IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE)
e-ISSN: 2278-1676,p-ISSN: 2320-3331, Volume 11, Issue 2 Ver. II (Mar. – Apr. 2016), PP 61-64
www.iosrjournals.org

A Review On Cross Layer Attack Aware Cognitive Radio Networks with Multihop Routing

Neha P.Gogulwar[1], Ashish Manusmare[2]
[1]*Dept. of Electronics and Communication Engineering, Ballarpur Institute of Technology Bamni Ballarpur (M.S.), India*
[2]*Dept. of Electronics and Communication Engineering, Assistant Professor, Ballarpur Institute of Technology Bamni Ballarpur (M.S.), India*

Abstract: *Cognitive Radio Networks (CRNs) with such spectrum aware devices is a hopeful solution to the spectrum insufficiency issue in wireless communication area. It is viewed as a revolutionary potential radio technology capable of offering dynamic spectrum contact. In this, an effective routing solution with a cross layer design is proposed for the multi-hop CRNs. It is seen that the in cognitive radio based networks there are cross layer attack which occur due to DDOS. Our work is concentrated on the issue of cross layer design for routing in cognitive radios which have DDOS attacks. We will be providing a layer for attack removal in the cross layer networks which will allow the system to provide efficiency in routing even under attacks .This will help the network to perform effective routing even if DDOS attack occur In this work, a routing algorithm based on Routing Protocols for Low power and lossy networks (RPL) is being proposed for the CRNs. Dynamic spectrum distribution is also done along with routing with the help of RPL. MATLAB simulation is done to analyse the effectiveness of the proposed algorithm.*

Keywords: *Cognitive Radio Network, Cross layer Routing, DDOS, Multi Hop Cognitive Radio Network, RPL*

I. Introduction

Cognitive Radio (CR), recommended by Joseph Mitola III, is an developing wireless communication model that can significantly improve the spectrum usage efficiency by offering dynamic spectrum access. CR Networks (CRNs) is a spectrum aware devices to the spectrum scarcity issue in wireless communication. Cognitive radio networks (CRNs) are composed of cognitive, spectrum devices capable of changing their configurations on the fly based on the spectral environment. This capability opens up the possibility of designing flexible and dynamic spectrum access strategies with the purpose of opportunistically reusing portions of the spectrum temporarily vacated by licensed primary uses. This work focuses on the problem of an attack aware cross layer routing .It improves the efficiency of network. In this paper, a brief overview of the CR technology is provided followed by a detailed analysis of the security attacks pointing Cross layer Routing protocol for multihop cognitive radio network .We aware the attacks with respect to the layer they target starting from the physical layer and moving up to the transport layer.

Routing in cognitive radio networks (CRNs) needs a cross-layering method. However, CRN routing protocols proposed in literature are partially cross-layer, for the reason that the information flow is only from physical layer to network layer, e.g. about channels availabilities. cross-layer routing protocol (CLRP)introduces , which considers both the channels that are known to be available at each node, as well as other channels that may be available. The availabilities of the latter channels are considered using a stochastic approach. CLRP computes an end to end path, and feeds the physical layer with information about which channels to sense and which nodes should perform the sensing, such that the expected route quality is improved which channels to be sensed.

Denial of Service (DoS) attacks is severe in all the attacks in security of wireless network. Also, cognitive radio networks are vulnerable to DoS attack due to their own characteristics. DoS attacks in ad hoc cognitive radio networks in different protocol layers Routing protocol being used in most of the existing work is the Ad-hoc On-demand Distance Vector protocol. In AODV, the Route Request (RREQ) messages, which are sent via spreading, contain locally obtained network state and deliver this detailed information to the destination, where they are processed to compute path and the routing decisions being adopted at the destination are then forwarded in the reverse path using the Route Reply (RREP) messages. Here comes the need for a protocol in CRN that can perform the routing as the control packet moves from one point to another.

RPL is a distance vector routing protocol for LLNs. Network devices running the protocol are connected in such a way that no cycles are present. For this purpose a Destination Oriented Directed Acyclic Graph (DODAG), which is routed at a single destination is built. It is the main candidate for acting as a standard routing protocol for Internet Protocol (IP) smart object networks. RPL is based on the topological concept of Directed Acyclic Graphs (DAGs). In this algorithm, routing is performed through the construction of a colored

Destination Oriented DAGs (DODAGs) with destination as the root and source(s) as the leaf node(s). Connection frequencies are represented using different It determines the best route from a source to destination. The algorithm selects the path with the minimum hop count and the minimum adjacent link interference as the best path. Also, two nodes will communicate in a CRN only if there exists a common channel between them.

II. Literature Survey

Irin Sajan , Ebin M. Manuel (feb 2015)[1] this paper present an effective routing solution with a cross layer design is proposed for the multi-hop CRNs. Most of the existing work uses Ad-hoc On-demand Distance Vector (AODV) protocol as the routing protocol for CRNs. In this work, a novel routing algorithm based on Routing Protocol for Low power and lossy networks (RPL) is being proposed for the CRNs. Routing is accomplished through the formation of colored Destination Oriented Directed Acyclic Graphs (DODAGs) of which the link frequencies are represented using colors. Hop count and adjacent link interference are counted as the routing metrics. Dynamic spectrum allocation is also done along with routing with the help of RPL. The CRN scenario is vulnerable to link failures due to the appearance of Primary Users (PUs). So route repairing using the Trickle algorithm offered by RPL. RPL is found to be a suitable routing protocol that can be carried out into the real CRN scenario.

Ramzi Saifan, Ahmed E.Kamal[2]A Cross-Layer Routing Protocol (CLRP) for Cognitive Radio Network routing protocols proposed in literature are partially cross-layer, because the information flow is only from physical layer to network layer, e.g., about channels availabilities. In this work, we introduce a cross-layer routing protocol (CLRP), which considers both the channels that are known to be available at each node, as well as other channels that may be available. The availabilities of the latter channels are considered using a stochastic approach. CLRP computes an end to end path, and feeds the physical layer with information about which channels to sense and which nodes should perform the sensing, such that the expected route quality is enhanced. Simulation results show that CLRP outperforms other cross-layer routing protocols in terms of throughput and stability of the path being setup, and increases the probability of finding an end-to-end path. In this paper we proposed a new approach for routing in CRN.

Trong Nghia Le,[May 2015][3] In this paper, the channel-tap power is utilized as a radio-frequency fingerprint (RF) to completely identify primary user emulation attacks (PUEAs) over multipath Rayleigh fading channels. To accurately know identities of primary users (PUs) and PUEAs, the cross-layer intelligent learning ability of a mobile secondary user (SU) is exploited to establish detection databases by seamlessly combining the quick detection of physical (PHY) layer with the accuracy of higher layer authentication. The proposed method helps PHY layer completely detect the identities of PUs and PUEAs**.** The uniqueness of channel-tap powers between the SU and Txs is utilized as a RF to detect PUEA and PU in mobile CR networks. In addition, this letter proposes cross-layer design to completely detect PUEA and PU based on detection databases established by seamlessly combining the accuracy of higher layer authentication with the quick detection of PHY layer. Simulations demonstrate that the proposed technique greatly enhances detection efficiency of PHY layer.

Wassim El-Hajj, Haidar Safa,[March 11][4]In this Cognitive Radio (CR) is a novel technology that promises to solve the spectrum shortage problem by allowing secondary users to coexist with primary users without causing interference to their communication. Although the operational aspects of CR are being explored vigorously, its security aspects have gained little attention. In this paper, a brief overview of the CR technology is provided followed by a detailed analysis of the security attacks targeting Cognitive Radio Networks (CRNs) along with the corresponding mitigation techniques. We categorize the attacks with respect to the layer they target starting from the physical layer and moving up to the transport layer. An evaluation of the suggested counter measures is presented along with other solutions and augmentations to achieve a secure and trusted CRN.

Azza Mohammed[Sep. 2015][5] MANET Mobile Ad hoc Network are evolved through various characteristics such as shared media, this property make a routing protocols vulnerable. AODV is a reactive routing where each intermediate node cooperates in the process of route discovery. In this case, the node that behaves as malicious exploit the malfunction of specified service. The black hole attack uses the sequence number that is used to select the freshest route and attract all exchanged data packets to destroy them. Many researchers have dealt with this attack and many solutions have been proposed. These solutions target the network layer only. In this paper, we present our approach to counter black hole attack. This approach is entitled Cross AODV and it is based on verification and validation process. The key point of our approach is the use of the inter layer interaction between networks layer and medium access within the distributed coordination function (DCF) to efficiently detect and isolate malicious nodes. During the route discovery, the verification process uses the RTS or CTS frame that contains information about the requested path. The validation process consists of comparing the routing information with the result of verification phase**.** Our Approach have been

implemented, simulated and compared to two related studies using the well know NS2 Simulator. The obtained results show the efficacy our proposal in term of packet delivery with a neglected additional delay.

Wang Weifang[2010][6] Denial of Service (DoS) attacks is severe in all the attacks in security of wireless network. Furthermore, cognitive radio networks are vulnerable to DoS attack due to their own characteristics. This paper analyzed the architecture of cognitive radio networks and emphatically discussed the possible various DoS attacks in ad hoc cognitive radio networks in different protocol layers**.** surveyed the denial of service attacks in different protocol layer in ad hoc cognitive radio networks. We concluded that adversaries can launch DoS attacks in every layer in ad cognitive radio networks after analysis. Protection against DoS attacks in cognitive radio networks requires a careful cross-layer design.

Tsvetko Tsvetkov[july2011][7] Low Power and Lossy Networks (LLNs) represent one of the most interesting research areas. They include Wireless Personal Area Networks (WPANs), low-power Power Line Communication (PLC) networks and Wireless Sensor Networks (WSNs). Such networks are often optimized to save energy, support traffic patterns different from the standard unicast communication, run routing protocols over link layers with restricted frame-sizes and many others . This paper presents the IPv6 Routing Protocol for Low power and Lossy Networks (RPL) , which has been designed to overcome routing issues in LLNs. It implements measures to reduce energy consumption such as dynamic sending rate of control messages and addressing topology inconsistencies only when data packets have to be sent. The protocol makes use of IPv6 and supports not only traffic in the upward direction, but also traffic flowing from a gateway node to all other network participants.

Natarajan Meghanathan [2013][8] We present a critical review and analysis of different categories of routing protocols for cognitive radio networks. We first classify the available solutions to two broad categories: those based on full spectrum knowledge (typically used to establish performance benchmarks) and those based on local spectrum knowledge (used for real-time implementation). The full spectrum gen based routing solutions are analyzed from a graph-theoretic point of view, and we review the layered graph, edge coloring and conflict graph models. We classify the various local spectrum knowledge based routing protocols into the following five categories: Lowest power, Minimum delay, Maximum throughput, Geographic and Class-based routing. A total of 25 routing protocols proposed for cognitive radio networks have been reviewed. We discuss the working principle and analyze the pros and cons of the routing protocols. Finally, we propose an idea of a load balancing-based resident spectrum knowledge-based routing protocol for cognitive radio ad hoc networks. In this paper, we have presented an exhaustive review and analysis of the routing protocols that have been proposed in the literature for cognitive radio networks. In fact, a licensed user need not be even aware of the presence of the unlicensed CR users, and there should be no appreciable degradation in the quality of service for the primary users. While the routing solutions proposed for centralized and/or infrastructure based CRNs are typically construed to provide performance benchmarks, the solutions proposed for dispersed/cooperative and/or infrastructure less ad hoc CRNs capture the practical difficulties and performance bottlenecks in real-time implementations.

Hicham Khalife, Naceur Malouch, Serge Fdida [8/10/2010][9]Routing is a fundamental issue to consider when dealing with multihop cognitive radio networks. We investigate in this work, the potential routing approaches that can be employed in such adaptive wireless networks. We argue that in multihop cognitive radio environments no general routing solution can be proposed but cognitive environments can be classified into three separate categories, each requiring specific routing solutions. Basically, this classification is imposed by the activity of the users on the licensed bands that cognitive radios try to access. First, over a relatively static primary band, where primary nodes idleness largely exceeds cognitive users communication durations, static mesh routing solutions can be reused, whereas second, over dynamically available spectrum bands new specific routing solutions have to be proposed, we give some guidelines and insights about designing such solutions. Third, if cognitive radios try to access over highly active and rarely available primary bands, opportunistic forwarding without pre-established routing is to be explored . Multihop cognitive radios is one of the most promising research area in already well explored wireless environments. A growing number of solutions targeting essentially routing and channel assignment in such environments are getting proposed by the research community no one has a clear vision on how multihop cognitive radios will look like and what is the time granularity the primary nodes will offer to cognitive radios communications. For this reason, we focus in this paper on multihop cognitive radio networks and on the routing solutions they can support. Essentially, we categorize cognitive radio networks into three separate categories depending on the timescale of the primary bands idle time compared to the cognitive communication duration. In fact, if the availability periods of the primary bands is greatly larger than the CR exchanges, the created multihop can be considered as a static mesh.

III. Methodology

In the previous researchers have focused mainly on the cross layer routing and mutihop cognitive radio networks. The protocols work perfectly in scenario where network attack are non-imminent. But this is not the case normally, usually in cognitive radio based network there are cross layer attacks which occur due to DDOS. Our focussed is on the issue of cross layer design for routing in cognitive radios which have DDOS attack. We will working on a network layer for attack removal in the cross layer networks which will allow the system to provide efficiency in routing even under attacks. This will help the network to perform effective routing even if DDOS attacks occur and it will increase the efficiency with greatest throught.

IV. Conclusion

In this paper, we studied the different research papers. Routing in cognitive radio network has attracted a lot of attention to the researcher's in the recent years. Routing in multi hop cognitive network is a new research area with a limited but rapidly growing set of results. In last few years attacks on cross layer routing protocol in multihop cognitive radio has become one of the most important research area in cognitive radio network. The main objective behind developing one layer which having DDOS attack will allow the system to provide more efficiency in routing even under attacks. We shall compare the efficiency of our proposed technique with the technique mentioned in the base work for checking performance improvement .This will help in improving energy efficiency in Multihop Cognitive Radio NetworkTo ensure a high-quality product, diagrams and lettering MUST be either computer-drafted or drawn using India ink.

Acknowledgements

We would like to thank Department of Electronics and Communication Engineering, BIT Ballarpur for providing the infrastructure and guidance for understanding the technical aspects of an attack which occur on cross layering.

References

[1]. Irin Sajan, Ebin M. Manuel [feb 2015] , "Cross Layer Routing Design Based on RPL for Multi-hop Cognitive Radio Networks" 978-1-4799-1823-2/1/$31.00 ©2015 IEEE
[2]. Ramzi Saifan, Ahmed E.Kamal "A Cross-Layer Routing Protocol (CLRP) for Cognitive Radio Network."
[3]. Trong Nghia Le,[May 2015] "Cross-Layer Design for Primary User Emulation Attacks Detection in Mobile Cognitive Radio Networks" IEEE COMMUNICATIONS LETTERS, VOL. 19, NO. 5, MAY 2015
[4]. Wassim El-Hajj, Haidar Safa,[March 11] "Survey of Security Issues in Cognitive Radio Networks" JOURNAL OF INTERNET TECHNOLOGY · MARCH 2011
[5]. Azza Mohammed[Sep. 2015] " A Cross Layer for Detection and Ignoring Black Hole Attack in MANET"10.5815/ijcnis.2015.10.05
[6]. Wang Weifang "Denial of Service Attacks in Cognitive Radio Networks" 2010 2nd Conference on Environmental Science and Information Application Technology
[7]. Tsvetko Tsvetkov[july 2011] **"**RPL: IPv6 Routing Protocol for Low Power and Lossy Networks" 10.2313/NET-2011-07-1_09
[8]. Natarajan Meghanathan [2013]A CRITICAL REVIEW OF THE ROUTING PROTOCOLS FOR COGNITIVE RADIO NETWORKS AND A PROPOSAL FOR LOAD BALANCING LOCAL SPECTRUM KNOWLEDGEBASED ROUTING , DOI : 10.5121/csit.2013.3702
[9]. Hicham Khalife, Naceur Malouch, Serge Fdida[8/10/2010] Multihop Cognitive Radio Networks: to Route or not to Route IEEE Network, Institute of Electrical and Electronics Engineers, 2009, 23 (4), pp.20-25. <10.1109/MNET.2009.5191142>. <hal-00524785>