IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 4 Issue 9, September 2017
ISSN (Online) 2348 – 7968 | Impact Factor (2016) – 5.264
www.ijiset.com

Energy Efficient Protocol for Cooperative Spectrum Sensing Cognitive Radio Networks

Rajesh D. Kadu[1], Dr. Pravin P. Karde[2] and Dr. V. M. Thakare[3]

[1] Research Scholar, SGB Amravati University, Amravati, India

[2] Information Technology Departments Government Polytechnic, Amravati, India

[3] P. G. Department of Computer Science, SGB Amravati University, Amravati, India

Abstract

In static allocation of spectrum, most of the spectrum remains underutilized by primary users (PUs). However, with ever growing wireless applications, the spectrum demand is also increasing. The underutilized spectrum by PUs can be used by unlicensed secondary users (SUs). In dynamic spectrum access (DSA), Cognitive radio (CR) nodes or SUs sense the spectrum to know PU is present in spectrum band or not. If PU is not utilizing the spectrum then this vacant band is utilized by SUs. In this way spectrum shortage problem can be solved. In cognitive radio networks (CRNs), unlicensed users can use idle spectrum with no interference to PU. As many wireless devices work simultaneously in CRNs, the energy spent by them is also important. The overall network life time needs to be improved for the better network performance. In this paper we discuss the various security attacks in CRNs which degrades the performance and propose the protocol to improve the energy efficiency of the network.

Keywords: *PUEA, SSDF, jamming attack, CSS, CRN, energy efficiency*

1. Introduction

In CRN, PUs does not make full utilization of the spectrum allocated to them. Most of the spectrum remains underutilized [1]. SUs sense the spectrum for its availability. If the PU is currently not using allocated spectrum then this vacant band is utilized by SUs. In this way, optimum utilization of the spectrum is carried out. All the SUs use the spectrum that is not used by PU in opportunistic manner called as dynamic spectrum access (DSA). As most of the wireless devices in CRNs are battery powered, their energy efficiency is important. If any one of the node in CRNs runs out of battery power then it cannot be used as intermediate node along the path from source node to destination node [2]. Spectrum sensing and quality transmission without interference with PU is major challenge in CRNs. The good performance of the network indicates better throughput which is number of bits delivered per second. The partially observable Markov decision process (POMDP) is used in [3] and [4] to improve the throughput of SU by applying optimal sensing duration. As per battery capacity constraint, idle or sensing action is scheduled. CR users use the residual energy in case of energy constraints. In case of more residual energy, CR users can sense and access the spectrum although channel conditions are not good.

If more number of malicious users (MUs) is present in network then they have significant effect on decision reliability, consumed energy and throughput. These MUs can launch many attacks in CRN such as primary user emulation attack (PUEA), spectrum sensing data falsification (SSDF) attack and jamming attack. These attacks degrade the network performance. Hence, it is important to identify the MUs in network and eliminate them. In spectrum sensing process, communication is established among SUs and also between SUs and fusion center (FC). The certain amount of energy is consumed by user nodes while transmitting the data.

2. Related Work

In [5], authors proposed energy-efficient based transmission duration design and power allocation methods. The joint optimization between medium access control (MAC) and physical layer is considered to improve the energy efficiency. The proposed scheme achieves maximum energy efficiency along with expected throughput. In order to maximize the energy efficiency of the wireless sensor network that makes use of the CR techniques, a constrained optimization problem is proposed in [6]. The proposed optimization problem is formulated as fractional programming problem which then transformed in equivalent concave optimization problem using Charnes-Cooper transformation. Then ε-optimal algorithm is used to obtained optimal solution for power allocation in energy efficient CRNs.

Saud Althunibat et al. [7] considered the effects of MUs present in CRN on its energy efficiency. The trade of between energy efficiency and security is taken in to consideration and optimal number of security bits derived to maximize the energy efficiency. The proposed symmetric cryptographic mechanism minimizes the effects of MUs on energy efficiency. In [8] authors considered the cyclostationary spectrum sensing in CRNs and used compressed spectrum sensing to improve the energy efficiency. The proposed scheme gives good detection performance for the given false alarm rate.

B. Senthil kumar and S. K. Srivatsa [9] proposed the artificial intelligence based spectrum sensing approach. The proposed approach includes spectrum segmentation, spectrum sensing and malicious user detection. In order to identify the vacant band or spectrum hole, Hybrid ANFIS method is used. With the proposed approach, the errors in spectrum sensing are minimized by fulfilling the requirements of spectrum sensing. In [10] authors discussed the methods such as gradient based iteration algorithm, water filling factors aided search method, efficient barrier method and extreme value theory to improve the energy efficiency. The performance evaluation of these methods is carried out with parameters energy efficiency and transmits power.

Shaowei Wang and Chonggang Wang [11] considered the OFDM base CRNs and addressed the joint improvement in energy efficiency and spectrum efficiency. In order to optimize the energy efficiency and spectrum efficiency at the same time, authors devised a multi-objective resource allocation problem. Fourat Haider et al. [12] considered the interference-tolerant CR networks to study spectral and energy efficiency. The energy required at link level is analyzed to gain particular spectral efficiency for CR channels under two types of power constraints. The study is also carried out at system level for spectral and energy efficiency of CR networks that shares spectrum with indoor network. It is shown that, by using CR technology, cellular operators can share their spectrum in opportunistic manner to improve performance of the network.

Efe F. Orumwense et al. [13] considered design and operation of CRNs in order to give analysis of energy efficiency metrics. The component level, equipment level, and network level metrics are considered. Satyam Agarwal and Swades De [14] proposed three protocols for energy efficient DSA for CRNs. The protocols support for maximum utilization of channel by SUs without degradation of PU performance. In this approach, performance of PU does not degrade below set threshold.
In [15] authors considered spectrum sharing and sensing system in time varying channels. The evaluation of energy efficiency is carried out by reducing the transmission power at secondary transmitter. This evaluation is carried out for both of schemes, spectrum sharing and sensing. It is observed that power minimization improves energy efficiency.

3. Spectrum Sensing Schemes

In CRNs, if PU is not using the spectrum then SUs can use it. The SUs have to sense the spectrum to check whether PU is transmitting or not. This spectrum sensing is carried out individually by each SU or in cooperative manner. In individual spectrum sensing (ISS), each SU independently takes the decision about presence or absence of PU in spectrum band. Due signal fading and shadowing effects, the ISS scheme is inaccurate and not reliable.

Hence, cooperative spectrum sensing (CSS) is more preferable than ISS scheme. It is more accurate and reliable. In CSS scheme, all the SUs sense the spectrum in cooperative manner and at the end of sensing period; send their spectrum sensing reports to fusion center (FC). The FC then takes decision about presence or absence of PU based on received spectrum sensing results from SUs. FC executes fusion process based on some fusion rules and takes final decision. FC then broadcast the result to all the SUs which were involved in spectrum sensing.

CSS schemes are categorized in two classes. These are centralized CSS and distributed CSS. In centralized CSS, if CRNs are centralized then separate FC is present to execute fusion process. In case of distributed CRNs, if centralized CSS scheme is used then any one SU can be used to play the role of FC. In distributed CRNs, if distributed CSS scheme is used then all the SUs share their spectrum sensing results between them and each SU executes fusion process based on received results.

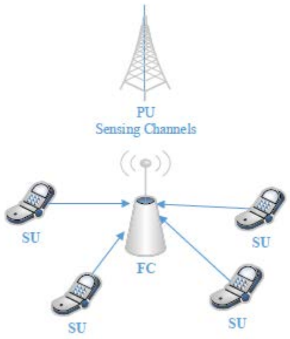

Fig. 1 : Centralized CSS

Fig. 2 : Distributed CSS

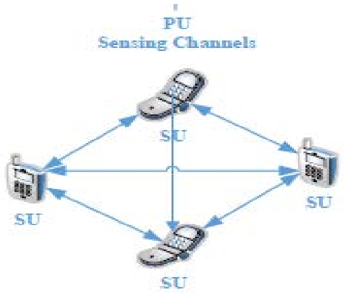

Fig. 1 and Fig. 2 shows centralized and distributed CSS respectively.

4. Attacks in CSS CRNs

While CSS is more accurate and reliable, it is more vulnerable to many attacks. Some of the genuine SUs can behave maliciously to launch the attacks such as primary user emulation attack (PUEA), spectrum sensing data falsification (SSDF) attack and jamming attack. As MUs in network increases, it impacts more on decision reliability, consumed energy and throughput. When these attacks are launched by MUs then network performance also degrades. It also affects the energy efficiency of the nodes.

4.1 PUEA: In this attack, some of misbehaving SUs can transmit signals which are having similar characteristics like PU signals. The main intension behind this attack is to make genuine SUs to believe into genuine PU is present in band but actually it is not. If attacker is selfish then it uses vacant band for transmission. In this case, genuine or good SUs will leave the band as they believe real PU is present. If attacker is malicious then simply there will be denial of service to good SUs.

4.2 SSDF Attack: In SSDF attack, some of the MUs send false reports of spectrum sensing to FC in order to have an effect on the decision process of FC. FC takes decision by using some fusion rules. Based on the outcome, presence or absence of PU is decided by FC.

4.3 Jamming Attack: In this attack, the intention of the attacker or jammer is to block the communication channels. This attack can be launched on both physical layer and MAC layer. In MAC layer, common control channel (CCC) is blocked by sending the bogus packets continuously. In jamming attack, communication of the SUs is blocked.

5. Simulation Environment and Results

The proposed protocol is simulated in NS-2 by considering 250 meter coverage area for nodes as their transmission range. The simulation time considered is 200 seconds and total number of users considered is 50. The network area considered is 800 X 800. Initial energy for each node is 100 Jules. Each node can send and receive 512 bytes of data per second. Hence the packet size is 512 byte. The proposed protocol also establishes the secure path among nodes during communication. Hence, it minimizes link disconnection thereby minimizing the transmission control packets. Therefore energy of the nodes is saved by controlling unnecessary channel detection.

The protocol provides authentication for SUs working in network. Authentication is provided by white space server. As nodes are active in network, it consumes some amount of energy. The average energy consumption (AEC) is considered to measure the energy consumption. It is the ratio of total energy consumed and total number of nodes. The average residual energy (ARE) is the ratio of total residual energy and total number of nodes. Threshold value is maintained for energy. Each node calculates its current energy level with threshold to extend the network life time.

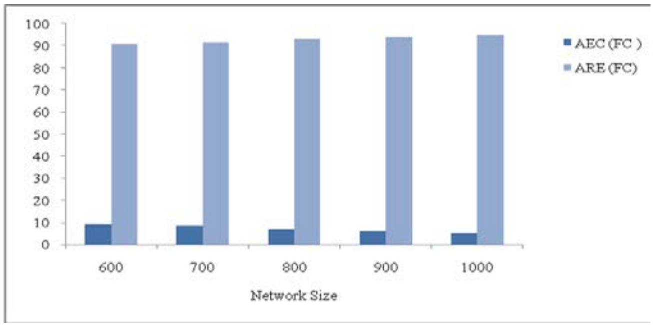

Fig. 3: AEC and ARE for increasing network size (FC)

Above re residual energy at FC and white space server (WSS) shows good performance and energy efficiency of the protocol. Fig. 3 shows results at FC and fig. 4 shows results obtained at WSS for increasing size of network. As network size increases AEC decreases at both FC and WSS.

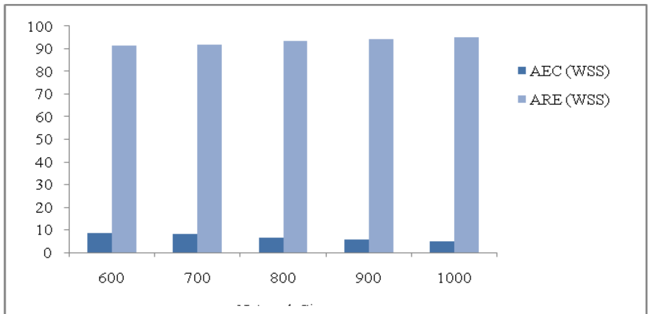

Fig. 4: AEC and ARE for increasing network size (WSS)

As number of users in network increases, traffic also increase. Following results in fig. 5 and fig. 4 shows better performance.

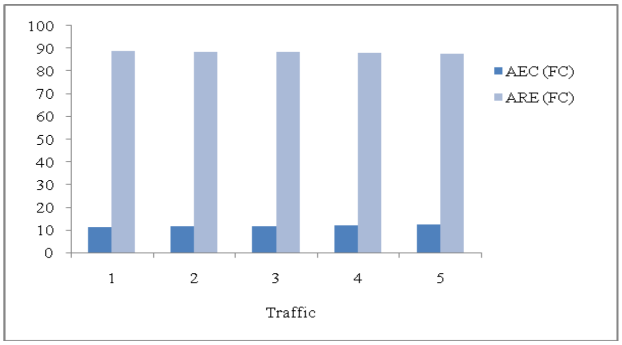

Fig. 5: AEC and ARE for increasing traffic (FC)

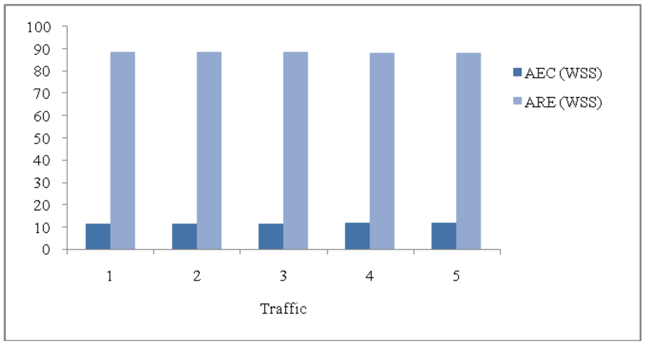

Fig. 6 AEC and ARE for increasing traffic (WSS)

6. Conclusion

CRNs are more vulnerable to many security threats and attacks compared to traditional wireless area networks. However, many wireless devices operate in CRNs which are battery powered. Attack launched by MUs degrades the performance of CRNs. The proposed protocol considers security aspects along with energy efficiency of CRNs. The devices compare current energy consumed with predefined threshold and hence increases network life time. Simulation results show better energy efficiency of the protocol with respect to increased network size and traffic. Proposed protocol minimizes disconnection of link due to secured path between source and destination. As a results transmission control packets are also minimized. It also saves energy due to needless channel detection.

References

[1] Y.Liang, Y.Zeng, E.Peh and A.Hoang, "Sensing throughput trade off for cognitive radio networks", IEEE Transactions on Wireless Communications, vol.7, issue 4, pp. 1326-1337, April 2008.

[2] K. Lakshmana Rao, C. Kalyana Chakravarthy and Shanti Chilukuri "Energy Efficient Routing in Cognitive Radio Networks: Challenges and Existing Solutions" ICTACT Journal on Communication Technology, Volume: 06, Issue: 01, pp. 1049-1052 March 2015.

[3] Y. Chen, Q. Zhao, and A. Swami, "Distributed cognitive MAC for energy-constrained opportunistic spectrum access," in Proc. IEEE Military Communication Conference, pp. 1–7, Oct. 2006.

[4] A. Hoang, Y.C. Liang, and T. C. Wong, "Opportunistic spectrum access for energy constrained cognitive radios" in Proc. IEEE (2008 Spring) Vehicular Technology Conference, pp. 1559–1563, May 2008.

[5] Liying Li, Xiangwei Zhou, Hongbing Xu, Geoffrey Ye Li, Dandan Wang, and Anthony Soong " Energy-Efficient Transmission in Cognitive Radio Networks" IEEE International

Consumer Communications and Network Conference (CCNC), Las Vegas, USA, 9-12 Jan. 2010.

[6] Muhammad Naeem, Kandasamy Illanko, Ashok Karmokar, Alagan Anpalagan and Muhammad Jaseemuddin **“**Energy-Efficient Cognitive Radio Sensor Networks: Parametric and Convex Transformations” Sensors Journal, vol. 13, issue 8, 2013.

[7] Saud Althunibat, Victor Sucasas, Hugo Marques, Jonathan Rodriguez, Rahim Tafazolli, and Fabrizio Granelli" On the Trade-Off Between Security and Energy Efficiency in Cooperative Spectrum Sensing for Cognitive Radio" IEEE communications letters, vol. 17, no. 8, Aug 2013.

[8] Viswanathan Ramachandran and Alice Cheeran “Improvement of Energy Efficiency of Spectrum Sensing Algorithms for Cognitive Radio Networks using Compressive Sensing Technique” International Conference on Computer Communication and Informatics (ICCCI -2014), Coimbatore India, 3-5 Jan. 2014.

[9] B. Senthil kumar and S. K. Srivatsa “An Efficient Spectrum Sensing Framework and Attack Detection in Cognitive Radio Networks using Hybrid ANFIS” Indian Journal of Science and Technology, vol. 8, issue 28, 2015.

[10] K.Sathya, B. K. AnuPreethi, V.Vijayaraghavan, and M.Laavanya “Analysis of Energy Efficiency for Cognitive Radio Networks” Asian Journal of Electrical Sciences, vol.4 no.2, July-December 2015.

[11] Shaowei Wang, Chonggang Wang “Joint optimization of spectrum and energy efficiency in cognitive radio networks” Elsevier journal of Digital Communication and Networks, vol. 1, issue 3, pp. 161-170, Aug. 2015.

[12] Fourat Haider, Cheng-Xiang Wang, Harald Haas, Erol Hepsaydir, Xiaohu Ge and Dongfeng Yuan “Spectral and Energy Efficiency Analysis for Cognitive Radio Networks” IEEE Transactions on Wireless Communications, vol. 14, issue 6, June 2015.

[13] Efe F. Orumwense, Thomas J. Afullo and Viranjay M. Srivastava “Energy Efficiency Metrics in Cognitive Radio Networks: A Hollistic Overview” International Journal of Communication Networks and Information Security (IJCNIS), vol. 8, no. 2, August 2016.

[14] Satyam Agarwal and Swades De “eDSA: Energy-Efficient Dynamic Spectrum Access Protocols for Cognitive Radio Networks” IEEE Transactions on Mobile Computing, vol. 15, issue 12, Dec. 2016.

[15] Mohammad Robat Mili, Leila Musavian, Khairi Ashour Hamdi and Farokh Marvasti “How to Increase Energy Efficiency in Cognitive Radio Networks” IEEE Transactions On Communications, vol. 64, no. 5, pp. 1829-1843, May 2016.