International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-1, 2019.

ISSN: 2581-3404 (Online)

Resource Allocation and Attacks in Wireless Sensor Network: A Review

Madhu Sharma[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]er.madhu05@gmail.com, [2]jitendramishra@gmail.com

ABSTRACT

Wireless technologies and services have been witnessed a rapid growth in the past few years, due to this development, spectrum scarcity and shortage has become a major concern, several spectrum portions of the static allocated licensed bands are under-utilized, Cognitive radio networks (CRNs) the most encouraging solution in enhancing the spectrum utilization by providing licensed spectrum portions to unlicensed users, however due to nature of these networks, CRNs are exposed to different types of security threats and attacks from different malicious users, which can affect the network availability and performance, in this paper we presents the survey for the resource allocation in wireless networks, and improve the security system.

Keywords: Wireless sensor networks, Attack, resource allocation, Cognitive radio network, Mobile ad-hoc networks.

INTRODUCTION

The last few years, significant developments in wireless technologies have made mobile devices, such as laptops, mobile phones, smart phones, and personal digital assistants, an essential part of the human life. According to the Silicon India Magazine's report [7], the number of cell phone subscriptions are estimated to increase from 6 billion in January 2013 to 7.3 billion in 2014, which is, interestingly enough, more than the world's current population. The future wireless communication networks are expected to aggregate the spectrum resource of heterogeneous wireless networks to support high-quality communication services for mobile terminals (MTs) [1]. In the fifth generation (5G) communication system, there exist some promising candidate technologies, e.g., heterogeneous wireless network, non-orthogonal multiple access (NOMA), and massive multiple input and multiple output (MIMO). With the advance of multi-homing technologies, each MT is able to connect to available wireless networks via different radio interfaces, and the data stream for each MT is split into multiple sub-streams, which are transmitted simultaneously over different types of wireless networks. In this need based scenario, advancement in Hardware Engineering made it possible, the invention of a number of mobile computing devices. PDA's, Pocket PC's and smart phones can be seen everywhere.

In the last decade, the massive growth in mobile computing devices brought a revolutionary change in computing, the evolution of ubiquitous computing. At present, the concept of ubiquitous computing is a research hot spot in Computer Science society. In ubiquitous computing environment, the individual users may retrieve information smoothly whenever and wherever they are by utilizing heterogeneous electronic platforms simultaneously [14]. Non-orthogonal multiple access (NOMA) technique is widely considered as one of the promising techniques to improve the system capacity of future wireless communication networks [3]. In particular, NOMA uses the power domain for multiple access, where different users are served at different power levels. Additionally, users employ successive interference cancelation (SIC) to remove the messages of other users before decoding their own messages. On the other hand, the spectrum resources are not utilized efficiently, and cognitive radio can be applied into NOMA-based wireless network via accessing the licensed spectrum opportunistically to improve the spectrum efficiency.

Cellular networks have so far been able to maintain QoS and provide good user experience in isolated areas, but current techniques in these networks will not be able to meet the increasing capacity demands of future mobile users in close proximity to each other, such as in a shopping mall or a concert. Discussions of a new standard (referred to as 5G) are underway in the academia and industry in order to meet the requirements of future cellular networks. The exact definition of 5G is not clear but it takes into consideration a wider range of use cases. 5G networks are expected to support existing and emerging technologies as well as integrate new solutions to meet the increasing demand for data rates [10]. These drivers have motivated research efforts toward efficient spectrum utilization in 5G cellular networks. Consider a geographical area with a primary network and a cognitive network, as shown in below figure. At the physical layer, the bandwidth is divided into orthogonal subchannels, and NOMA technology is adopted at each sub-channel for both primary network and cognitive radio network. There is an eavesdropper in NOMA-based cognitive radio network, who is passive and aims to wiretap the transmission signal in all the data-bearing subchannels.1 Additionally, the wireless channels between the secondary users and the secondary BS or the eavesdropper are assumed to be perfectly known [3].

As spectrum usage varies temporally and spatially in wireless networks, the spectrum band is fragmented into several spectrum segments. The spectrum segments that are unused by the PUs in a time interval, are known as spectrum holes in a cognitive radio network (CRN). These spectrum holes appear as usable channels to a secondary user (SU). To leverage the spectrum holes/channels for an effective network throughput, mechanisms for spectrum/channel assignment in CRNs must be developed. In this paper, we use spectrum assignment and channel assignment to represent the similar concept of channel mapping to radio interfaces of nodes in the CRNs. Channel assignment in CRNs is defined as a problem of determining an optimal mapping between the available licensed channels and the cognitive radio such that the performance of CRN is optimized.

In cognitive heterogeneous networks, resource allocation can be formulated to maximize spectral efficiency, energy efficiency, and fairness. For maximizing spectral efficiency, a random subcarrier allocation algorithm is proposed based on super modular game theory, a joint resource allocation and spectral sensing framework is investigated to maximize the spectrum efficiency. Different from an energy-efficient resource allocation algorithm is solved with stackelberg game theory for cognitive heterogeneous femtocell networks. Based on smart grid is further considered in cognitive heterogeneous femtocell networks, and a stackelberg game framework with three-level structure is proposed to decide electricity price, interference price and energy-efficient power allocation. For guaranteeing the fairness of secondary MTs, a fair resource allocation scheme with imperfect spectral sensing is proposed under cross-tier/co-tier interference constraints for cognitive heterogeneous femtocell network [2].

Opportunistic Routing, however, considers the shared wireless medium as an opportunity rather than a limitation. In fact, the key idea behind opportunistic routing is to overcome the drawback of unreliable wireless transmission by taking advantage of the broadcast nature of the wireless medium. That is, instead of pre-selecting a specified relay node at each transmission, opportunistic routing broadcasts a data packet so that it is overheard by multiple neighbors which later form the candidate relays set. Then, the actual packet forwarder will be chosen from this set of candidates which have successfully received this data packet. This property is called multi-user diversity because it refers to a type of spatial diversity existing across multiple receivers (or users)[8].

The rest of this paper is organized as follows in the first section we describe an introduction of about the wireless sensor network and attack. In section II we discuss about the Non orthogonal multiple access, In section III we discuss about the Cognitive radio network. In section IV we discuss about the rich literature survey, finally in section V we conclude the about our paper.

II NON-ORTHOGONAL MULTIPLE ACCESS

In order to improve the network performance further, the joint power allocation and user scheduling algorithms are designed in. A joint sub-channel assignment, user scheduling, and power allocation for NOMA-based wireless network is presented via many-to-many two-sided matching game to maximize weighted sum-rate, a joint power allocation and user scheduling algorithm for NOMA-based wireless network is proposed via Lagrangian duality and dynamic programming methods. Two joint power allocation and user scheduling algorithms for multicarrier NOMA-based wireless network are designed with a full duplex base station serving multiple half-duplex downlink and uplink users. For NOMA-based wireless network with one base station and multiple energy harvesting users, a resource allocation algorithm via greedy method is proposed to improve the individual transmission rate and user fairness. Although the joint user scheduling and power allocation problems are investigated for NOMA-based wireless network , how cognitive radio technology affects the security-aware resource allocation problem for NOMA-based wireless network needs further studies.

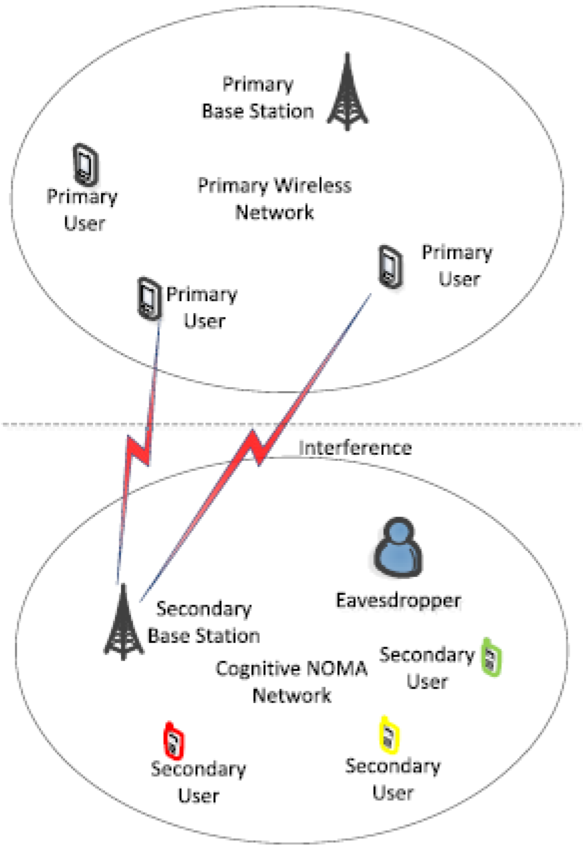

Fig 1: NOMA-based cognitive radio network [3].

III COGNITIVE RADIO NETWORKS

The CRNs are also known as secondary networks, DSA networks, or unlicensed networks. The nodes in the CRNs are equipped with the cognitive radios (CRs) that are capable of changing the transceiver parameters based on the changes in the environment within which the CRN nodes operate. The CRNs are further classified into two groups, namely: a) infrastructure-based CRNs [7] and b) infrastructure less CRNs or cognitive radio ad-hoc networks (CRAHNs). The infrastructure-based CRNs have one central network entity, such as the base station for communication control. Examples of such networks are cognitive radio cellular networks (CRCNs) and wireless regional area networks (WRANs). A CRN may have a spectrum broker that maintains and distributes the spectrum resources among various CRNs.

In below figure shows an architecture of the CRN. The SUs can utilize both the available licensed portions of the spectrum owned by a PU and the unlicensed portions of the spectrum. The CR base station communicate with a secondary node at channel on which the secondary receiver node is tuned. The color of a wireless link in diagram shows the spectrum band whereas a number on the wireless link represents the channel ID. The devices on the horizontal spectrum separating line have multiple available channels. The operations involved in accessing and using a particular portion of a spectrum vary according to the type of spectrum band. The licensed band is normally used by the PUs; therefore, the SUs are required to detect the activity of the PUs. The channel capacity of licensed band for secondary node is dependent on the interference received at the nearby PUs. Moreover, the SUs must vacate the band upon detection of the PUs presence within the spectrum. In this case, the SUs switch to the next best available channel. To access the unlicensed band, the SUs must compete with the other SUs. The CRs are used by the researchers to improve the network capacity of various wireless networks.

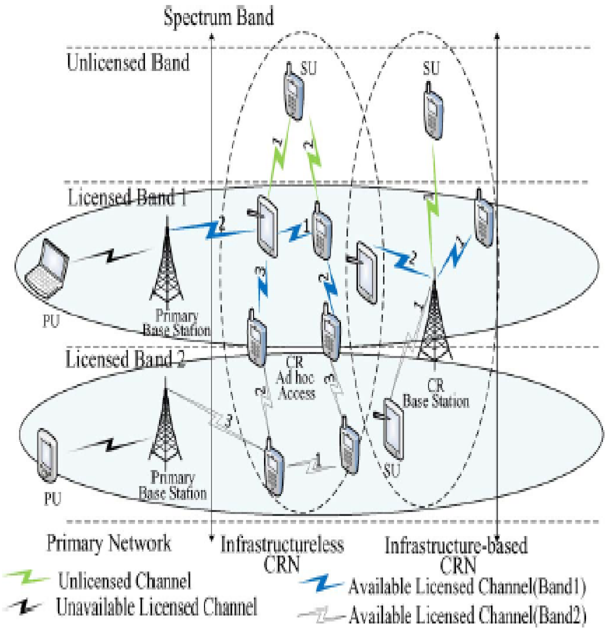

Fig 2: The CRN architecture.

IV RELATED WORK

[1] In this paper, a security-aware energy-efficient resource allocation is modeled as a fractional programming problem for heterogeneous multi-homing networks. The security-aware resource allocation is formulated as a secrecy energy efficiency maximization problem subject to the average packet delay, the average packet dropping probability, and the total available power consumption. In order to guarantee the packet-level quality of service (QoS), first, the average packet delay and the average packet dropping probability requirement for each mobile terminal at the link layer are transformed into a minimum secrecy rate constraint at the physical layer. Then, the non-convex secrecy energy efficiency maximization problem is approximated by a convex problem through epigraph representation.

[2] In this paper, they studied the uplink security-aware proportional fairness power and sub channel allocation problem for cognitive heterogeneous networks with inter-network cooperation. Each secondary MT adjusts radio power and sub channel according to imperfect spectral sensing and channel state information, so as to maximize the secrecy throughput under the QoS constraints. To solve the above bi-convex optimization problem, an optimal security-aware power and sub channel allocation algorithm was proposed via the dual decomposition method. Finally, the heuristic power and sub channel allocation algorithms were proposed by the greedy method.

[3] In this paper, a downlink security-aware resource allocation problem with delay constraint via spectrum sensing is modeled as a mixed integer non-linear problem for non-orthogonal multiple access-based cognitive radio network. The security-aware resource allocation is subject to constraints in required delay for each secondary user, maximum number of accessed secondary users at each sub-channel, total interference power threshold introduced to primary users, and total power consumption at secondary BS. The security-aware resource allocation is based on channel state information at the physical layer and queue state information at the link layer.

[4] This article presents the challenges for experimentation, the test beds built, results, lessons learned, and the impact of that work to place wireless community networks as one sustainable way toward an Internet accessible to all. Research and development in the last five years has produced a large set of results (software, algorithms, models, evaluations) and improvements around resource allocation, routing, cross-layer optimized systems and services, benchmarking methods and tools, and detailed evaluations of social, technological, economic, and legal aspects in several developing and developed areas of the world.

[5] In this paper, they exploit the intrinsic nature of social networks, i.e., the trust formed through social relationships among users, to enable users to share resources under the framework of 3C. Specifically, we consider the mobile edge computing (MEC), in-network caching and device-to-device (D2D) communications. When considering the trust-based MSNs with MEC, caching and D2D, we apply a novel deep reinforcement learning approach to automatically make a decision for optimally allocating the network resources. The decision is made purely through observing the network's states, rather than any handcrafted or explicit control rules, which makes it adaptive to variable network conditions. Google Tensor Flow is used to implement the proposed deep Q-learning approach. Simulation results with different network parameters are presented to show the effectiveness of the proposed scheme.

[6] In the survey, they review the existing assumptions of CSI which have been considered in physical layer security, while we discuss three ways to characterize the uncertainties of the imperfect eavesdropper's CSI. It is observed that, to cope with the problems of the imperfect or unknown CSI of eavesdroppers, the robust security designs, probabilistic view of security, or QoS-based optimization is usually considered in physical layer security to get a compromise solution. In addition, they discuss possible future trends and open challenges from the aspects involving the problems of imperfect CSI, eavesdropper models, and hardware impairments, as well as cross-layer security designs, global performance optimizations, and commercial application of physical layer security.

[7] This paper presents a comprehensive survey on the state-of-the-art channel assignment algorithms in cognitive radio networks. They also classify the algorithms by presenting a thematic taxonomy of the current channel assignment algorithms in cognitive radio networks. Moreover, the critical aspects of the current channel assignment algorithms in cognitive radio networks are analyzed to determine the strengths and weaknesses of such algorithms. The similarities and differences of the algorithms based on the important parameters, such as routing dependencies, channel models, assignment methods, execution model, and optimization objectives, are also investigated. They also discuss open research issues and challenges of channel assignment in the cognitive radio networks.

[8] In this paper they provide a comprehensive survey of the existing literature related to opportunistic routing. They first study the main design building blocks of opportunistic routing. Then, we provide a taxonomy for opportunistic routing proposals, based on their routing objectives as well as the optimization tools and approaches used in the routing design. Hence, five opportunistic routing classes are defined and studied in this paper, namely, geographic opportunistic routing, link-state-aware opportunistic routing, probabilistic opportunistic routing, optimization-based opportunistic routing, and cross-layer opportunistic routing. They also review the main protocols proposed in the literature for each class. Finally, they identify and discuss the main future research directions related to the opportunistic routing design, optimization, and deployment.

[9] In this article, they first summarize privacy constraints and primary attacks based on new

features of IoT. Then they present three case studies to demonstrate principal vulnerabilities and classify existing protection schemes. Built on this analysis, they identify three key challenges: a lack of theoretical foundation, the trade-off optimization between privacy and data utility, and system isomerism over-complexity and high scalability. Finally, they illustrate possible promising future directions and potential solutions to the emerging challenges facing wireless IoT scenarios. they aim to assist interested readers in investigating the unexplored parts of this promising domain.

[11] In this paper, a proposed countermeasures for layered security attacks are introduced to authenticate and secure CRNs based on a modified digital signature technique using a new customized cryptographic hash function and authentication mechanisms that implemented in CRNs, the proposed hash function is tested and associated with RSA (Rivest, Shamir, Adleman), public key cryptography digital signature algorithm, and then applied in a proposed CRNs framework, with authentication mechanisms, that is designed and simulated using OMNeT++ discrete event simulator, the complete proposed system, can provide security proofs such as authentication, access control.

V CONCLUSIONS AND FUTURE SCOPE

The Mobile Ad hoc Networks (MANETs) are optimal choice to accommodate this growing trend but there is a problem, security is the core issue. MANETs rely on wireless links for communication. Wireless networks are considered more exposed to security attacks as compared to wired networks, especially; MANETs are the soft target due to vulnerable in nature. Lack of infrastructure, open peer to peer connectivity, shared wireless medium, dynamic topology and scalability are the key characteristic of MANETs which make them ideal for security attacks. In this paper, we discuss about the various attacks in the wireless sensor networks, in future we plan to implement the resource allocation mechanism in the wireless sensor network without any attack.

REFERENCES:-

[1] Lei Xu , Hong Xing , Arumugam Nallanathan , Yuwang Yang, and Tianyou Chai, “Security-Aware Cross-Layer Resource Allocation for Heterogeneous Wireless Networks”, IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 67, NO. 2, FEBRUARY 2019, pp 1388-1399.

[2] Lei Xu , Lin Cai , Yansong Gao, Jian Xia , Yuwang Yang, and Tianyou Chai, “Security-Aware Proportional Fairness Resource Allocation for Cognitive Heterogeneous Networks”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 67, NO. 12, DECEMBER 2018, pp 11694-11704.

[3] Lei Xu, Arumugam Nallanathan, Xiaofei Pan, Jian Yang, and Wenhe Liao, “Security-Aware Resource Allocation With Delay Constraint for NOMA-Based Cognitive Radio Network”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 13, NO. 2, FEBRUARY 2018, pp 366-376.

[4] Leandro Navarro, Roger Baig Viñas, Christoph Barz, Joseph Bonicioli, Bart Braem, Felix Freitag, and Ivan Vilata-i-Balaguer, “Advances in Wireless Community Networks with the Community-Lab Testbed”, IEEE 2016, pp 20-27.

[5] Ying He, Chengchao Liang, F. Richard Yu, and Zhu Han, “Trust-based Social Networks with Computing, Caching and Communications: A Deep Reinforcement Learning Approach”, IEEE 2018, pp 1-14.

[6] Dong Wang, Bo Bai, Wenbo Zhao, and Zhu Han, “A Survey of Optimization Approaches for Wireless Physical Layer Security”, IEEE 2018, pp 1-34.

[7] Ejaz Ahmed, Abdullah Gani, Saeid Abolfazli, Liu Jie Yao, and Samee U. Khan, “Channel Assignment Algorithms in Cognitive Radio Networks: Taxonomy, Open Issues, and Challenges”, IEEE COMMUNICATIONS

SURVEYS & TUTORIALS, VOL. 18, NO. 1, FIRST QUARTER 2016, pp 795-824.

[8] Nessrine Chakchouk, “A Survey on Opportunistic Routing in Wireless Communication Networks”, IEEE COMMUNICATION SURVEYS & TUTORIALS, VOL. 17, NO. 4, FOURTH QUARTER 2015”, pp 2214-2241.

[9] Youyang Qu, Shui Yu, Wanlei Zhou, Sancheng Peng, Guojun Wang, and Ke Xiao, “Privacy of Things: Emerging Challenges and Opportunities in Wireless Internet of Things”, IEEE Wireless Communications, IEEE 2018, pp 91-97.

[10] Furqan Jameel , Zara Hamid, Farhana Jabeen, Sherali Zeadally, and Muhammad Awais Javed, “A Survey of Device-to-Device Communications: Research Issues and Challenges”, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 20, NO. 3, THIRD QUARTER 2018, pp 2133-2168.

[11] John N. Soliman, Tarek Abdel Mageed, Hadia M. El-Hennawy, “Countermeasures for Layered Security Attacks on Cognitive Radio Networks based on Modified Digital Signature Scheme”, Research gate 2017, pp 1-8.

[12] Sarita Soni, Samir Srivastava, “ Survey of Quality of Service Routing Protocol in MANET”, International Journal of Computer Application, 2016, pp 6-10.

[13] Jean-Aime Maxa, Mohamed-Slim Ben Mahmoud, Nicolas Larrieu, “Survey on UAANET Routing Protocols and Network Security Challenges”, Ad Hoc Sensor Wireless Networks, PKP Publishing Services Network 2017.

[14] Asif Shabbir, Fayyaz Khalid, Syed Muqsit Shaheed, Jalil Abbas, M. Zia-Ul-Haq, “Security: A Core Issue in Mobile Ad hoc Networks”, Journal of Computer and Communications, 2015, pp 41-66.

Madhu Sharma received her Bachelor`s degree in Electronics & comunication, MIT, Ujjain, M.P., in 2011. Currently she is pursuing Master of Technology Degree in Electronics & Comunication (Digital communication) from PIES, (RGPV), Bhopal, Madhya Pradesh India. Her 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 area of Interests are Antenna & Wave Propagation, Digital Signal Processing, Wireless Communication, Image Processing etc.