blocking other legitimate secondary users and reducing the overall throughput of the cognitive radio network.

Mitigation Techniques for Control Channel Saturation:

A trust approach, to the control channel saturation attack, is proposed in [45] based on Sequential Probability Ratio Test (SPRT). In this approach, neighboring nodes of the secondary user perform sequential analysis on observations of data to determine whether this user is malicious or trusted. Another technique based on dynamic channelization is suggested in [46]. In dynamic channelization, an atomic channel of b Hz is defined and the common control channel shifts its center frequency, f_0, so that the new center frequency, f, is calculated as follows:

$$f = f_0 + mb \tag{2}$$

where $m = 0, \pm 1, \pm 2, etc$. The bandwidth of the permissible migrated control channel takes odd-number multiple of b, *i.e.*, kb, where $k = 1, 3, 5, etc$. Hence, any permissible control channel can be denoted by a pair of integers (m, k). Figure 8 shows a control channel migration for $(m, k) = (5, 3)$.

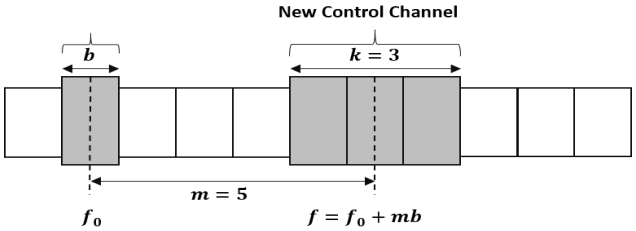

Figure 8. Common Control Channel Migration for $(m, k) = (5, 3)$ [46].

It is important to mention that security attacks degrade the efficiency and reliability of communication within smart grid networks on one hand, and affect service providers and customers on the other hand. More precisely, security attacks result in communication disruption by either delaying communication or causing denial of service. Therefore, this will have major consequences on the smart grid from economical, technical, and social perspectives. From a service provider's point of view, security attacks will affect collecting and exchanging data that is important for grid monitoring, fault detection, demand/supply management, and bill pricing. Economic consequences will arise due to the lack of reliable communication between smart grid elements, where power outages will be more frequent and power demand/supply will not be controlled and managed properly. Furthermore, these attacks can result in life-threatening consequences, when the grid is not well-monitored and faults are

not detected or controlled. From a customers' perspective, security threats will affect their experience and satisfaction, as their information will be vulnerable to attacks resulting in the violation of their privacy and miss representation of their data. This will discourage them from being part of the smart grid paradigm and affect the spread and development of smart grid networks.

The above mentioned CR attacks can easily be exploited to have a direct impact on smart grid. These vulnerabilities might allow attackers to access the smart grid network, break the confidentiality and integrity of transmitted data, and make services unavailable. Next we list other vulnerabilities that are most serious in smart grids:

- Exposure of customer's private data: Smart meters autonomously collect massive amounts of data, which includes consumers' private data, and transport it to the utility company, consumers, and service providers. If not protected, this data can be used to infer consumer's activities, devices being used, and times when the home is vacant.
- Physical security: Smart grid network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.
- Exploitation of intelligent devices: A smart grid includes several intelligent devices that are used in managing the electricity supply and demand network. Exploitation of such devices can lead to easy entry points for attacking the network.
- Insider attacks: The fact that smart grid has many stakeholders that can give raise to a very dangerous attack known as the insider attack. Insiders can be driven by different motives and expertise to utilize their access and exploit different vulnerabilities causing damage to the network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors, or customers.

4. Access Control Model for Smart Grid Networks

In the case of cognitive radio-based communication for smart grid, the access of secondary users to licensed bands should be controlled to avoid causing interference to primary users. Moreover, secondary users should have the permission to terminate the connection whenever a malicious user is detected. Therefore, the need to develop an access control mechanism that enforces access policies in cognitive-based communication within smart grid networks, and alleviates the effect of security attacks on smart grid performance and privacy is crucial.

An efficient access control model should be used to guarantee that only authorized users can access the collected data, control sent data and measurements. In this paper, we propose an integration of the well-known access control model called Role-Based Access Control (RBAC) with cognitive radio-based communication within smart grid to ensure proper management and access policies enforcement. RBAC can be used to control the access to smart meters during the communication phase. It allows the owners of smart meter services to control who can identify smart meters locations, approve or disapprove their subsequent connections, based on a set of parameters [8]. Moreover, RBAC supports some important security principles such as least privilege, separation of duties, and data abstraction, which can help in mitigating the risks associated with some of the threats that can lead to the attacks described above. Least privilege is supported, because RBAC can be configured such that only those permissions are assigned to the role required for the tasks conducted by members of the role. Separation of duties is achieved by ensuring that mutually exclusive roles must be invoked to complete a sensitive task, such as requiring a cognitive radio base station and a spectrum data base for sensing spectrum and assigning available frequency bands. Data abstraction is supported by means of abstract permissions such as join, leave, join as a sender, join as a receiver, *etc.* rather than just read, write and execute permissions typically provided by the operating system. Finally, through its role hierarchy feature, RBAC can be used to "securely" manage communications between HANs, NANs, and WANs, which are also of a hierarchical structure. The following section briefly describes the proposed RBAC model.

Role-Based Access Control (RBAC)

RBAC has been proven to be a good alternative to traditional discretionary and mandatory access control. In RBAC, a role is a semantic construct forming the basis for the access control policy. In addition, in RBAC, permissions are associated with roles. Users are made members of appropriate roles based on their responsibilities and qualifications, thereby acquiring the permissions of these roles. In RBAC, users can easily be reassigned from one role to another. Roles can also be granted new permissions as needed, and permissions can be revoked when needed. This can simplify the security management process significantly.

A general RBAC model was defined by Sandhu [8] and summarized in Figure 9. The model is based on three sets of entities called users (U), roles (R), and permissions (P). A user is a human being or an autonomous agent. A role is a job function or job title within the organization with some associated semantics regarding the authority and responsibility conferred on a member of the role. Permission is an approval of a particular mode of access to one or more objects in the system. The user assignment (UA) and permission assignment (PA) relations of Figure 9 are both many-to-many relationships (indicated by the double-headed arrows). A user can be a member of many roles, and a role can be assigned to many users. Similarly, a role can have many permissions, and the same permission can be assigned to different roles.

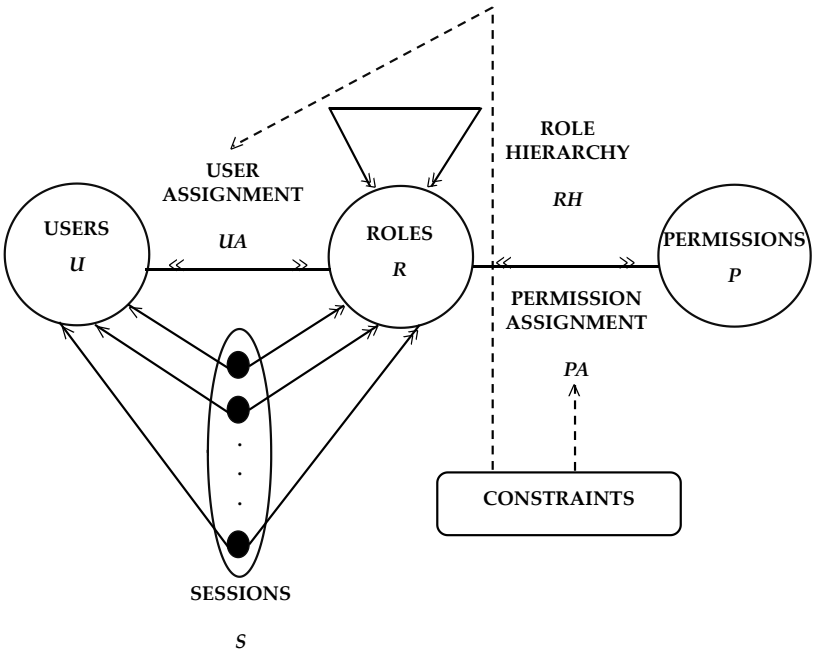

Figure 9. RBAC Model.

Role hierarchy (RH) in RBAC is a natural way of organizing roles to reflect the organization's lines of authority and responsibility. The hierarchy is partially ordered, so it is reflexive, transitive, and anti-symmetric. Inheritance is reflexive because a role inherits its own permissions. Transitivity is a natural requirement in this context, and anti-symmetry rules out roles that inherit from one another and are therefore redundant.

5. RBAC Integration for Cognitive Radio in Smart Grid

This section discusses how RBAC is used to manage and control the cognitive radio-based communication infrastructure for smart grid. First, system requirements and design goals are stated, then, access control policies for these requirements are specified, and finally, an access control model to

enforce these policies is defined. In this paper, we focus our attention on two design goals; customers' privacy and communication efficiency/security.

Customers' privacy refers to protecting customers' data against unauthorized access. This data is very critical and confidential, as it carries important details about customer's name/address, monthly bill amount, energy consumption profile, and active appliances, *etc*. Therefore, it is important to define access control policies to determine who can access this data and/or modify it. Access to this data has to be controlled over the communication link: smart meters ↔ HGW ↔ NGW ↔ CR base station ↔ utility control center.

On the other hand, the communication infrastructure we investigate in this paper is cognitive radio-based. Therefore, it is vulnerable to many security attacks pertained to cognitive radio as we listed previously. These attacks are usually initiated by a malicious user who can access the communication infrastructure resources. Through sending false sensing information, the malicious user negatively affects communication reliability and efficiency as the available spectrum for opportunistic access is compromised. Moreover, the malicious user may jam communication channels and result in a DoS situation blocking authorized users. Therefore, access control policies have to be defined to determine who has permission to access the communication infrastructure and sense the spectrum. Only authorized users can be assigned to roles related to spectrum sensing and granted permissions to allow them sense the spectrum and access spectrum databases.

Based on the well-known RBAC model, we introduce our role-based access control mechanism to control communication in smart grid and achieve the two design goals discussed above. Our approach is based on using the notion of roles to control who can access the data being transmitted between role members. In addition, we take advantage of the multi-layer hierarchal structure of the cognitive radio-based communication infrastructure. This Hierarchal structure divides the communication infrastructure into groups (sub-networks), where the users, roles, and permissions of each group can be easily defined and controlled to force the flow of data in a certain direction as shown in Figure 10. A role hierarchy is also defined to ensure a proper data flow between the utility control center and smart meters, as depicted in Figure 11. The most powerful (senior) role is on the top of the hierarchy *i.e.*, utility control center, while the least powerful (junior) role is at the bottom of the hierarchy *i.e.*, smart meters. By definition of RBAC, a senior role inherits permissions assigned for a junior role as inheritance of permissions is transitive.

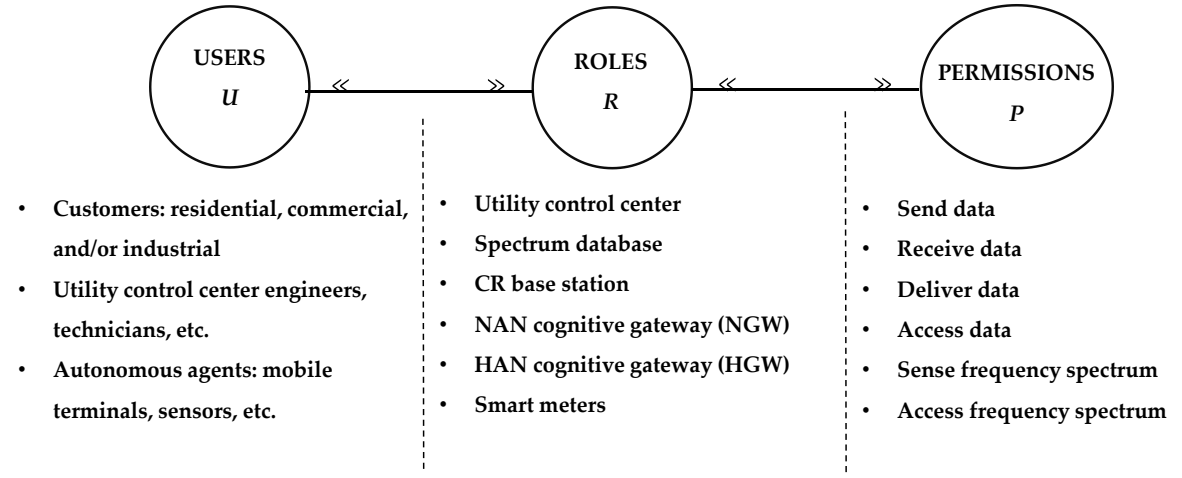

Figure 10. Users, Roles, Permissions Assignment.

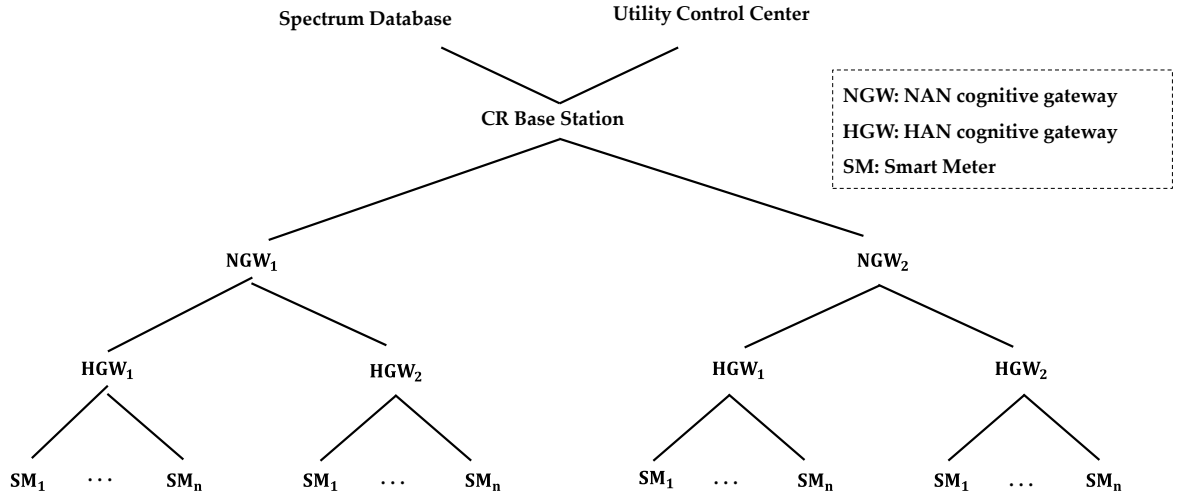

Figure 11. Role Hierarchy.

5.1. Model for Access Control Policies in Cognitive Radio-Based Communication Infrastructure

In this section, we describe the policies for access control in cognitive radio-based communication infrastructure for smart grid. The following assumptions are applied to the proposed model:

- There are three main groups: HAN, NAN, WAN.
- Each group maps each role to a set of permissions based on the sensitivity level of the roles (senior or junior).
- Each group has rules to control who can join the group as sender only.
- Each group has rules to control who can join the group as receiver only.
- Each group has rules to control who can access data.
- Sending, receiving, and delivering data are treated as permissions.
- Access to customers' data is treated as a permission.
- Spectrum sensing is treated as a permission.

Definitions:

- E: a set active system entities such as; users, autonomous agents, *etc*.
- S: a set of sessions
- R: a set of roles
- P: a set of permissions
- T: a set of message types
- UA_R $\subseteq$ U $\times$ R, is many to many User to Role assignment relation
- PA_R $\subseteq$ P $\times$ R, is many to many Permission to Role assignment relation

According to RBAC model, access to the system data is authorized using the following relation:

$$\text{Can} - \text{access} \subseteq \text{R} \times \text{R}$$

The meaning of (x, cr, z) $\in$ can-access is that a system active entity (a subject) can access a data item (an object) if the following hold: The subject is a member of a role (x), and whose membership in x allows him to access z, based on pre-request condition cr. This means that the permission assigned to x's roles must allow access, otherwise access is denied.

In our model, we assume that all security decisions pertain to the administrative activities in RBAC, such as the user-role assignments and permission-role assignments, are handled by a security officer who is located at the control center.

5.2. Enforcement Facilities

One of the most critical issues in using RBAC for enforcing the specified access policies in cognitive-based smart grid environment is to use the concept of a reference monitor (RM), which has been introduced, and extensively discussed by the access control community for years, and has become the ISO standard for access control framework [47]. The RM concept has been considered as the core control mechanism for access and usage of digital information. In classical access control, subjects can access digital objects only through the reference monitor, which is a process inside the trusted computer base that is always running and is a tamper proof.

The following section discusses our conceptual structure of RBAC/CR access control domains based on the reference monitor. In our architecture, a customized version of the well-known ISO reference monitor standard is placed inside the call control center. According to this ISO standard, the reference monitor consists of two facilities: Access Control Enforcement Facility (AEF) and Access Decision Facility (ADF). The AEF and ADF interact with each other in such way that every request by a subject to access an object in the system get intercepted by AEF. The AEF in turn asks the ADF for a decision on whether to approve or disapprove the request, and subsequently the ADF returns either "yes" or "no" as appropriate. The enforcement of this decision takes place at the AEF. Our reference monitor is similar but differs in the details from that of ISO reference monitor. We incorporate the role-based access control to handle the authorization rule. Figure 12 shows the conceptual structure of the RBAC/CR reference monitor. As Figure 12 shows, any request to access any smart grid resource "*i.e.*, user data" is intercepted by the AEF. Before making any decisions, the AEF forwards the request to the ADF, which in turn adheres to the RBAC policy decision of whether to grant or reject the authorization request. RBAC will allow authorization of an active (subject) entity to execute a certain right on a passive (resource) entity only if the subject belongs to a role that RBAC has previously assign that right to. The rest of the decision process by AEF would continue only if RBAC grants authorization. Otherwise, process is stopped and response by the ADF is negative (no authorization). Furthermore, RBAC allow authorization after it tests other decision factors, mainly, hierarchal relationships and constraints. For example, if the condition for granting authorization is met (*i.e.*, the request is within the range of the allowed operating time), then the ADF returns a positive response "Authorize" to the AEF, otherwise request is denied.

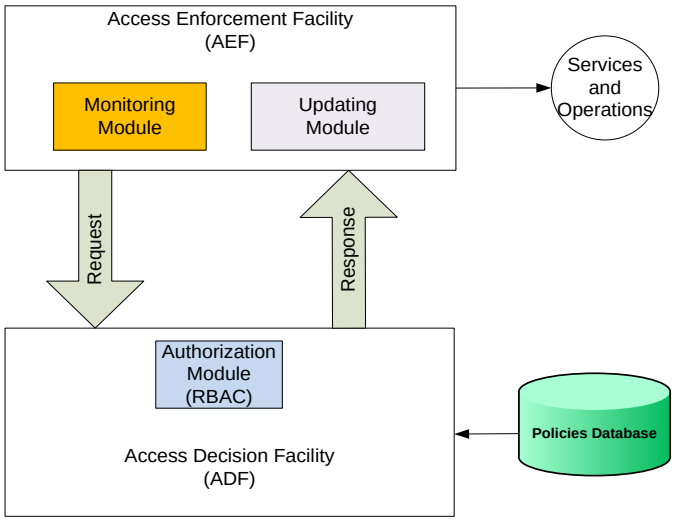

Figure 12. Conceptual Structure for RBAC/CR Reference Monitor.

6. Conclusions and Future Work

In this paper, we surveyed how cognitive radio as a mean of communication can be utilized to serve a smart grid deployment from home area networks to power generation. We discussed the motivations behind this and showed how cognitive radio can be mapped to integrate the different communication networks in smart grid. Furthermore, we defined and discussed various applications in smart grid and how cognitive radio can be used to fulfill their communication requirements. From a security perspective, in this paper, we discussed the information security issues pertained to the use of cognitive radio in a smart grid environment and at different levels and layers and suggested mitigation techniques. Furthermore, we introduced an access control model based on RBAC and integrated it with cognitive radio-based communication in order to specify and enforce access policies for securely utilize the cognitive radio as part of a smart grid communication network. We have demonstrated that our approach can be simple, but yet powerful enough in controlling access to system resources in an environment, which is hierarchically structured such as this. For our future work, we intend to address implementation issues of RBAC in the context of smart grid. We will show how the assignments of users to roles and the assignments of permissions to roles are done. In addition, we will include an architecture, and implementation of such a model and simulate its performance.

Acknowledgments: This research is funded by the UAEU research grant number 31T060.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yu, R.; Zhang, Y.; Gjessing, S.; Yuen, C.; Xie, S.; Guizani, M. Cognitive radio based hierarchical communications infrastructure for smart grid. *IEEE Netw.* **2011**, *25*, 6–14. [CrossRef]
2. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. Available online: http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf (accessed on 10 December 2015).
3. Report of the Unlicensed Devices and Experimental Licenses Working Group Federal Communications Commission Spectrum Policy Task Force November 15, 2002. Available online: https://transition.fcc.gov/sptf/files/E&UWGFinalReport.pdf (accessed on 12 December 2015).
4. General Survey of Radio Frequency Bands—30 MHz to 3 GHz. 2010. Available online: http://www.sharedspectrum.com/wp-content/uploads/2010_0923%20General%20Band%20Survey%20-%2030MHz-to-3GHz.pdf (accessed on 15 November 2015).
5. Metke, A.R.; Ekl, R.L. Security technology for smart grid networks. *IEEE Trans. Smart Grid* **2010**, *1*, 99–107. [CrossRef]
6. Yucek, T.; Arslan, H. A survey of spectrum sensing algorithms for cognitive radio applications. *IEEE Commun. Surv. Tutor.* **2009**, *11*, 116–130. [CrossRef]
7. Ghassemi, A.; Bavarian, S.; Lampe, L. Cognitive radio for smart grid communications. In Proceedings of the First IEEE International Conference on Smart Grid Communications (SmartGridComm), Gaithersburg, MD, USA, 4–6 October 2010; pp. 297–302.
8. Sandhu, R.S.; Coyne, E.J.; Feinstein, H.L.; Youman, C.E. Role-based access control models. *Computer* **1996**, *29*, 38–47. [CrossRef]
9. Yu, R.; Zhong, W.; Xie, S.; Zhang, Y.; Zhang, Y. QoS differential scheduling in cognitive-radio-based smart grid networks: An adaptive dynamic programming approach. *IEEE Trans. Neural Netw. Learn. Syst.* **2016**, *27*, 435–443. [CrossRef] [PubMed]
10. Al Hussien, N.; Abdel-Hafez, M.; Shuaib, K. Collaborative sensing for cognitive radio under log-normal shadowing. In Proceedings of the 2015 IEEE 8th GCC Conference and Exhibition (GCCCE), Muscat, Oman, 1–4 February 2015; pp. 1–6.
11. Erol-Kantarci, M.; Mouftah, H.T. Energy-efficient information and communication infrastructures in the smart grid: A survey on interactions and open issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 179–197. [CrossRef]

12. Li, L.; Zhou, X.; Xu, H.; Li, G.Y.; Wang, D.; Soong, A. Energy-efficient transmission in cognitive radio networks. In Proceedings of the 7th IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 9–12 January 2010; pp. 1–5.
13. Baykas, T.; Kasslin, M.; Cummings, M.; Kang, H.; Kwak, J.; Paine, R.; Reznik, A.; Saeed, R.; Shellhammer, S.J. Developing a standard for TV white space coexistence: Technical challenges and solution approaches. *IEEE Wirel. Commun.* **2012**, *19*, 10–22. [CrossRef]
14. Filin, S.; Baykas, T.; Harada, H.; Kojima, F.; Yano, H. IEEE standard 802.19.1 for TV white space coexistence. *IEEE Commun. Mag. Commun. Stand. Suppl.* **2016**, *54*, 22–26. [CrossRef]
15. Flores, A.B.; Guerra, R.E.; Knightly, E.W.; Ecclesine, P.; Pandey, S. IEEE 802.11af: A standard for TV white space spectrum sharing. *IEEE Commun. Mag.* **2013**, *51*, 92–100. [CrossRef]
16. Khan, A.A.; Rehmani, M.H.; Reisslein, M. Cognitive radio for smart grids: Survey of architectures, spectrum sensing mechanisms, and networking protocols. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 860–898. [CrossRef]
17. Cacciapuoti, A.S.; Caleffi, M.; Marino, F.; Paura, L. Enabling smart grid via TV white space cognitive radio. In Proceedings of the IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 568–572.
18. Gungor, V.C.; Sahin, D. Cognitive radio networks for smart grid applications: A promising technology to overcome spectrum inefficiency. *IEEE Veh. Technol. Mag.* **2012**, *7*, 41–46. [CrossRef]
19. Althunibat, S.; Wang, Q.; Granelli, F. Flexible channel selection mechanism for cognitive radio based last mile smart grid communications. *Ad Hoc Netw.* **2016**, *41*, 47–56. [CrossRef]
20. Ranganathan, R.; Qiu, R.; Hu, Z.; Hou, S.; Pazos-Revilla, M.; Zheng, G.; Chen, Z.; Guo, N. Cognitive radio for smart grid: Theory, algorithms, and security. *Int. J. Digit. Multimed. Broadcast.* **2011**, *2011*. [CrossRef]
21. Cacciapuoti, A.S.; Caleffi, M.; Marino, F.; Paura, L. Sensing-time optimization in cognitive radio enabling Smart Grid. In Proceedings of the Euro Med Telco Conference (EMTC), Naples, Italy, 12–15 November 2014; pp. 1–6.
22. Yang, C.; Fu, Y.; Yang, J. Optimisation of sensing time and transmission time in cognitive radio-based smart grid networks. *Int. J. Electron.* **2016**, *103*, 1098–1111. [CrossRef]
23. Deng, R.; Chen, J.; Cao, X.; Zhang, Y.; Maharjan, S.; Gjessing, S. Sensing-performance tradeoff in cognitive radio enabled Smart Grid. *IEEE Trans. Smart Grid* **2013**, *4*, 302–310. [CrossRef]
24. Li, Q.; Feng, Z.; Li, W.; Gulliver, T.A.; Zhang, P. Joint spatial and temporal spectrum sharing for demand response management in cognitive radio enabled Smart Grid. *IEEE Trans. Smart Grid* **2014**, *5*, 1993–2001. [CrossRef]
25. Schneider, K.; Gerkensmeyer, C.; Kintner-Meyer, M.; Fletcher, R. Impact assessment of plug-in hybrid vehicles on pacific northwest distribution systems. In Proceedings of the IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–6.
26. Kempton, W.; Udo, V.; Huber, K.; Komara, K.; Letendre, S.; Baker, S.; Brunner, D.; Pearre, N. A Test of Vehicle-to-Grid (V2G) for Energy Storage and Frequency Regulation in the PJM System; Results from an Industry-University Research Partnership. November 2008. Available online: http://www.udel.edu/V2G/resources/test-v2g-in-pjm-jan09.pdf (accessed on 20 October 2015).
27. Shuaib, K.; Khalil, I.; Abdel-Hafez, M. Communications in smart grid: A review with performance, reliability and security consideration. *J. Netw.* **2013**, *8*, 1229–1240. [CrossRef]
28. Giani, A.; Bitar, E.; Garcia, M.; McQueen, M.; Khargonekar, P.; Poolla, K. Smart grid data integrity attacks. *IEEE Trans. Smart Grid* **2013**, *4*, 1244–1253. [CrossRef]
29. Kim, T.T.; Poor, H.V. Strategic protection against data injection attacks on power grids. *IEEE Trans. Smart Grid* **2011**, *2*, 326–333. [CrossRef]
30. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE Commun. Surv. Tutor.* **2012**, *14*, 998–1010. [CrossRef]
31. Zhuo, L.; Xiang, L.; Wenye, W.; Wang, C. Review and evaluation of security threats on the communication networks in the smart grid. In Proceedings of the Military Communications Conference, MILCOM, San Jose, CA, USA, 31 October–3 November 2010; pp. 1830–1835.
32. Hlavacek, D.; Chang, J.M. A layered approach to cognitive radio network security: A survey. *Comput. Netw.* **2014**, *75*, 414–436. [CrossRef]

33. Clancy, T.C.; Goergen, N. Security in cognitive radio networks: Threats and mitigation. In Proceedings of the 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008, Singapore, 15–17 May 2008; pp. 1–8.
34. Parvin, S.; Hussain, F.K.; Hussain, O.K.; Han, S.; Tian, B.; Chang, E. Cognitive radio network security: A survey. *J. Netw. Comput. Appl.* **2012**, *35*, 1691–1708. [CrossRef]
35. Bhattacharjee, S.; Sengupta, S.; Chatterjee, M. Vulnerabilities in cognitive radio networks: A survey. *Comput. Commun.* **2013**, *36*, 1387–1398. [CrossRef]
36. El-Hajj, W.; Safa, H.; Guizani, M. Survey of security issues in cognitive radio networks. *J. Internet Technol.* **2011**, *12*, 181–198.
37. Dubey, R.; Sharma, S.; Chouhan, L. Secure and trusted algorithm for cognitive radio network. In Proceedings of the Ninth International Conference on Wireless and Optical Communications Networks (WOCN), Indore, India, 20–22 September 2012; pp. 1–7.
38. Chen, R.; Park, J.-M.; Reed, J.H. Defense against primary user emulation attacks in cognitive radio networks. *IEEE J. Sel. Areas Commun.* **2008**, *26*, 25–37. [CrossRef]
39. Xu, W.; Trappe, W.; Zhang, Y.; Wood, T. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACM International Symposium on Mobile *ad hoc* Networking and Computing, Urbana-Champaign, IL, USA, 25–28 May 2005; pp. 46–57.
40. Xu, W.; Wood, T.; Trappe, W.; Zhang, Y. Channel surfing and spatial retreats: Defenses against wireless denial of service. In Proceedings of the 3rd ACM Workshop on Wireless Security, Philadelphia, PA, USA, 26 September–1 October 2004; pp. 80–89.
41. León, O.; Hernández-Serrano, J.; Soriano, M. Securing cognitive radio networks. *Int. J. Commun. Syst.* **2010**, *23*, 633–652. [CrossRef]
42. Chen, C.; Song, M.; Xin, C.; Alam, M. A robust malicious user detection scheme in cooperative spectrum sensing. In Proceedings of the IEEE Global Communications Conference (GLOBECOM), Anaheim, CA, USA, 3–7 December 2012; pp. 4856–4861.
43. Kaligineedi, P.; Khabbazian, M.; Bhargava, V.K. Secure cooperative sensing techniques for cognitive radio systems. In Proceedings of the IEEE International Conference on Communications, ICC'08, Beijing, China, 19–23 May 2008; pp. 3406–3410.
44. Rawat, A.S.; Anand, P.; Hao, C.; Varshney, P.K. Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks. *IEEE Trans. Signal Process.* **2011**, *59*, 774–786. [CrossRef]
45. Bian, K.; Park, J.-M. MAC-layer misbehaviors in multi-hop cognitive radio networks. In Proceedings of the US-Korea Conference on Science, Technology, and Entrepreneurship (UKC), Teaneck, NJ, USA, 10–13 August 2006; pp. 65–73.
46. Ma, L.; Shen, C.-C.; Ryu, B. Single-radio adaptive channel algorithm for spectrum agile wireless *ad hoc* networks. In Proceedings of the 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, DySPAN, Dublin, Ireland, 17–20 April 2007; pp. 547–558.
47. Sandhu, R.; Park, J. Usage control: A vision for next generation access control. In *Computer Network Security*; Springer: New York, NY, USA, 2003; pp. 17–31.