International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-2, Issue-6, 2018.
www.ijirtm.com *ISSN: 2581-3404 (Online)*

Secure and Energy Efficient Spectrum Sensing for Cognitive Radio Sensor Network

Shujaat Khan[1], Prof. Jitendra Mishra[2]
[1]M. Tech Scholar, Department of EC, PIES, Bhopal (India)
[2]Head & Professor, Department of EC, PIES, Bhopal (India)
[1]shujaatsk@gmail.com, [2]jitendra.mishra260@gmail.com

ABSTRACT
Wireless sensor network (WSN) has emerged as one of the most promising technologies for the future. This has been enabled by advances in technology and availability of small, inexpensive, and smart sensors resulting in cost effective and easily deployable WSNs. Thus, the next generation of wireless sensor networks is the cognitive wireless sensor networks (CWSNs). Cognitive radio has been proposed as a promising technology to resolve the spectrum scarcity problem by dynamically exploiting underutilized spectrum bands. Wireless sensor networks operating in the license free spectrum suffer from uncontrolled interference as those spectrum bands become increasingly crowded. With the rapid development of cognitive radio technology, increasing attention has been paid to securing spectrum sensing against SSDF attacks. In this article we proposed a new method for the attack detection in cognitive radio sensor network and improve the performance of system using accuracy, attack probability and detection speed evaluation parameters etc.

Keywords: Cognitive Radio, Cognitive Radio Sensor Networks, SSDF, Attack, Spectrum sensing.

INTRODUCTION

As the explosion of wireless devices and services make the unlicensed spectrum increasingly crowded, traditional sensor networks operating on the unlicensed spectrum may suffer from severe interference caused by the nearby applications working on the same spectrum band. This situation is getting worse with our proceeding to the Internet of- Things era [1].

Due to worldwide growth of the number of mobile terminals and the request of higher data rates, a tremendous increase of the energy consumption of the telecommunications industry has been recently reported, which has a significant environmental impact. From the mobile terminals' perspective, given the limitation on energy resources, energy consumption poses a main concern. Thus, energy efficiency has recently triggered a significant amount of research [1]. Indeed, energy efficiency is receiving a higher priority for some wireless systems and becomes a pressing need for their operation. A notable example is Cognitive Radio (CR) [10].

WSN technology offers numerous advantages over conventional networking solutions, such as, lower costs, scalability, reliability, accuracy, flexibility, and ease of deployment that enable their use in a wide range of diverse applications. With advancements in technology and sensors getting smarter, smaller, and cheaper, billions of wireless sensors are being deployed in numerous applications. Some of the potential application domains are military, environment, healthcare, and security. In military, sensor nodes can be used to detect, locate or track enemy movements. In case of natural disasters, sensor nodes can sense and detect the environment to forecast disasters in advance. In health care, sensor nodes can help in monitoring a patient's health. In security, sensors

can offer vigilant surveillance and increase alertness to potential terrorist at tacks. It will not be farfetched to say that eventually WSNs will enable the automatic monitoring of forest fires, avalanches, hurricanes, failure of country wide utility equipment, traffic, hospitals, etc [3].

Trust and reputation based approaches are the most widely studied techniques in this approach, The main idea of these approaches is to update the trust values of spectrum sensing nodes according to their historical sensing behaviors, and design weighted decision making strategies to resist SSDF attacks based on the evaluated trust values [1]. Spectrum sensing is a daunting task; however, it is crucial to the performance of the cognitive radio network (CRN).

Spectrum sensing of a single CR user becomes unreliable due to factors such as shadowing, fading and time-diversity of wireless channels. Cooperative spectrum sensing is used to reliably sense the spectrum in the above scenarios. In cooperative spectrum sensing, a slotted frame structure is used to sense the spectrum and transmit data. Spectrum is sensed continuously by cooperating CR users in the first portion of the slotted frame-structure, which is known as sensing slot. The remaining time slot, known as transmission slot, is utilized to transmit data. As the sensing time increases, the spectrum sensing becomes more reliable; however, this occurs at the expense of less time for actual data transmission and vice versa [6].

In the spectrum sharing stage, power consumption is mainly due to SUs' data transmission. If all SUs adopt the highest transmission power, they would interfere with each other, and little throughput could be achieved, leading to extremely low efficiency. Therefore, the energy efficiency problem in spectrum sharing is essentially a resource allocation problem. There are centralized and distributed scheduling techniques to resolve the utility maximization problem of resource allocation in SUs' spectrum sharing. As discussed earlier, compared to centralized scheduling, which requires a scheduler to know complete channel state information of the whole secondary network, the decentralized technique based on game theoretical analysis is more effective and practical, which aims at achieving an energy-efficient equilibrium among SUs [4].

WSNs and CWSNs are two types of sensor networks that have a number of common characteristics. They consist of miniature devices, called motes or sensors that are severe resource constrained devices in terms of memory, processing, and energy. They usually do not perform any computation on the data they collect; they just forward this information to much more powerful devices (called sinks) for further processing. The communication medium used for both WSNs and CWSNs has a broadcast nature and the used spectrum is split into several channels, depending on the protocol used. For example, there are up to 16 available channels for the IEEE 802.15.4 in the 2.4GHz frequency band [5].

A diverse range of vulnerabilities are exploited by adversaries who can have several incentives, for example, network disruption, information theft, and so forth. In general, there are two types of attackers : (i) external attackers that are not authorized participants of the sensor network and (ii) internal attackers that have compromised a legitimate sensor and use it to launch attacks in the network. Furthermore, attackers can be classified into passive and active. Passive attackers monitor network traffic without interfering with it. Their aim is to eavesdrop on the exchanged information and to acquire private data or to infer about information-sensitive applications that execute in the sensors. Active attackers disrupt network operation by launching several types of attacks that cause DoS (denial of service) in the WSN [5].

The rest of this paper is organized as follows in the first section we describe an introduction of about the Cognitive Radio Sensor Networks. In section II we discuss about the application domain and deployment model. In section III we discuss about the comparative result study for the Spectrum sensing in Cognitive Radio Sensor Networks, finally in section V we conclude the about our paper.

II APPLICATION DOMAINS AND DEPLOYMENTS

WSNs have been adopted in a large number of diverse application domains. It is envisioned that in future everyday objects will be embedded with sensors to make them smart. Smart objects can explore their environment, communicate with other smart objects, and interact with humans. Taxonomy of WSN applications is shown in below figure In general, WSN applications can be of two types: monitoring and tracking. As shown in the taxonomy (Below figure), the leading application domains of WSNs include military and crime prevention, environment, health (Body Area Networks), industry and agriculture, and urbanization and infrastructure. Military operations involving force protection with unattended ground sensors formed into intelligent networks around forward operating bases are receiving much attention.

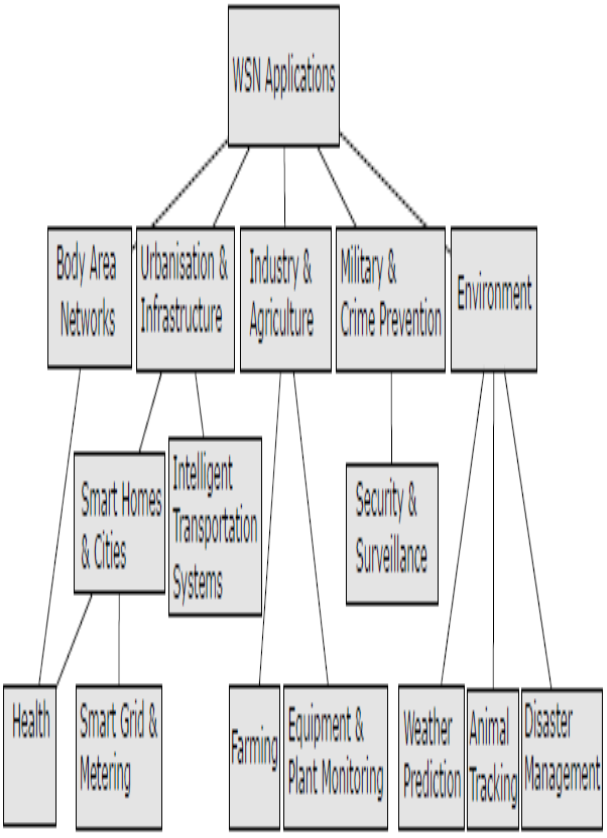

Fig. 1: Taxonomy of WSN applications [3].

III EXPERIMENTAL RESULTS DISCUSSION

In this section, we validate our theoretical analysis and evaluate the performance of our proposed schemes. We setup a CRSN with number of licensed channel sensor nodes. The network process is divided into a sequence of time periods. At the beginning of each time period, the sink randomly chooses a number of sensor nodes to sense a licensed channel.

In this section we compare our proposed method with existing method for the attack probability and detection ration and our proposed methods shows better results than previous methods. Proposed methods improve the accuracy using more attack detection in a cognitive radio sensor networks.

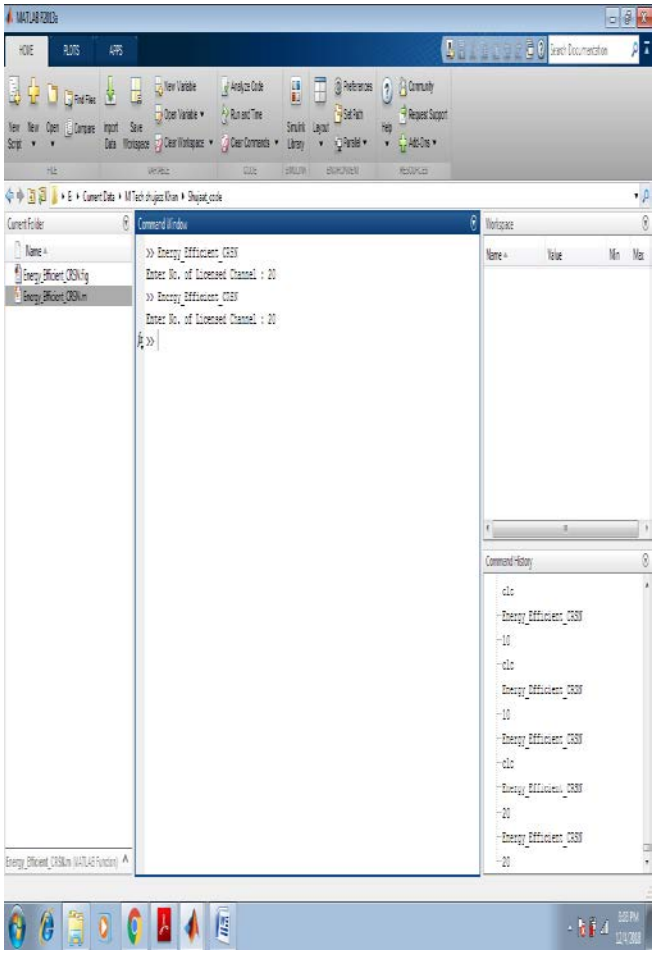

Fig. 2: Figure shows that the initally enviornemnt setup for the experimental procedure.

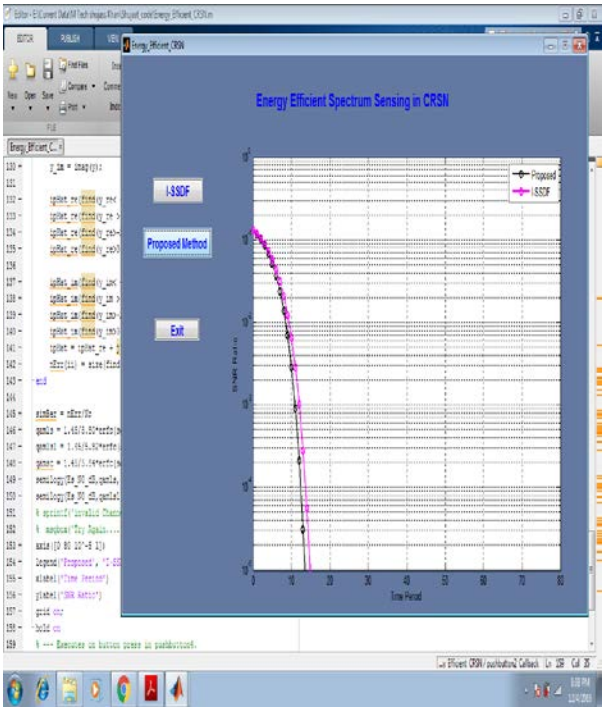

Fig. 3: Figure shows that the compartive experomental result for the proposed work.

IV CONCLUSION

In this context, the WSNs will be playing a significant role in the everyday life of people, and thus their security is of great importance. This explosion in the number of wireless sensing and actuating devices in city areas together with the continuous installation of many (public and private) wireless access networks in these areas has resulted in congestion in the unlicensed spectrum bands that are used for both WSNs and Wi-Fi. In this paper we proposed a model for attack detection in wireless sensor networks and compare with previous methods our methods shows better results.

REFERENCES:-

[1] Ju Ren, Yaoxue Zhang, Qiang Ye, Kan Yang, Kuan Zhang, Xuemin (Sherman) Shen, "Exploiting Secure and Energy-Efficient Collaborative Spectrum Sensing for Cognitive Radio Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 15, NO. 10, OCTOBER 2016 pp 6813-6827.

[2] Ju Ren, Yaoxue Zhang, Ning Zhang, Deyu Zhang, Xuemin Shen, "Dynamic Channel Access to Improve Energy Efficiency in Cognitive Radio Sensor Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 15, NO. 5, MAY 2016 pp 3143-3157.

[3] Priyanka Rawat, Kamal Deep Singh, Hakima Chaouchi, Jean Marie Bonnin, "Wireless Sensor Networks: recent developments and potential synergies", Article in The Journal of Supercomputing · April 2013.

[4] Chunxiao Jiang, Haijun Zhang, Yong Ren, and Hsiao-Hwa Chen, "Energy-Efficient Non-Cooperative Cognitive Radio Networks: Micro, Meso, and Macro Views", IEEE Communications Magazine, 2014. pp 14-21.

[5] Alexandros Fragkiadakis, Vangelis Angelakis, Elias Z. Tragos, "Securing Cognitive Wireless Sensor Networks: A Survey Alexandros", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks pp 1-12.

[6] Hurmat Ali Shah, Muhammad Usman, and Insoo Koo, "Bioinformatics-Inspired Quantized Hard Combination-Based Abnormality Detection for Cooperative Spectrum Sensing in Cognitive Radio Networks", IEEE SENSORS JOURNAL, VOL. 15, NO. 4, APRIL 2015, pp 2324-2335.

[7] Yi Liu, Shengli Xie, Rong Yu, Yan Zhang, Xi Zhang, Chau Yuen, "Exploiting temporal and spatial diversities for spectrum sensing and access in cognitive vehicular networks", WIRELESS COMMUNICATIONS AND MOBILE COMPUTING Wirel. Commun. Mob. Comput. 2015, pp 2079–2094.

[8] Waleed Ejaz, Muhammad Naeem, Adnan Shahid, Alagan Anpalagan, Minho Jo, "Efficient Energy Management for the Internet of Things in Smart Cities", IEEE 2017, pp 84-90.

[9] Oladayo Bello, Sherali Zeadally, "Intelligent Device-to-Device Communication in the Internet

of Things", IEEE SYSTEMS JOURNAL, 2014. pp 1-11.

[10] Saud Althunibat , Marco Di Renzo, Fabrizio Granelli, "Towards Energy-E_cient Cooperative Spectrum Sensing for Cognitive Radio Networks-An Overview", Article in Telecommunication Systems · May 2014, pp 1-25.

[11] MINHO JO, TARAS MAKSYMYUK, BOHDAN STRYKHALYUK, AND CHOONG-HO CHO, "DEVICE-TO-DEVICE-BASED HETEROGENEOUS RADIO ACCESS NETWORK ARCHITECTURE FOR MOBILE CLOUD COMPUTING", IEEE 2015, pp 50-59.

[12] Melike Erol-Kantarci, Hussein T. Mouftah, "Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues", IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 1, FIRST QUARTER 2015, pp 179-198.

[13] Bukhari, SHR, Rehmani, MH and Siraj, "A Survey of Channel Bonding for Wireless Networks and Guidelines of Channel Bonding for Futuristic Cognitive Radio Sensor Networks". IEEE Communications Surveys and Tutorials, 2016, pp. 924-948.

[14] Derrick Wing Kwan Ng, Ernest S. Lo, Robert Schober, "Multi-Objective Resource Allocation for Secure Communication in Cognitive Radio Networks with Wireless Information and Power Transfer", IEEE 2013, pp 1-18.

[15] Athar Ali Khan, Mubashir Husain Rehmani, Martin Reisslein, "Cognitive Radio for Smart Grids: Survey of Architectures, Spectrum Sensing Mechanisms, and Networking Protocols", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 1, FIRST QUARTER 2016, pp 860-898.

Shujaat Khan received his Bachelor`s degree in Electronics & Comunication Engineering, MIT, Bhopal, M.P., in 2011. Currently he is pursuing Master of Technology Degree in Electronics & comunication (Digital Communication) from PIES, (RGPV), Bhopal, Madhya Pradesh India. His research area include Wireless sesnor networks.

Mr. Jitendra Kumar Mishra he is Associate Professor and Head of the Department of Electronics and communication in PIES, Bhopal (RGPV). His received Master of Technology and Bachelor's of engineering respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 10 years of teaching experience and publish 30+ papers in International journals, conferences etc. His areas of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Image Processing etc.