International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 04 | July-2015 www.irjet.net p-ISSN: 2395-0072

Design Approach for Cross Layer Attacks Defence in Cognitive Radio

Shwetali V. Wankhede [1], Prof. M. N. Thakare[2], Prof. S. R. Vaidya[3]

[1] *Student Mtech 4th Sem, Electronics (Comm), SDCE Selukate, Wardha, Maharshtra, India*
[2] *Assistant Professor, Department of Electronics & Telecomm. Engg, BDCE Sevagram, Wardha, Maharashtra, India*
[3] *Assistant Professor, Department of Electronics Engg, SDCE Selukate, Wardha, Maharashtra, India*

Abstract - *A latest communication technology named **"CRN" is a network in which an un**-licensed user can use a freed channel in a spectrum band of licensed user without causing interference to the incumbent transmission. Cognitive Radio networks are vulnerable to attacks, as some unwanted user can use this empty channel through attacks and threats. The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. Cross-layer design is a concept introduced to increase network efficiency through information exchange among different layers, has brought revolutionary view change to the networking research community in the past. In this paper, we are working on detecting and defeating attacks in cross layer. .*

Key Words: Cognitive Radio Network (CRN)1…

1. INTRODUCTION

Communication is a transfer of information from one point to another. Today's communication is very advance; we use many new technologies as if Cognitive radio network is latest one. The term Cognitive Radio was first presented by Mitola and Maguire in 1999. In Cognitive radio network an unlicensed user can use an empty channel in a spectrum band of licensed user. Cognitive Radio Networks (CRNs) is an intelligent network that adapt to changes in their network to make a better use of the spectrum. CRNs solve the spectrum shortage problem by allowing unlicensed users to use spectrum band of licensed user without interference. Licensed users are known as primary users and un-licensed users are secondary users. When information is send through a licensed spectrum band is a primary user, only some channel of band is used, others are empty. Un-licensed user called secondary user uses these empty channels. Secondary users always watch the activities of primary user, and detect the empty channel and occupy the channel without disturbing the primary user. When the primary users are active, the secondary user should either avoid using the channel. An empty channel also known as spectrum holes.
Meanwhile if a SU detects any PU signal in its currently used band it should vacate this band for PUs and senses another vacant band in its environment and switches to new sensed hole. Essential security mechanisms should be used for successful deployment of cognitive radio networks (CRNs) to prevent misuse of valuable spectrum bandwidth.

Two types of Band based on frequency spectrum

1. Licensed Band CR
2. Unlicensed Band CR

Two types of Users of CRNs

1. Primary Radio (PR) user, which operates in its licensed spectrum band.
2. Cognitive Radio (CR) user, which operates either in unlicensed spectrum band or in the licensed spectrum band of PR nodes while ensuring that it does not interfere with PR nodes.

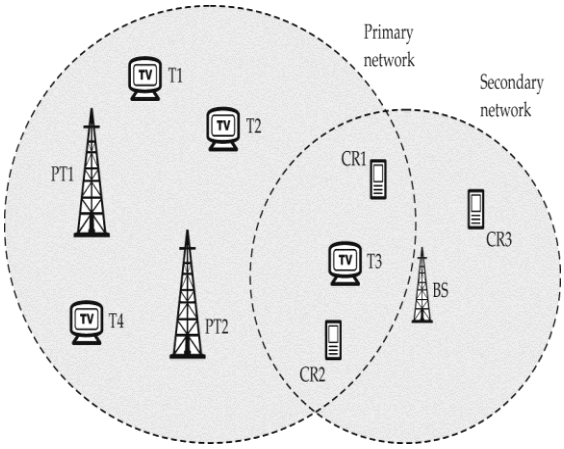

Fig -1: Cognitive Radio

Four main functions of CR

1. Spectrum sensing: It determines which portions of the spectrum are available and detect the presence of licensed users.
2. Spectrum management: It is to select the best available channel.
3. Spectrum sharing: It coordinates access to this channel with other users.
4. Spectrum mobility: It vacates the channel when a licensed user is detected.

This radio spectrum sharing policy among the licensed and unlicensed users, however, opens up the possibility of various security threats. A number of attacks targets CRNs in different layers i.e physical layer, link layer, network layer, transport layer and solutions have been presented to detect those attacks. Here, we are focussing on cross layer attacks in CRNs.

1.1 Attacks in Cognitive Radio

There are many attacks in wireless communication, only few attacks we categorized through four major layers: physical layer, link layer (also known as MA++ layer), network layer and transport layer. In physical layer there are three main attacks- Primary User Emulation (PUE), Objective function attack and jamming. In Link layer- Spectrum Sensing Data Falsification (SSDF), Control Channel Saturation DoS Attack (CCSD), and Selfish Channel Negotiation (SCN). In Network Layer, the routing attacks, HELLO Flood attack and Sinkhole attack. In transport Layer- Lion Attack. This are the attacks on the physical layer, link layer, network layer and transport layer which are yet been detected and defeated.

1.2 Cross Layer attacks

Cross-layer design is a concept introduced to increase network efficiency through information exchange among different layers, has brought revolutionary view change to the networking research community in the past. Nowadays, the increasingly ubiquitous and distributed networking systems are facing vicious and intelligent attacks that exploit almost all network protocols and surely do not restrict themselves within the boundaries of network layers. Attackers have the capability to launch attacks in multiple layers simultaneously. Smart attackers can coordinate the attack activities in different layers to better achieve their goals. A smart attacker can launch several attacks co-ordinately, referred to as cross layer attacks.

Cross-layer design emphasizes on the network performance optimization by enabling different layers of the Communication stack to share state information or to coordinate their actions in order to jointly optimize network performance. Hence the concept of cross layer design must be compared with the traditional layered architecture so that people can be motivated towards the use of the violation of the layered design.

2. LITERATURE REVIEW

This paper describes that Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities [1]. Peng Zhang, Yixin Jiang, Chuang Lin proposed P-Coding which is a novel security scheme against eavesdropping attacks in network coding [2]. This paper discusses the challenges and opportunities of using cross-layer techniques for enhancing wireless network security. It investigate the impact of cross-layer techniques on security and network performance [3]. It propose a trust-based cross-layer defense framework that relies on abnormal detection in individual layers and cross-layer trust fusion. Simulation results demonstrate that the proposed defence framework can significantly reduce the maximum damage caused by attackers [4]. It proposes that in the upper layer, the spoofing attack is considered similarly to the bad data injection toward the power system. A trustworthiness evaluation, which is based on both the physical layer information and power grid measurements, is applied to identify the PMU being attacked [5]. In this, many of attack can attack in different layers of cognitive radio network. Some of them can advertise itself as licensed PUs, or some of them can send false data to the network [6]. This paper describes a CRN based on IEEE wireless regional area network (WRAN) and describes some of the security threats against it [7].

3. DESIGN MODULE

It consist of:

i) Formation of network i.e wired and wireless network,

ii) Creation of nodes within wireless network,

iii) Dataflow within the network.

CR ad hoc network, does not have infrastructure support, and then nodes must rely on local coordination for providing different CR functionalities. Nodes can communicate with each other in a multi hop manner on both licensed and unlicensed spectrum bands. It is assumed that CR users implement functions incorporated into the layering protocols for performing spectrum-aware operations, which form a cognitive cycle. Each CR device owns one declared receiver that listens to a Common Control Channel (CCC) in addition to one or more receivers or transceivers.

4. RESULTS

4.1 Wired Network Formation

Figure 2 shows the formation of network in NS2. Here, five nodes are created in the network and their linking with one another is shown. The above figure shows connection oriented network.

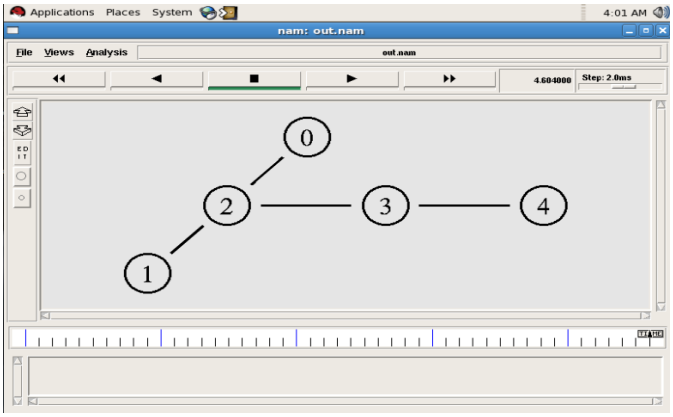

Fig -2: Output window of wired Network formation.

4.1.1 Dataflow

Figure 3 shows the wired or connection oriented communication between node 0 and node 4. Here data is being send from node 0 to node 4.

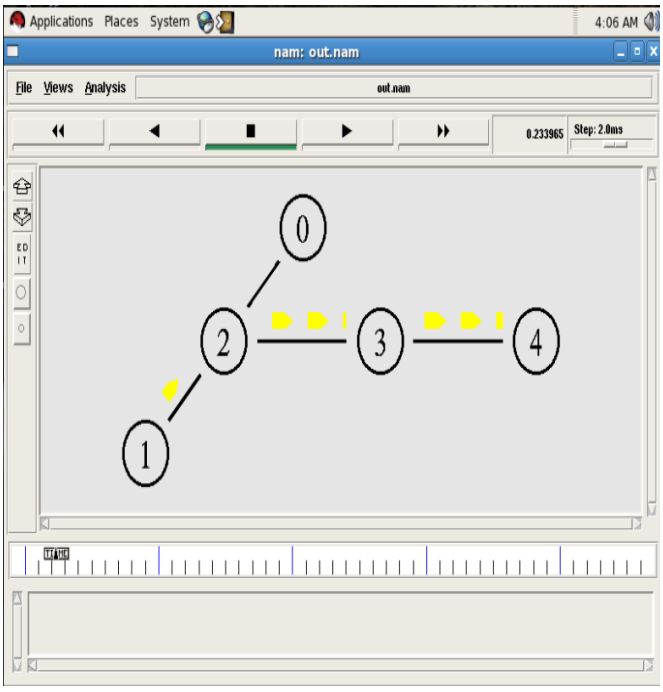

Fig -3: Output window of data flow in wired network

Figure 4 shows that if at same time if data is being send from two different nodes, i.e node 0 is sending data to node 3 whereas node 1 is sending data to node 4. Here in response to the reception of data node 3 is sending an acknowledgement to node 3.

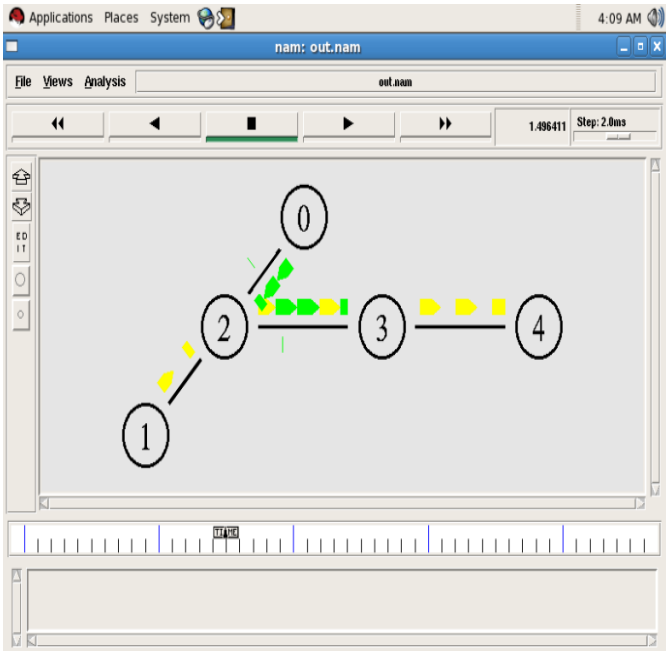

Fig -4: Data flow in wired network with acknowledgement.

4.2 Wireless Network Formation

Cognitive radio is a form of wireless communication. So we are focusing on the wireless network formation in NS2. Here, specified number of nodes are created within a network are located at different places in the network.

Figure 5 shows 20 nodes are created within the network which are not linked with one another i.e wireless communication is created. This nodes are placed at different locations within the network.

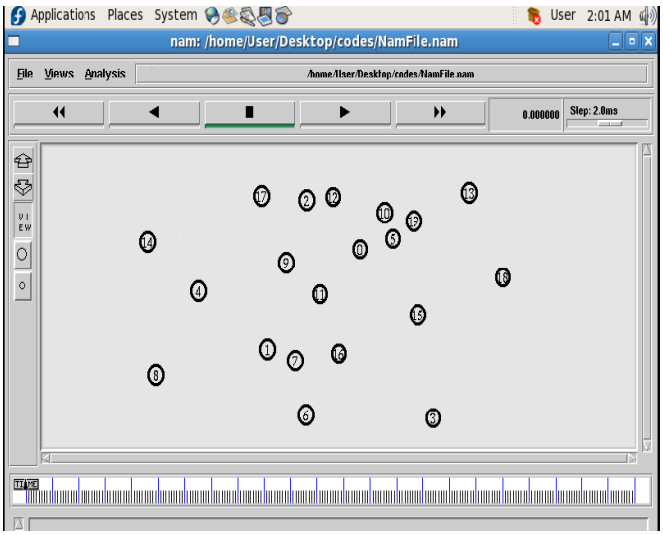

Fig -5: Output window of creation of nodes

Figure 6 shows the broadcasting of signals along the nodes.

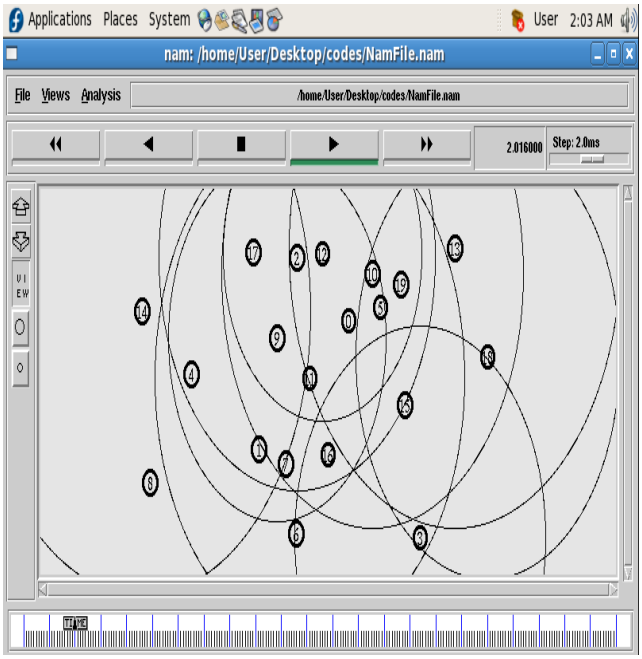

Fig -6: Output window of Broadcasting of signals

4.2.1 Dataflow

Figure 7 shows the Data communication between node 1 and node 7, where node 1 is sending data to node 7.

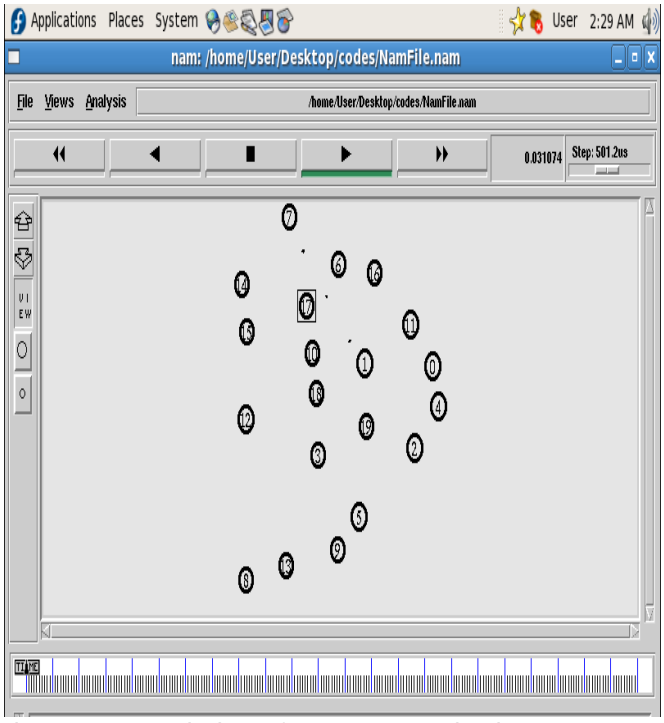

Fig -7: Output window of Data Communication

REFERENCES

[1] Mukesh Barapatre, Prof. Vikrant Chole, Prof. L. Patil. "A Review on Spoofing Attack Detection in Wireless Adhoc Network". (IJETTCS)Volume 2, Issue 6 November-December 2013.

[2] Peng Zhang, Yixin Jiang, Chuang Lin. "P-Coding: Secure Network Coding against Eavesdropping Attacks". INFOCOM, 2010 Proceedings IEEE.

[3] Geethapriya Thamilarasu and Ramalingam Sridhar, "Exploring Cross-layer techniques for Security: Challenges and Opportunities in Wireless Networks" 2007 IEEE.

[4] Wenkai Wang and Yan (Lindsay) Sun, Husheng Li and Zhu Han. "Cross-Layer Attack and Defense in Cognitive Radio Network" Conference (Globecom 2010)

[5] Yawen Fan, Zhenghao Zhang, Matthew Trinkle, Aleksandar D. Dimitrovski, Bin Song, and Husheng Li. "A Cross-Layer Defense Mechanism Against GPS Spoofing Attacks on PMUs in Smart Grids" 1949-3053 _c 2014 IEEEY.

[6] Pooja Dubey and Prof. Sapna Choudhury. "A Survey-Cognitive Radio Network Attacks & Preventions". (IJAFRC) Vol.1, Issue 2, Feb 2014. ISSN 2348 – 4853

[7] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, "Intrusion Detection System (IDS) for Combating Attacks Against Cognitive Radio Networks" IEEE Network Magazine, vol. 27, no. 3, pp. 51-56, May-June 2013.

[8] Khaleel Husain, Premala Patil, "A survey on different cross-layer attacks and defenses in manets" IJRET eISSN: 2319-1163 | pISSN: 2321-7308.

[9] Wassim El-Hajj, Haidar Safal, Mohsen Guizani. "Survey of Security Issues in Cognitive Radio Networks". Journal of Internet Technology Volume 12 (2011) No.2.

[10] Ms. Shikha Jain and Ms. Anshu Dhawan, Dr. C.K Jha. "Emulation Attack in Cognitive Radio Networks: A study". (IJCNWC), ISSN: 2250-3501 Vol.4, No2, April 2014.

[11] Hong-Ning Dai, QiuWang, Dong Li and Raymond Chi-Wing Wong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas". International Journal of Distributed Sensor NetworksVolume 2013, Article ID 760834S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

