Cognitive Radio for Smart Grid: A Decentralized Emergency Management Approach

Rajab, Husam; Kamel, Mohammed B. M.; Hamoud, Alaa Khalaf; Farag, Hossam; Cinkler, Tibor; Ligeti, Peter

Published in:
2022 32nd International Telecommunication Networks and Applications Conference (ITNAC)

DOI (link to publication from Publisher):
10.1109/ITNAC55475.2022.9998396

Publication date:
2022

Document Version
Accepted author manuscript, peer reviewed version

Cognitive Radio for Smart Grid: A Decentralized Emergency Management Approach

Husam Rajab *, Mohammed B. M. Kamel †‡§, Alaa Khalaf Hamoud ¶, Hossam Farag ‖,
Tibor Cinkler * and Peter Ligeti †
*Budapest University of Technology and Economics, Budapest, Hungary
†Department of Computer algebra, Eötvös Loránd University, Budapest, Hungary
‡Department of Computer Science, Furtwangen University, Furtwangen, Germany
§Department of Computer Science, University of Kufa, Iraq
¶Department of Computer Science, University of Basrah, Iraq
‖Department of Electronic Systems, Aalborg University, Denmark
husamrajab@tmit.bme.hu, mkamel@inf.elte.hu, alaa.hamoud@uobasrah.edu.iq,
hmf@es.aau.dk, cinkler@tmit.bme.hu, ligetipeter@inf.elte.hu

***Abstract*—With the remarkable advancements in wireless technology, the scarcity of the available spectrum has become more severe. Cognitive Radio (CR) technology is introduced as an emerging solution to alleviate the imbalance between spectrum under-utilization and high spectrum demands. CR enables unlicensed users to opportunistically transmit data through spectrum holes in licensed bands. In the context of smart grids, CR has become a key component to improve communication efficiency and spectrum usage. In particular emergency situations, some nodes are prone to failure, however the network must remain connected to the designated destination. In addition, the generated emergency communication and disaster relief cause high load of traffic that in turn will lead to congestion and affect the network coverage and capacity. In this paper, we introduced an efficient CR-based architecture for Smart Grid networks to enhance capacity coverage and scalability in the disaster and emergency case. The architecture is decentralized and consists of a set of clusters that communicate with each other in a secure way through number of gateways. CRT-based group key management has been used to manage the distribution of keys between gateways. In addition, the asymmetric encryption will assure the confidentiality of transmitted packets.**

***Index Terms*—Cognitive Radio, Smart Grid, Disaster relief, Emergency Communications, Secure communication, Decentralized Architecture.**

I. Introduction

The connotation of the smart grid (SG) is an intelligent control system that adopts a combination of technologies such as sensing, machine learning and network grid to optimize the efficiency power generation and utilization in connected power units [1], [2]. While wired solutions were conventionally adopted for realizing SGs requirements, wireless technology is proved to be a more efficient and flexible alternative, especially in disaster and emergency cases. Substantial research is being achieved in communications technologies for the SG. However, most of the researches by academia and industry have focused on the distribution of the power consumption more than the transmission grid under uncertain conditions. Since SGs require the delivery of a tremendous amount of multimedia surveillance data and control commands, a fundamental limitation is the scarcity of the available frequency spectrum to accommodate the wireless transmissions. In that sense, Cognitive Radio (CR) is considered to be a viable communication solution for SG applications [3].

CR technology offers a promising solution for the existing interference between spectrum under-utilization and the high spectrum demand [4]. Cognitive radio technology enables wireless devices to sense the radio spectrum, determine the state of the frequency channels, and reconfigure the connection parameters to reach the quality-of-service requirements while decreasing their energy consumption [5]. The traditional fixed assignment of the frequency spectrum to particular users, named Primary Users (PUs), causes some assigned bands to remain idle in a specific time or geographical area. CR introduces a dynamic spectrum access scheme called Secondary Users (SUs) are allowed to opportunistically utilize frequency bands that are not used by their PUse, preventing adverse interference [6]. Since PUs have the highest priority to utilize the frequency band, SUs must immediately evacuate the frequency band and jump to another free band.

Spectrum sensing (SS) is a crucial component in CR to enable SUs to intelligently determine the presence of PUs in a given band before starting transmitting their data. Spectrum sensing process is a very power-consuming function and poses significant challenges for implementing seamless communications in large-scale SG deployments. In cooperative spectrum sensing(CSS), multiple CRs cooperate to perform spectrum sensing by sending sensing decisions to a central Fusion Centre (FC) to make the final decision regarding the presence of PUs [7]. Accordingly, novel solutions need to be

This research was partially supported by Project no. TKP2021-NVA-29 has been implemented with the support provided by the Ministry of Innovation and Technology from the National Research, Development and Innovation Fund.

deployed to achieve feasible cognitive radio sensor network (CRSN) based SG communications. The least hardware, for example, employing single radio, and the minimum advanced spectrum sensing functionalities can be used to reduce the energy consumption and decrease the complexity level of the sensing processes [8]. Machine learning algorithms are utilized in different sectors of communication networks such as 5G networks [9] and CRs [10].Machine learning approaches proved their abilities in different fields and used for different purposes such as prediction, classification, clustering, forecasting, and support decision-making [11]. Due to characteristics of the CRs, there is an a need for the abilities of the machine learning approaches, such as the fields of covert data integrity assault, quality of service aware traffic, security of communication, the proactive handoff of the secondary user , and compressing the high frequency measurements . The approach of decentralized emergency management in CRs needs an approach that can assist in communication with heterogeneous technologies or legacy systems, determining the best solutions for communication, reduce the energy consumption, and reduce the interference. Support vector machine (SVM) approach outperformed in reducing the energy consumption by reducing the time of finding PUs, hence improving the result throughput Decision tree approach can also be used for improving the identification accuracy based on single-feature parameter and enhancing the sampling system requirements. Next, the clustering approach is utilized to maximize the network lifetime to achieve bi-channel activity [12]. SVM, Naïve Bayes, and random forest machine learning approaches are used for sensing the spectrum in CRs based on energy, and sample correlation matrix values [13]. Finally, association rules mining approach can be used for blind identification to recognize the length of codes by receiver in a blind environment [14].

In recent years, the use of technology for disaster management has been investigated. According to the "Golden 72 hours" idea, those rescued within the first 72 hours of being caught in a disaster have a good chance of surviving. Every strategy for managing disasters includes: Disaster reduction through mitigation. Preparation: providing people with the tools they need to endure a disaster and reducing the tragedy's effects is response step three. Recovery is step four, which involves returning lives to normal. In this research, the utilization of cognitive radio ad hoc networks (CRAHN) for disaster response scenarios is the main topic. The cognitive radios in CRAHN's nodes allow them to switch their communication spectrum. Without any infrastructure, the nodes naturally organize themselves. These networks are excellent choices for disaster management due to their adaptability, simplicity in deployment, and capacity to utilize the spectrum efficiently.

Frequently, during a disaster, the communication infrastructure may get damaged and cannot be relied on sufficiently. To solve this problem, we proposed a novel architecture based on a Cognitive Radio Ad Hoc Network (CRAHN). The proposed architecture is digitally signed to provide authenticity and integrity. By efficiently utilizing cognitive capabilities, the proposed network is capable of using more extended capacities when more frequency spectrum is available and is less prone to variations in frequency availability and adverse SNR conditions. The transmitted packets between the end nodes securely received. Also, the set of gateways (i.e., the cluster heads) uses a shared key to transfer the data among each other. The CRT-based group key management [15] has been used as a re-keying algorithm in which no trusted authority or centralized key distributor is needed. This method is computationally efficient by slightly increasing the storage complexity, which is critical in mobile devices. The rest of this paper is organized as follows: Section II discuss the related work. Section III presents the system model of the proposed architecture. Section IV shows the system analysis and evaluation. Finally, conclusions are drawn in Section V.

II. Related Work

As declared earlier, SG has bidirectional communication. There are massive communication technologies that are an essential aspect of an SG network due to the extensive coverage range required in SG. It is crucial to study the performance of several access technologies to ascertain the suitable ones for a reliable SG network. That requires an investigative study on performance measurements of access technologies on CR for an SG network. Therefore, communication network architecture in SGs has been discussed in several studies [22].

There are several advantages of using CR in SG. Firstly, the produced energy to represent the transmitted data will be up to hundreds of thousands of terabytes. That represents a critical challenge for any existing communication network to collect, transfer, and store such large-scale data crucial for smart grid network [16]. The value of cognitive radio in the smart grid is the potential to improve the spectrum utilization and communication capacity to support such large data transmissions. Secondly, the smart grid communications structure shall cover home areas, neighborhood areas, and vast areas. Consequently, it is a fundamentally heterogeneous communication network with several complementary technologies, which requires intelligent devices/terminals to control the communications within individual subarea and the connections between various service ranges [17].

The current corrosion of the communication infrastructure cannot endure the modernized SG network [18]. Therefore, upgrade the communication infrastructure of SG is required. That supports heterogeneous and diverse network topology environment. Other notable problems are design challenges that affect the scalability for further smart devices or technologies [19]. Cyber security to mitigating vulnerabilities in SG investigated in [20], and interoperability for communication of various networks and standardization of protocols [19]. The National Institute of Standards and Technology (NIST) has proposed a massive-scale outdoor path loss model in [21].

For last-mile wireless communication in various segments of an SG (WAN, NAN, FAN, and AMI). However, In our proposed architecture, we propose CRAHN applying to the SG network. This is due to the diverging propagation requirements in an SG environment. However, the Log-Normal shadowing path loss model has been the most extensively applied in SGs and Internet of Things (IoT)-based SG [22], [23]. Our contribution in this work is proposing a novel architecture based on a Cognitive Radio Ad Hoc Network (CRAHN) for SG. In addition, our proposal includes a secure communication model for gateways in the SG.

III. Proposed System Architecture

Some of the provided emergency services rely on data communications on public radio networks like GPRS. Periodically in disaster circumstances, even GSM is applied for voice communication among relief workers or as an emergency communication channel [24]. Though, in the cause of the emergency, the public networks may get overloaded. Furthermore, the relief network must be able to manage multimedia signals and has to deal with large, possibly irregular amounts of data. Following the occurrence of a large-scale disaster, e.g., earthquake or a hurricane, there are crucial actions that should be simultaneously carried out to relieve such disasters [25]. The communication infrastructure is naturally destroyed by a disaster, such as base stations crashing, base station to Mobile Switching Center (MSC) connectivity being lost, power generators running out of fuel, mobile phones losing power, and the network experiencing congestion. The existence of infrastructure (such as DHCP servers, directory services, and security servers) is not required for the decentralized operation of the communication protocols. This work suggests a revolutionary CRAHN-based disaster management system. Therefore, it is indicated in this work that nodes functioning in the area will create a CRAHN to facilitate communication. The adoption of CRAHN eliminates the issue of limited spectrum availability by allowing the nodes to operate in the licensed spectrum of other users (primary users).

Based on the conducted discussion in Section II, we propose a CRAHN as the communication infrastructure, so that no infrastructure is required and the network is less vulnerable to local damages. Moreover, if some parts of the network are not functional, the whole network would persist operational.our propose use the dynamically selected gateways that can collect information from their associated cluster. The proposed emergency network architecture consists of three parts: Incident Area Network (IAN), Jurisdiction Area Network (JAN) and External Area Network (EAN) as depicted in Fig. 1.

The IAN serves dense network designed for a specific incident in a small and temporary area. JAN serves as a backbone with which IAN can access general purpose dense networks as well as EAN. Finally, EAN includes all infrastructure networks, including Public Switched Telephone Network (PSTN), Internet, etc. The information related to the disaster

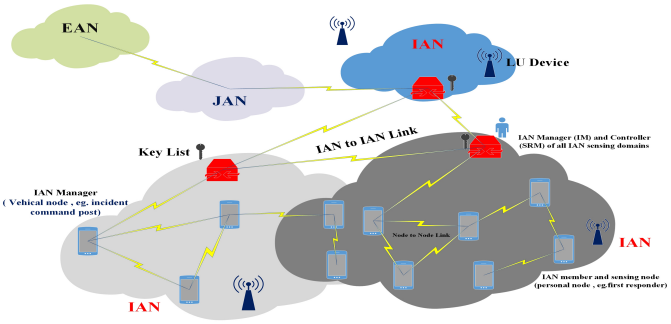

Fig. 1. The proposed CRAHN architecture for SG in Emergency case

is gathered based on either direct observation of people or authorized entities. At the same time, the other part is collected from the Supervisory Control and Data Acquisition (SCADA) systems of the SG [26]. Based on the collected information, there are quick and adequate decisions should be performed to manage disaster circumstances.

Most crisis management systems in use today use manual tables and charts that are updated via verbal communications transmitted over radios. This method, nevertheless, is impractical because a circumstance like that calls for immediate and ongoing situation monitoring. Real-time decision-making help is also necessary. This work suggests that to solve this issue, rescue workers should be equipped with laptops or other computing devices that have real-time applications installed so they can observe the present situation. The following information will be included in the GUI: a) location; b) circumstance, with values of green; yellow; and red; c) timestamp; d) a brief message; and e) a lengthy message. If a rescue worker needs assistance, they can publish a message with the present location, the situation's status as "red," a brief word like "help," and a longer message outlining the assistance needed. The rescuers can use the real-time display to make decisions, take necessary action, etc. The nodes functioning in the disaster area must be able to communicate with one another, and semantic conflicts must be addressed automatically. Situation data is maintained and distributed using a standard XML format to address these interoperability problems. Localized emergency due to a disaster would not commence to the failure of the whole system. The system can still pass information to the nearest disaster control station through functional nodes even if a group of nodes get failed. Furthermore, the nodes are grouped in clusters to surely detect vacant frequency bands. Each cluster compromises the group of nodes that have similar decisions regarding the availability of frequency bands [30].

A data mining approach can be adapted with the disaster control station system for detecting the optimal path and finding the available vacant frequency bands. The data aggregation speed, and energy of transmission are the challenges that can be resolved using such approach of data mining [27]. A hybrid model also can be adapted to group the nodes with adequate

energy to form a connected dominating set to ensure the network validity [28].

To avoid a single point of failure, each element in the network must maintain more than one link to others. The following is a description of the proposed scheme process:

- Step 1: The channel information will be updated through (IAN) given by spectrum sensing system and request the participating nodes $N_c = \{N_1, \ldots, N_m\}$ at the IAN to send, their decisions to the BS (Gateway). Every node $i \in N_c$ will sign its transmitted decision before transmission.
- Step 2: The cluster head (Gateway) receives those local observations from the same cluster (IAN) and then makes a cluster decision according to some fusion function (k-out-of- N).
- Each slot the IM (IAN Manager) signs and broadcasts the network decision on the presence of the primary based on the inputs received from the nodes in the previous slot. The individual decisions obtain according to a k-out-of-N.
- Step 4: Each node in IAN follows the K-out of-N decision distributed by (Gateway) cluster head after verifying it, and in case the two decisions are in agreement, the node increases the counter of the number of correct decisions and reduces the number of users makes sense.

In order to decrease false detection probability, the nodes in separate cluster carry out dispersed sensing. There are two metrics, namely: the probability of detection (P_d) and the false alarm probability (P_f) to estimate the reliability of the final decision for any cognitive system whatever spectrum sensing technique used. Whereas the probability of detection is the probability that the final decision divides the channel as busy when it is working, the probability of false alarm indicates the probability that the final decision classifies the channel as busy when it is free. Both of these measures are very significant and must be taken into consideration when any spectrum sensing algorithm proposed. The value of P_d and P_f depend on several factors including the number of received decisions, and in any system, they must be within specific ranges as shown in (1)

$$\begin{aligned} P_d &= f\,(N, T_s, ...) \geq P_d^{th} \\ P_f &= f\,(N, T_s, ...) \geq P_f^{th}, \end{aligned} \tag{1}$$

Where P_d^{th} is the minimum detection probability that can be accepted, and P_f^{th} is the maximum false alarm probability that can be tolerated. Commonly used fusion rules are OR rule, AND rule, and k-out-of-N rule. OR rule declares the presence of PU on the primary channel if at least one SU claims that the channel is busy. In contrast, under AND rule, the channel is estimated to be busy only if all SUs' sensing results indicate it is occupied. Similarly, the primary channel will be declared as busy by the BS if more than k out of N SUs suggest that the channel is in use under k-out-of-N rule [29]. In fact, OR and AND rules are individual cases of the k-out-of-N rule when $k = 1$ and $k = N$, respectively. Fig. 2 shows the P_d against Signal-to-Noise Ratio (SNR) for the three fusion rules.

The set of gateways $G = \{G_1, \ldots, G_m\}$ that consists of m nodes communicate with each other using a shared key. The used key has to satisfy the following requirements:

- Key Secrecy: The current used key between gateway nodes can only be computed by one of the members of G.
- Forward Secrecy: While the members of G have the information of the current used key, it is hard to find the future used keys for the gateway nodes that leave G.

Depending on the used method of gateway selection, the members of G could be changed (i.e. new nodes could join and existing nodes could leave G). Therefore, after leaving a node the previously used common key has to be changed in order to prevent previous members to get access to the transferred data between gateways. Additionally, the newly computed key between members of G has to satisfy the two security requirements of key secrecy and forward secrecy. CRT-based group key management [**?**], [15] is used to update the used key. In case of key update either as a reason of a node joining or leaving the set G, there are five steps that the members have to follow:

- Step 1: The gateway node $G_1 \in G$,i.e., the first gateway that becomes available and sends a specific signal, chooses two large prime numbers a and r where $a > r$. The r value is a public parameter and will be sent to all group members.
- Step 2: In this step G_1 generates the m_i value for each user $G_i \in G$ such that $a > m_i > r$. All the generated m_i values have to be prime numbers. Then, it computes the value of M by multiplying the m_i values of all the gateway nodes. Finally, the pair (M, m_i) will be shared to the corresponding group members in a secure manner.
- Step 3: Each gateway node $G_i \in G$ selects two prime numbers p_i and $q_i \in Z_r^*$ and computes $\partial i = p_i \times q_i$, where ∂i is used as the modulus for both the public and private keys. Then, it computes Euler's totient function by using (2).

  $$\phi(\partial i) = \phi(p_i) \times \phi(q_i) \tag{2}$$

  The public key values e_i which should be $1 < e_i < \phi(\partial i)$ or $gcd(e_i, \phi(\partial i)) = 1$. The value e_i will be issued as a broadcast message to members of G. Finally, the corresponding private key will be computed that satisfied (3)

  $$e_i d_i \equiv 1 \, mod \, \phi(\partial i) \tag{3}$$

- Step 4: In this step each gateway node G_i computed the group key. The computed key is derived based on the parameters received from the other gateway nodes. The group key K is computed using (4) :

  $$K \equiv \sum_{i=1}^{m} M_i y_i(e_i) \, mod \, M, \tag{4}$$

  where $M_i = M/m_i$ and $M_i y_i e_i, (mod \, m_i)$.

- Step 5: At this step the members of G can transmit encrypted data using key K. The messages can be encrypted using (5) and decrypted using (6)

$$c \equiv (m \times K) \, mod \, M \tag{5}$$

$$S_i \equiv K \, mod \, m_i,$$
$$m \equiv \left((c \, mod \, m_i \times {e_i}^{-1} \, mod \, m_i) mod \, m_i \right)^{s_i \times d_i} \, mod \, \partial i \tag{6}$$

IV. Evaluation

In this section, the overall system has been evaluated. In addition, the security of the proposed model is analyzed.

A. System Evaluation

The k-out-of-N rule is mostly applied, where N is a predefined integer value, $1 \leq k \leq N$. In that rule, the decision upon the spectrum availability is decided as follows.

$$\text{Final decision} = \begin{cases} \text{Busy}, & \sum_{i=1}^{N} u_i \geq K \\ \text{Free}, & \sum_{i=1}^{N} u_i < K, \end{cases} \tag{7}$$

where u_i is the binary decision of the $i-th$ SU.

Several gateway nodes are deployed, acting as routing bridges between the clusters. These nodes communicate in vacant bands that are nor used by their PUs. Members of the IANs have an interface (i.e., gateway node) to the JAN, applying operational command up to the set of all IANs. In each IAN, the gateway nodes could be selected using different methods and parameters, such as connectivity, mobility, and power efficiency [16]–[18]. The JAN is connected to the EAN, e.g., the internet, and acting as a communication network for first responders in emergencies. Besides, the JAN controls the IAN traffic that requires connecting to the EAN. The traffic within different IANs is routed through the JAN. At the same time, the connection between the IAN and the JAN can be based on various radio technologies, such as GSM/UMTS or satellite communication. Fig. 2 shows the comparative performance of several hard decision fusion rules on the probability of detection P_d at FC vs. the average S-channel SNR for CR users. Excellent detection performance improvement for CSS has been observed with increasing average S-channel SNR for all fusion rules (OR, AND, K-out of-N). Higher values of missed detection are obtained with OR fusion rule as compared to other fusion rules such as AND rule and k-out of-N as SNR increases from a low value (-15 dB) to a high value (20 dB).

The Simulation in Figure 3 shows the performance detection of the proposed scheme in both cases when the K-out of-N has been used as the fusion rule and in case of absent of it in the emergency network. Adoption of K-out of-N rule, resulted in increasing the performance of our proposed scheme. The proposed scheme relies on ad-hoc network which allows

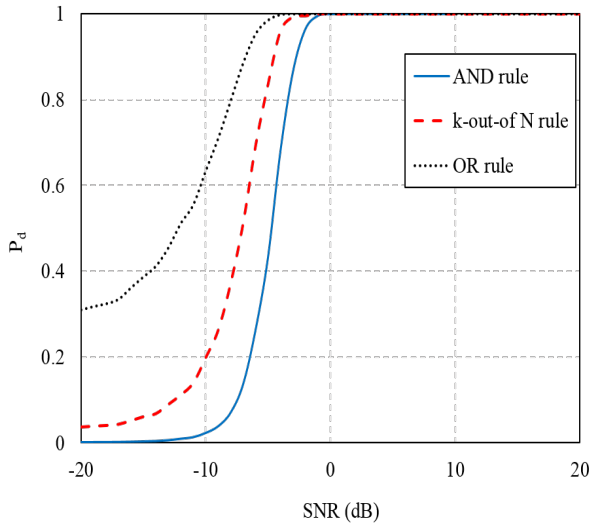

Fig. 2. Probability of detection against SNR of different fusion rules

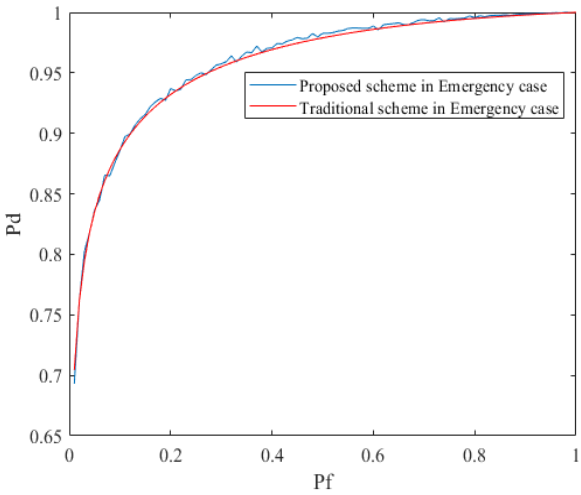

Fig. 3. Probability of Detection (Pd) vs. Probability of False Alarm (Pf)

assigning of a channel to sense to each of the cluster nodes. This assignment is done according to the previously estimated channel occupation statistics.

B. Security Analysis

The architecture assumes two user behaviors. The honest members that always follow the steps and compute/send nothing more and the malicious members that do not send messages according to the predefined steps, but are not able to interrupt the communication. The architecture satisfies two security requirements, namely completeness and gateway key privacy.

- Completeness: Any honest participating member is able to successfully verify the incoming decision distributed by the honest cluster head. This requirement is satisfied by the signed incoming decision and by successfully passing the verification step.
- Gateways key privacy: the used key by gateways for encryption/decryption of the transmitted data is secure against the malicious nodes, and the gateways are able to modify the session key without revealing any private data to the possible malicious members. Since the integer factorization problem of computing the private parameters p and q is considered hard, the completeness is achieved.

V. Conclusion

In this paper, we have presented how the use of CRAHNs as an infrastructure of smart grid communications can simultaneously serve dependable data transfer in smart grid and help disaster management teams to make timely decisions based on smart grid data and other sensible information from the nodes. Moreover, we have analyzed some of the security requirements which the proposed architecture should satisfy during a disaster. This includes the usage of asymmetric encryption for data confidentiality and sender authentication, and CRT-based group key management as a re-keying algorithm of gateway nodes. Based on these requirements, a CRAHN network was proposed. The applied FR in the proposed approach is K-out of-N that detect the spectrum usage based on incoming SUs decisions.

References

[1] R. Moghaddass and J. Wang, "A hierarchical framework for smart grid anomaly detection using large-scale smart meter data," *IEEE Trans. Smart Grids*, vol. 9, no. 6, pp. 5820-5830, Nov. 2018.

[2] Y. Chen, J. Martínez-Ortega, P. Castillejo and L. López, "A homomorphic-based multiple data aggregation scheme for smart grid," *IEEE Sensors J.*, vol. 19, no. 10, pp. 3921-3929, May. 2019.

[3] A. A. Khan, M. H. Rehmani, and M. Reisslein, "Cognitive radio for smart grids: survey of architectures, spectrum sensing mechanisms, and networking protocols," *IEEE Commun. Surv. Tut.*, vol. 18, no. 1, pp. 860-898, Firstquarter 2016.

[4] M. Luís, R. Oliveira, R. Dinis and L. Bernardo, "RF-spectrum opportunities for cognitive radio networks operating over gsm channels," *IEEE Trans. Cognitive Commun. Netw.*, vol. 3, no. 4, pp. 731-739, Dec. 2017.

[5] B. Li, B. Zhang, J. Guo, and J. Yao, "Study on cognitive radio based wireless access communication of power line and substation monitoring system of smart grid," in 2012 International Conference on Computer Science and Service System, pp. 1146–1149, Nanjing, China, August 2012.

[6] F. Awin, E. Abdel-Raheem and K. Tepe, "Blind spectrum sensing approaches for Interweaved cognitive radio system: a tutorial and short course," *IEEE Commun. Surv. Tut.*, vol. 21, no. 1, pp. 238-259, Firstquarter 2019.

[7] H. M. Farag and E. M. Mohamed, "Soft decision cooperative spectrum sensing with noise uncertainty reduction," *Pervasive and Mobile Computing J.*, vol. 35, no. 2, pp. 146-164, Feb. 2017.

[8] Besher, K. M.; Nieto-Hipolito, J. I.; Vazquez, B. M.; Buenrostro, M. R. SenPUI: Solutions for Sensing and Primary User Interference in Cognitive Radio Implementation of a Wireless Sensor Network. Wireless Communications and Mobile Computing. 2019.

[9] Najm, Ihab Ahmed, et al. "Machine learning prediction approach to enhance congestion control in 5G IoT environment." *Electronics*, vol. 8, no. 6, pp. 607, 2019.

[10] L. Xixiang, H. Li, and B. Wang. "Group key agreement for secure group communication in dynamic peer systems," *J. Parallel Distrib. Comput.*, vol. 72, no. 10, pp. 1195-1200, 2012.

[11] Bertoli, Gustavo De Carvalho, et al. "An end-to-end framework for machine learning-based network intrusion detection system." IEEE Access 9 (2021): 106790-106805.

[12] Sun, X.; Su, S.; Zuo, Z.; Guo, X.; Tan, X. Modulation Classification Using Compressed Sensing and Decision Tree–Support Vector Machine in Cognitive Radio System. Sensors 2020, 20, 1438. https://doi.org/10.3390/s20051438.

[13] R. Prajapat, R. N. Yadav and R. Misra, "Energy-Efficient k-Hop Clustering in Cognitive Radio Sensor Network for Internet of Things," in IEEE Internet of Things Journal, vol. 8, no. 17, pp. 13593-13607, 1 Sept.1, 2021, doi: 10.1109/JIOT.2021.3065691.

[14] Krishnan, Gauri, et al. "Eigenvalue-Based Spectrum Sensing in Cognitive Radio Networks Using Supervised Learning." 2021 10th International Conference on Internet of Everything, Microwave Engineering, Communication and Networks (IEMECON). IEEE, 2021.

[15] Dai, L., Ren, C. Guo, J. "Blind Reconstruction of Binary Linear Block Codes Based on Association Rules Mining." Circuits Syst Signal Process 40, pp. 4144–4168, 2021.

[16] V. Dehalwar, M. Kolhe, and S. Kolhe, "Cognitive radio application for smart grid," *Int. J. Smart Grid Clean Energy*, vol. 1, pp.79-84, 2012.

[17] Aroua, S. Spectrum resource assignment in cognitive radio sensor networks for smart grids. Doctoral dissertation, Université de La Rochelle, 2018. Online: https://tel.archives-ouvertes.fr/tel-02009821/document Accessed: 11-02-2020

[18] Khan AA, Rehmani MH, Reisslein M. Cognitive radio for smart grids: survey of architectures, spectrum sensing mechanisms, and networking protocols. IEEE Commun Surv Tutor. 2016;18(1):860-898.

[19] Rekik S, Baccour N, Jmaiel M, Drira K. Wireless sensor network based smart grid communications: challenges, protocol optimizations,and validation platforms. Wirel Pers Commun. 2017;95(4):4025-4047.

[20] Basharat M, Ejaz W, Ahmed SH. Securing cognitive radio enabled smart grid systems against cyber attacks. Paper presented at 2015 First International Conference on Anti-Cybercrime (ICACC); 2015; Riyadh, Saudi Arabia.

[21] Cypher D. NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications. Gaithersburg, MD: Advanced Network Technologies Division, NIST; 2014. NISTIR 7761, Rev. 1.

[22] Sandoval RM, Garcia-Sanchez AJ, Garcia-Haro J. Improving RSSI-based path-loss models accuracy for critical infrastructures: a smart grid substation case-study. IEEE Trans Ind Inform. 2018;14(5):2230-2240.

[23] Sandoval R, Garcia-Sanchez AJ, Garcia-Sanchez F, Garcia-Haro J. Evaluating the more suitable ISM frequency band for IoT-based smart grids: a quantitative study of 915 MHz vs. 2400 MHz. Sensors. 2017;17(1):76.

[24] M. B. M. Kamel and L. E. George, "Secure model for sms exchange over gsm," *Int. J. Comput. Netw. and Inf. Security*, vol. 8, no. 1, pp. 1-8, Jan. 2016.

[25] N. Uchida, K. Takahata and Y. Shibata, "Cognitive wireless network for large scale disaster," In *Proc. Int. Conf. on Intelligent Netw. and Collaborative Syst.*, Nov. 2011, pp. 362-366.

[26] Y. Zhang, L. Wang, Y. Xiang and C. Ten, "Power system reliability evaluation with scada cybersecurity considerations," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1707-1721, Jul. 2015.

[27] Basappa, Prapulla S., Shobha Gangadhar, and Tiptur Chandrashekar Thanuja. "Energy-efficient data-aggregation for optimizing quality of service using mobile agents in wireless sensor network." International Journal of Electrical Computer Engineering (2088-8708) 12.4 (2022).

[28] Saravana Kumar, N.M., Suryaprabha, E. and Hariprasath, K. Machine learning based hybrid model for energy efficient secured transmission in wireless sensor networks. J Ambient Intell Human Comput 13, 887–902 (2022). https://doi.org/10.1007/s12652-021-02946-y.

[29] H. M. Farag and E. M. Mohamed, "Soft decision cooperative spectrum sensing with noise uncertainty reduction," *Pervasive and Mobile Computing J.*, vol. 35, no. 2, pp. 146-164, Feb. 2017.

[30] H. N. Saad, and M. B. M. Kamel, "Weight Analysis for Weighted Cluster Algorithms in Mobile Ad-Hoc Network," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 14, pp. 3352-3364, 2017.