CHALLENGES FOR EVOLVING COUNTERMEASURES AGAINST SECURITY THREATS IN COGNITIVE RADIO NETWORKS

Srishti Priya Chaturvedi[1], T. L. Singal[2]
E-Mail Id: [1]srishti.chtaurvedi@chitkara.edu.in, [2]tl.singal@chitkara.edu.in
Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab, India

Abstract- Cognitive radios have created an ability to transmit data to licensed users in several bands without causing harmful interference. But this has also resulted in newer security threats along with the awareness of cognitive radios. Adversaries exploit vulnerabilities of this latest technology and cause significant degradation of the performance. The existing research on security issues in cognitive radio networks indicates that cognitive networks are very prone to multiple security threats on various protocol layers. Moreover, possible countermeasures are suggested to combat threats at different layers but which countermeasures are really capable of counteracting these threats are very difficult to identify. In this paper, a detailed analysis of globally identified security threats within a cognitive radio network (CRN) is presented. Upon careful review of the researches been done so far, graphical representation of potential countermeasures to combat security threats at each layer is given. There is vast scope of implementing these countermeasures and measure the performance of cognitive radio networks.
Keywords: CRN, Countermeasures, Security threats.

1. INTRODUCTION

An emerging technology named as Cognitive Radio is capable of resolving the drawback of under-utilization of wireless spectrum by letting secondary users to opportunistically access the licensed channels without disturbing the communications of the primary users [1]. In general, users are categorized into two types, a user who possess a valid licence for the defined segment of the spectrum termed as primary or incumbent users while a user who holds access of spectrum in an opportunistic manner without causing harm to the existing communication of primary user is known as cognitive or secondary user [2]. The working of a CR device is based on its capability of sensing its environment, identifies the white or the unused portion in the spatial domain and picks it as per the requirement [3]. Numerous spectrum sensing techniques are available so far which are cyclostationary detection, filter matching and energy detection etc. and also multiple techniques are available for spectrum management and decision.

An advancement in the domain of wireless communication paves the ways towards a revolutionizing approach like CRNs which are supposed to efficiently manage the spectrum inadequacy problem through intelligent utilization of available vacant spectrum bands. Nevertheless, because CR networks are wireless in design, they face all the security threats seen in conventional wireless networks because of which it is vulnerable to multiple attacks [4]. The security objectives of any wireless networks are segregated into four categories which are confidentiality, integrity, availability and access control. Confidentiality denies, unauthorized access of information by the unapproved users while integrity recognizes any intentional or unintentional modifications in data communication. Similarly, availability allows accessing network resources by the individual when required by them and access control prohibits resources of the network to authorized users or devices only [2-3].

Although CR in a wireless network is an efficient strategy to successfully address the problem of the wireless spectrum depletion, simultaneously the features of CR resulted into creation of completely different forms of security risks and problems in a networks. Therefore, having good security safeguards is the most critical criteria for CRN. Although security threats and challenges in CRN has been studied for many years and there is a significant number of contributions that concentrated particularly on CRNs security which are categorized into two parts - theoretical contributions, and contributions explaining detailed approaches for the prevention and detection of particular security attack [5]. Furthermore, it has been observed that the attacks usually adopts a hierarchical approach like the attacks such as Objective Function, Primary User Emulation (PUE), and Jamming occur in the Physical Layer [4]. Similarly, some of the link layer attacks are Spectrum Sensing Data Falsification (SSDF) and the Control Channel Saturation DoS. Likewise, attacks such as HELLO Flood, Sybil attack and Sinkhole attack takes place at Network Layer while attacks such as the Key Depletion Attack and Lion Attack happens at Transport Layer.

Besides, these attacks, there are some attacks, for instance Jellyfish Attack, might originates from one layer and have its influences and consequences on adjacent layers, these types of attacks are termed as cross-layer attacks [6]. However, the proposed security countermeasures at various layers of cognitive radio networks has not been well investigated until recently. In this article a systematic survey of various types of attacks in a cognitive radio network at different layers and their corresponding countermeasures and then a detailed comparison is developed to analyze the most effective countermeasure for elimination of specific security threat aroused at specific layer. A thorough

study of all the above attacks and the related methods for their identification is the main aim of this work. The major findings of this article are:

- An explanation of cognitive radio network in scope of spectrum scarcity and the inadequate utilization of the spectrum.
- A description and classification of the already existing security threats associated to the cognitive radio network
- Comparative analysis of the already prevailed countermeasures at various layers of cognitive radio network and observing the most effective countermeasures.

The paper is divided in different sections. Section 2I gives a detailed literature review concerning existing work in context of spectrum sensing and management, security threats and countermeasures in CRN. In Section 3, comparative analysis of various security threats at different layers of TCP protocol stack is carried out. Section 4 describes the countermeasures at various layers are presented in the form of graphs.

2. LITERATURE REVIEW

The remarkable evolution of cognitive radio over the past several years emphasizes more on this domain and it emerged out as an active research area for the researchers. With the advancement in the CR technology, the concerns of operational robustness and security implications obtained significance. While several studies on this topic have been developed so far. Some important researches can be summarized as follows:

Alireza Attar et.al [1] (2012) proposed a review article based on security challenges in cognitive radio network. This article primarily focuses on the exogenous or external attacker, intruding faulty nodes and selfish CR nodes. Furthermore, infrastructure related threats were discussed which are infrastructure-based CRNs as well as infrastructure-less networks. Out of multiple spectrum sensing techniques, specifically, energy detection spectrum sensing with additive white Gaussian noise (AWGN) and fading channels is taken into consideration since it is the most extensively used spectrum sensing approach in terms of implementation and flexibility of deployment in both scattered and centralized CRNs. Besides consequences of such attacks on CRN is discussed along with the probable solutions to combat those security attacks. The author concluded with the suggestion that future researches can be developed in directions like A. CRN Security based on Cross-Layer Approach B. Distributed CRN Monitoring C. Joint Link and System Level Learning, D. Incentive-Based Security Mechanisms, E. Reliable Spectrum Sensing Schemes, F. Anti-Jamming CR Techniques, G. Robust Cognitive Communications.

A.C Sumathi et al. [2] (2012) proposed that primary user emulation attack is the major threat in the cognitive radio networks and discussed various defensive methods against PUE attack. These defensive methods against PUE attacks include, DRT and DDT, LocDef, social Network, Fenton's approximation and Markov inequality, Wald's sequential Probability ratio test, Variance detection method, NEAT, Robust Spectrum Decision protocol, 3D-CTMC and Sybil attack are overviewed in detail.

Alexandros G. Fragkiadakis et al. [3] (2013) The authors categorized the security threats on the basis of two essential features of cognitive radios: reconfigurability and cognitive capability, and defines that the security attacks which are based on transmission of false interpretations associated to spectrum sensing comes under cognitive capability while attackers utilizes the malicious code to exploit the cognitive radios cognitive radios and results in reconfigurability. This paper discusses the possible attacks and their characteristics on several layers.

Zhihui Shu et al. [4] (2013) overviewed several existing security attacks to the physical layer in cognitive radio networks. Besides, countermeasures to defend against these attacks were also discussed.

Suchismita Bhattacharjee et al. [5] (2014) discussed the security threats of Cognitive Radio Networks and analysed the attacks on three layers of CRN model such as physical, link network layer Overview of Primary User Emulation Attack (PUEA), Spectrum Sensing Data Falsification Attack (SSDF), Objective Function Attack (OFA), Sinkhole Attack, Jamming Attack, Cross- layer Attack,Control Channel Saturation, Hello Flood Attack, DoS Attack (CCSD), Lion Attack are discussed in detail.

Mahmoud Khasawneh, et al. [6] (2014) This article discusses the key problems, security threats and their mitigating strategies in CRN. The security attacks are discussed based on the type of TCP protocol layer it has affected. Besides, discussing the attacks on the complete model, security requirement on various layers has also been discussed.

José Marinho et al. [7] (2015) This article is a broad and interconnected view of key threats impacting CRN in context of the identification of primary users, with a special emphasis on PUE and SSDF attacks. This research work concluded with the suggestions that distributed CRN can offers a better solution as compared to centralized strategies, while complicating the designing of suitable techniques. Furthermore, effects of the attacks and their possible countermeasures has been addressed.

Rong Yu et al. [8] (2015) This paper discusses security issues resulting from attacks on physical layer in CRN. Two-level database-assisted monitoring technique is suggested to protect CR networks against attacks like PUE .The proposed approach incorporates energy detection and location verification for reliable and quick detection. Furthermore, an admission control based security strategy is proposed to minimize the efficiency loss of a CR network due to PUE attack. This paper overviewed classification of Attackers-Selfish and Malicious Attackers, Power-Fixed and Power-Adaptive Attackers, Static and Mobile Attackers.

Shruthi N1 et al. [9] (2016) This paper surveyed the existing detection techniques as well as counter measures relevant to Network layer attacks. They are Sinkhole Attacks, Sybil Attacks, Hello Flood Attacks, Page Hole Attack, Ripple Effect, Channel Endo Parasite Attack, Network Endo Parasite Attack (NEPA), Homing, Node Replication/Clone Attacks, Selective Forwarding, Alteration, Spoofed and Replay of information, Acknowledgement Spoofing, Rushing. Shekhar Raj et al. [10] (2017) discussed security attacks on various layers of CRN model besides providing the possible countermeasures of these attacks.

3. LAYER SPECIFIC SECURITY THREATS

This section briefly describes the TCP protocol stack and the fundamental roles and responsibilities of each layer is depicted in Fig. 3.1.

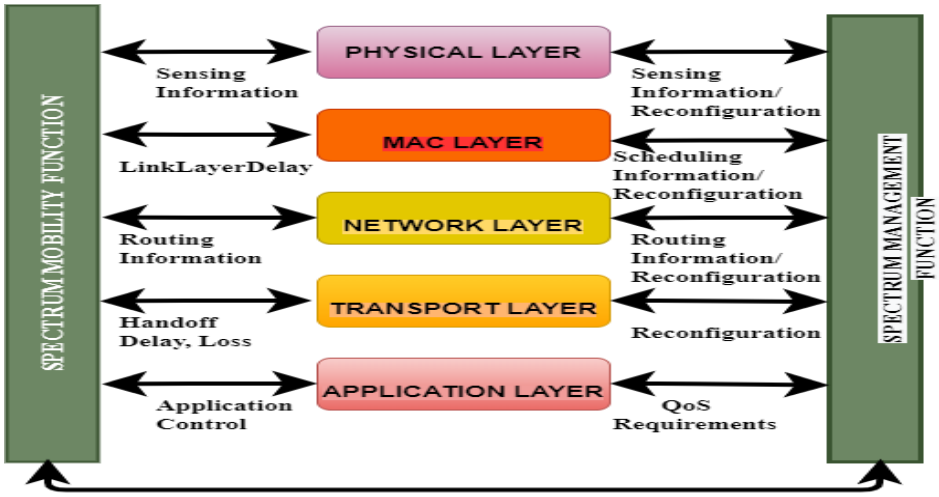

Fig. 3.1. TCP Protocol Stack

Now different protocols layers of CRN and potential security threats at each layer are discussed in following paragraphs.

3.1 Physical Layer

This layer is responsible for the data transmission [11]. While on the other hand, the features of CRN have present new challenges to the security of physical layer. Since, the network is comprised of both primary users and secondary users and secondary users should be capable of identifying the distance between malicious nodes and primary users. Secondly, it should be capable of recognizing the precision of sensing data obtained [12].

3.2 MAC/ Link Layer

Link layer effectively performs framing of data packet while restricting its connection to the physical layer [11]. It is responsible for controlling the data traffic, error identification and correction for numerous users present within the identical network. Thus in many security threats, the MAC address is at the key target [15].

3.3 Network Layer

Wireless network in CRN requires routing of data which is controlled by the network layer. It is also responsible for enforcing the QoS requirement in a network [13-14]. CRN routing is difficult because of its complex design and the strategies for spectrum handoff. CRN are also vulnerable to security risks because of the susceptibilities associated with wireless network architectures.

3.4 Transport Layer

This layer ensures transference of data between two participating devices or users in a network. This layer is responsible for multiple communication processes that include but are not restrained to: delivery of end-to - end data errors, recovery of errors, etc. Round Trip Time (RTT) is a way to analyse the performance of transport layer which can be explained as "the time taken to transmit a signal and receive its acknowledgment [14]."

3.5 Application Layer

Allocation of resources, effective QoS handling, defining users and allowing the application software to be used on communication devices are some of the core functions performed by the application layer. Since, this layer is the bottom most layer in the TCP protocol stack, it will also be affected by the attack charged in adjacent layers [16-17]. Therefore, CRNs running on application software and are also vulnerable to undesirable viruses. This cognitive radio virus has got the tendency of replicating itself by over writing memory, consuming space and executing undesirable codes. The characteristics of CRN supports self-propagation system, which in further allows viruses to propagate to other users easily resulting in countless untrue spectrum decisions. Additionally, because cognitive users are artificially smart machines, they can adapt to the malicious environment and continue to function with ensuing false decisions.

3.6 Cross Layer

The attacks in Cross-layer influence several communication protocol layers, and therefore can be responsible for significant network devastation. Jellyfish attack is an example which originates from network layer but targets transport layer [18]. Therefore, similar types of attacks can target multiple layers of communication protocol stack. Besides, attacks like Lion attack and jamming attacks are also part of this category [18-19].

Security threats on five layers of TCP protocol stack in CRN are summarized in Table 3.1.

Table-3.1 Security Threats on Various Layers of TCP Protocol Stack

Physical Layer	MAC or Link Layer	Network Layer	Transport Layer	Cross layer
Primary User Emulation (PUE) attack, HELLO attack, Objective Function attack (OFA), Jamming attack, Common Control Data attack (CCD)	Spectrum Sensing Data Falsification attack (SSDF) or Byzantine, Control Channel Saturation attack (CCS), Beacon, Denial of Service attack (DOS), Biased Utility attack, Feedback attack, False Fabrication attack, Flooding attack	Hello Flood attack (Routing), Sinkhole attack, Sybil Attack, blackhole attack, Lowcost ripple effect, Channel endo or network endo parasite attack, grayhole attack, homing attack, nodes replication attack, selective forwarding attack, wormhole attack, Alteration or spoofed or replay of information attack, Misdirection internet SMURE attack, Acknowledgement spoofing attack, Rushing attack	Lion attack, Key depletion attack, Jellyfish attack,	Lure attack

Fig. 3.2 depicts typical number of possible security attacks in each layer of CRN TCP protocol stack.

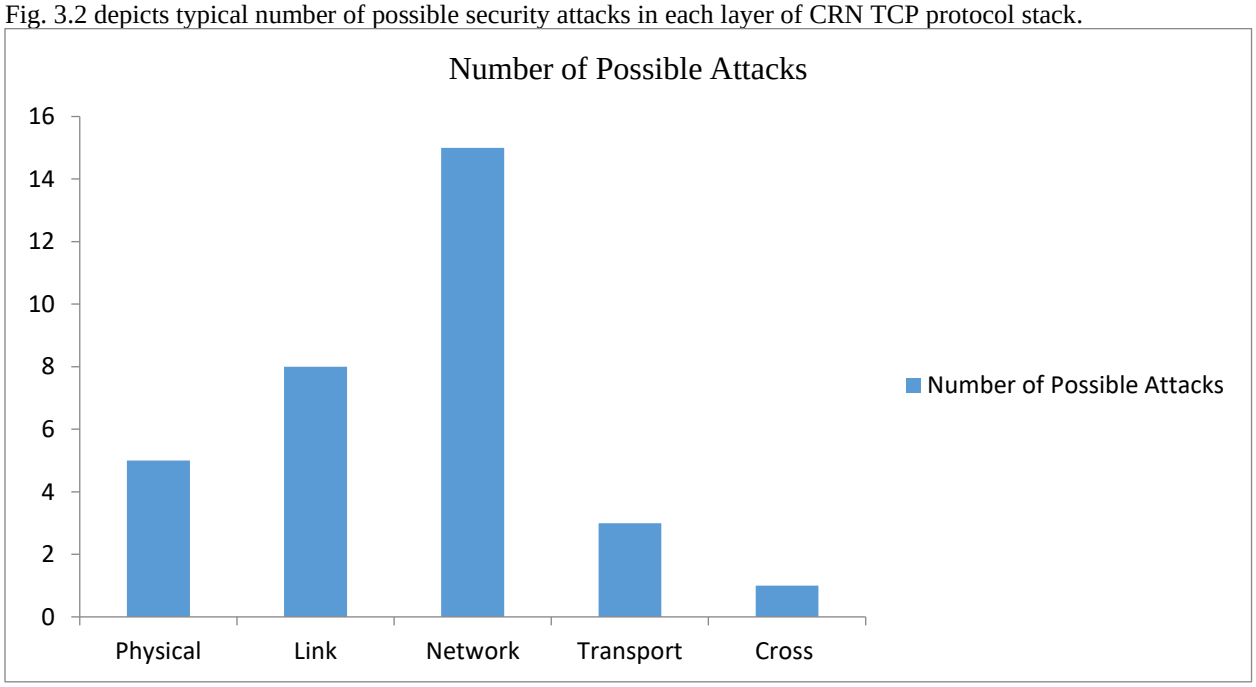

Fig. 3.2 Number of Possible Security Attacks on Various Layers

4. SECURITY COUNTERNEASURES

Countermeasures against different security attacks at various layers of CRNs are discussed next.

4.1 Countermeasures at Physical Layer

Fig. 4.1 shows the possible countermeasures against security threats at physical layer of TCP protocol stack in CRN.

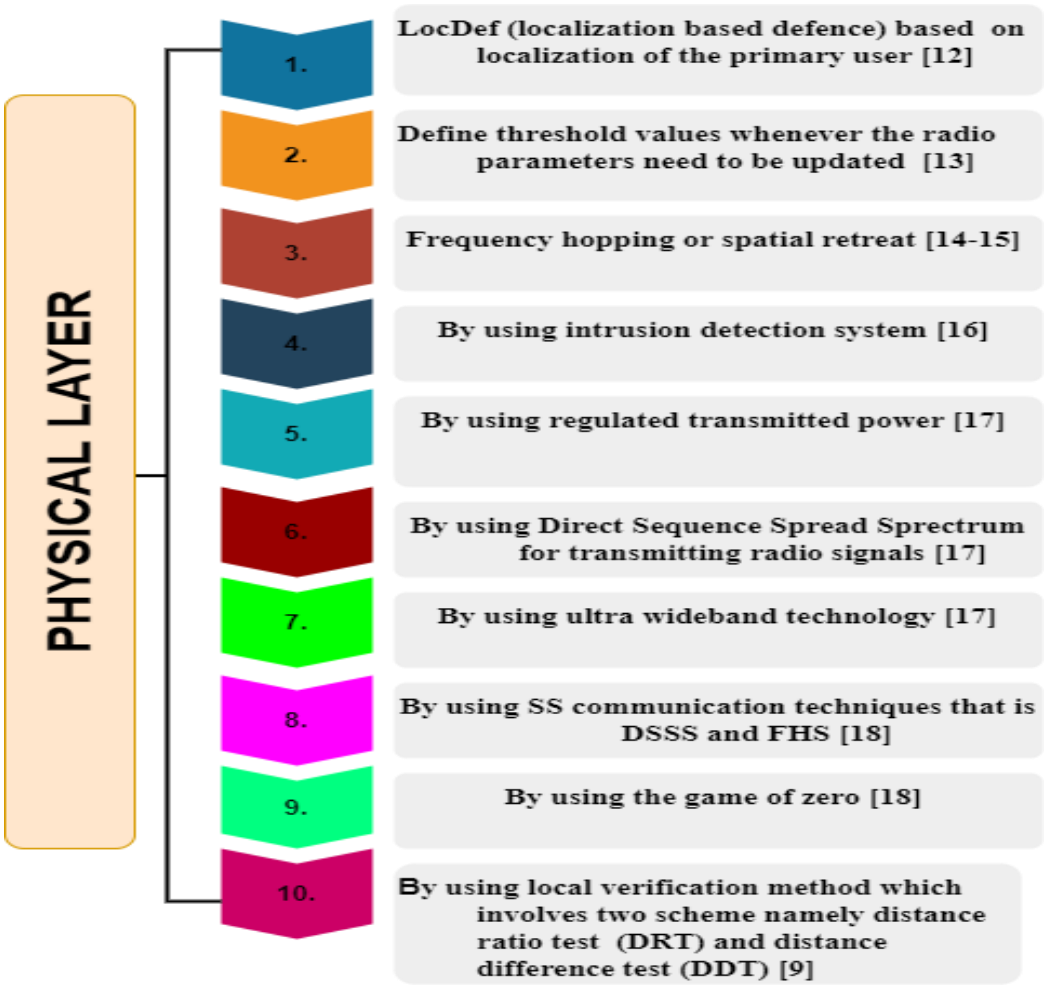

Fig. 4.1 Countermeasures at Physical Layer

4.2 Countermeasures at MAC or Link Layer

The possible countermeasures approaches for security threats at MAC or link layers can be generalized as shown in Fig. 4.2.

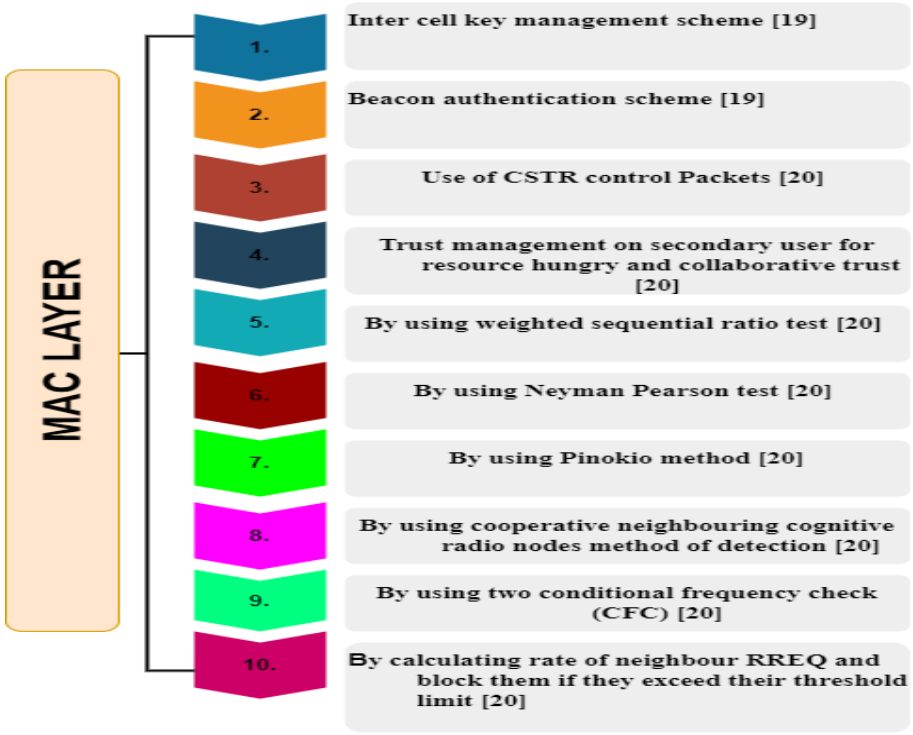

Fig. 4.2 Countermeasures in MAC/Link Layer

4.3 Countermeasures at Network Layer

Countermeasures against security threats in network layer are summarized and depicted in Fig. 4.3.

Fig. 4.3 Countermeasures in Network Layer

4.4 Countermeasures at Transport Layer

In this sub-section, the possible countermeasures against security threats at transport layer are represented in Fig. 4.4.

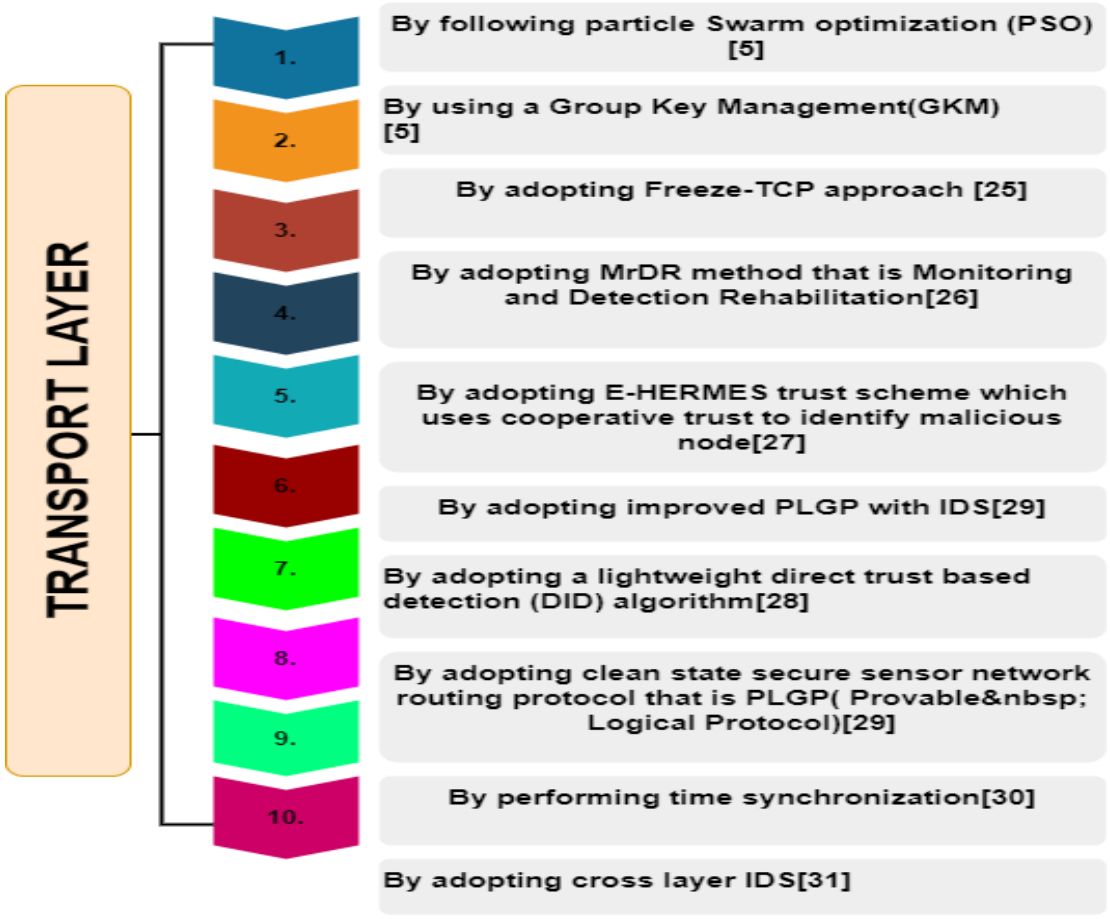

Fig. 4.4. Countermeasures in Transport Layer

DOI Number: https://doi.org/10.30780/specialissue-ICACCG2020/020
Paper Id: IJTRS-ICACCG2020-020

4.5 Countermeasures at Cross Layer

Lastly, the concept of cross layer attacks and the possible defence framework is depicted in Fig. 4.5.

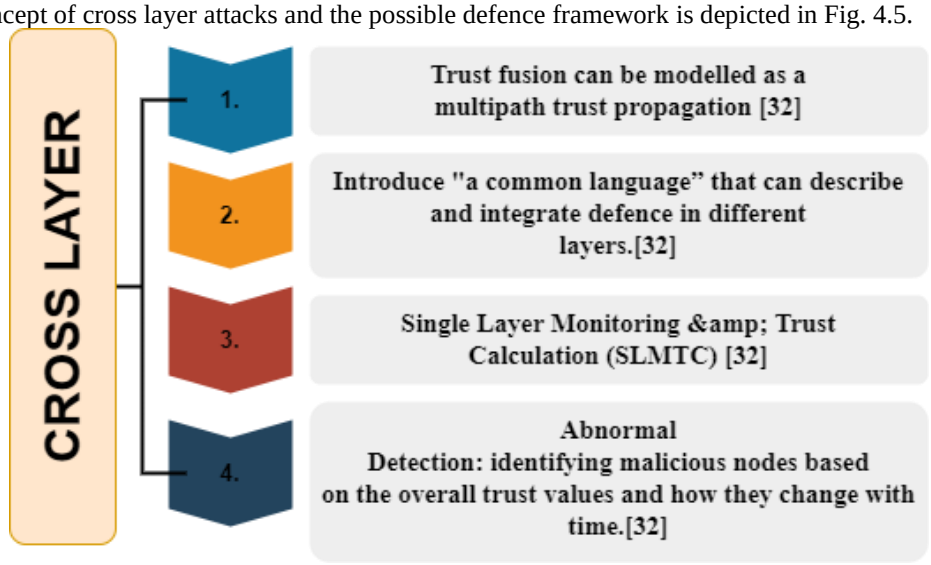

Fig. 4.5. Countermeasures in Cross Layer

DISCUSSION AND CONCLUSIONS

To evaluate the security threats on various cognitive radio network protocol levels, a detailed review was carried out and the most impactful threats were outlined in tabulated form. In addition, its potential countermeasures are analyzed in the form of figures. Cognitive radio is an extensive diverse field which attracts numerous researchers for study with a significant range of security and precise sensing challenges in the field of wireless communications. In this paper all potential security threats at various layers of TCP protocol stack of CRN are discussed. This is followed by graphical presentation of some potential countermeasures against security threats at various levels of CRN. However, the security issues in a CRN environment are still in its immature phase and allow the research community to do a more detailed analysis and evolve solutions.

REFERENCES

[1] Attar, A., Tang, H., Vasilakos, A.V., Yu, F.R. and Leung, V.C., 2012. A survey of security challenges in cognitive radio networks: Solutions and future research directions. Proceedings of the IEEE, 100 (12), pp.3172-3186.

[2] Fragkiadakis, A.G., Tragos, E.Z. and Askoxylakis, I.G., 2012. A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys & Tutorials, 15(1), pp.428-445.

[3] Sumathi, A.C. and Vidhyapriya, R., 2012, November. Security in cognitive radio networks-a survey. 12th IEEE International Conference on Intelligent Systems Design and Applications (ISDA), pp. 114-118.

[4] Shu, Z., Qian, Y. and Ci, S., 2013. On physical layer security for cognitive radio networks. IEEE Network, 27(3), pp.28-33.

[5] Bhattacharjee, S., Rajkumari, R. and Marchang, N., 2014. Cognitive radio networks security threats and attacks: A review. International Journal of Computer Applications, 975, p. 8887.

[6] Khasawneh, M. and Agarwal, A., 2014, March. A survey on security in Cognitive Radio networks. 6th IEEE International Conference on Computer Science and Information Technology (CSIT), pp. 64-70.

[7] Marinho, J., Granjal, J. and Monteiro, E., 2015. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP Journal on Information Security, 2015(1), p.4.

[8] Sharma, G. and Sharma, R., 2015, December. A review on recent advances in spectrum sensing, energy efficiency and security threats in cognitive radio network. IEEE International Conference on Microwave, Optical and Communication Engineering, pp. 114-117.

[9] Yu, R., Zhang, Y., Liu, Y., Gjessing, S. and Guizani, M., 2015. Securing cognitive radio networks against primary user emulation attacks. IEEE Network, 29(4), pp.68-74.

[10] Zhu, J., Zou, Y. and Zheng, B., 2017. Physical-layer security and reliability challenges for industrial wireless sensor networks. IEEE access, 5, pp.5313-5320.

[11] Raj, S. and Sahu, O.P., 2017, Countermeasures to security threats/attacks on different protocol layers in cognitive radio networks: An overview. IEEE International Conference On Smart Technologies For Smart Nation (SmartTechCon), pp. 1076-1082.

[12] Singal T. L., 2012. Analog and Digital Communications, 1st Edition, Tata McGraw-Hill Education, pp. 867-868.

[13] Leon O., Serrano J. H. and Soriano M., 2010, Securing Cognitive Radio Networks," International Journal of Communication Systems, vol. 23, pp. 633–52.

[14] W. El-Hajj, H. Safa, and M. Guizani, 2011, Survey of Security Issues in Cognitive Radio Networks," Journal of Internet Technology, vol. 12, no. 2, pp. 25–37.

[15] Singal, T. L., 2013. Issues of interoperability among heterogeneous wireless communication networks, International Journal of Computing and Business Research, Vol. 4, Issue 2, pp. 1-10.

[16] León, O., Hernández-Serrano, J. and Soriano, M., 2010. Securing cognitive radio networks. international journal of communication systems, 23(5), pp.633-652.

[17] Rai, A., Sehgal, A., Singal, T. L., Agrawal, R., 2020, Spectrum Sensing and Allocation Schemes for Cognitive Radio, Machine Learning and Cognitive Computing for Mobile Communications and Wireless Networks, Wiley, pp 91-130.

[18] Attar, A., Tang, H., Vasilakos, A.V., Yu, F.R. and Leung, V.C., 2012. A survey of security challenges in cognitive radio networks: Solutions and future research directions. Proceedings of the IEEE, 100(12), pp.3172-3186.

[19] Chang, S.Y., Hu, Y.C., Laurenti, N., 2015. Simplemac: A simple wireless MAC-layer countermeasure to intelligent and insider jammers. IEEE Transactions on Networking, 24(2), pp.1095-1108.

[20] Rajalakshmi, S. and Saravanan, K., 2013. Survey on link layer attacks in cognitive radio networks. International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), 3(6).

[21] Shruthi, N., Vinay, C.K., 2016. Network layer attack: Analysis & solutions a survey. IOSR Journal of Computer Engineering, 18(2), pp.67-80.

[22] Mamatha, G.S. and Sharma, D.S., 2010. Network layer attacks and defense mechanisms in MANETS-a survey. International Journal of Computer Applications, 9(9), pp.12-17.

[23] El-Hajj, W., Safa, H. and Guizani, M., 2011. Survey of security issues in cognitive radio networks. Journal of Internet Technology, 12(2), pp.181-198.

[24] Karlof, C., Wagner, D., 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2-3), pp.293-315.

[25] Hernandez-Serrano, J., León, O. and Soriano, M., 2011. Modeling the lion attack in cognitive radio networks. EURASIP Journal on Wireless Communications and Networking, pp.1-10.

[26] Alsumayt, A., Haggerty, J. and Lotfi, A., 2015, October. Comparison of the MrDR method against different DoS attacks in MANETs, IEEE Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 219-224.

[27] Zouridaki, C., Mark, B.L., Hejmo, M. and Thomas, R.K., 2009. E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks. Ad Hoc Networks, 7(6), pp.1156-1168.

[28] Laxmi, V., Lal, C., Gaur, M.S. and Mehta, D., 2015. JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET. Journal of Information Security and Applications, 22, pp.99-112.

[29] Geethu, R. and Babu, H.K., 2014. Provable Security Against Resource Depletion Attacks in Wireless Ad hoc Networks. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), 3(3), p.120.

[30] Chelli, K., 2015, July. Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the World Congress on Engineering, Vol. 1, No. 20.

[31] Bhawsar, D. and Suryavanshi, A., 2015. 'Collaborative intrusion detection and prevention against jellyfish attack in MANET. International Journal of Computer Applications, 129(13).

[32] Wang, W., Sun, Y., Li, H. and Han, Z., 2010, December. Cross-layer attack and defense in cognitive radio networks. IEEE Global Telecommunications Conference GLOBECOM 2010 (pp. 1-6).

ABOUT THE AUTHORS

Srishti Priya Chaturvedi is research scholar, pursuing her Masters in Electronics and Communication Engineeing at Chitkara University, Punjab. She is CCNA certified at level 1 and 2. Earlier she has worked as network analyst with Tech Mahindra, India. Her research area includes power optimization methods in FPGA, computer and wireless networks.

T. L. Singal is currently working as Professor at Chitkara University, Punjab. He is an alumnus of NIT Kurukshetra India (1976-81). He has worked with telecom industries in India, Germany and USA. He has authored text-books `Wireless Communications (2010)', `Analog and Digital Communications (2012)', `Digital Communication (2015)' and `Optical Fiber Communications: Principles and Applications (2017)' with McGraw-Hill Education and Cambridge University Press. His research areas include cognitive radio networks and LTE 5G cellular technology.