INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

Adaptive Security Mechanism for Cognitive Radio Communications based on Robust Authentication

Mehakpreet Kaur
IT department, CEC Landran
Mohali

Navleen Kaur
IT department, CEC Landran
Mohali

Abstract—the fundamental techniques for cognitive radio standard generates the new security threats and the primary operative issues and challenges to wireless communications. Spectrum occupancy failure, the policy management failures, wireless node localization failures, transceiver failures, framework problems and other concerns must be efficiently covered and resolved while imposing the security techniques over the cognitive channels. In the process, it will produce the security threats-primary user emulation attacks. When the attacker has detected the idle spectrum, he will send out a signal similar to the primary user's signal in this band. The attacks will affect the secondary user detect the idle spectrum and the spectrum cannot be used effectively. An attacker occupies the unused channels by emitting a signal with similar form as the primary user's signal so as to prevent other secondary users from accessing the vacant frequency bands. The performance of the proposed security model for cognitive radio channels would be evaluated in the performance parameters of security packet volume, authentication delay, security system overhead, etc. The trust and authentication based proposed model will be designed to offer the robust security level over the cognitive channel.

Keywords—Cognitive Radio, Security, Authentication, Tunnelling security.

I. INTRODUCTION

In the past one decade, we have seen the rapid growth in wireless systems communications just because of smart phones and mobile devices which leads to skyrocketing the demand of commercial spectrum. For example, AT&T predicts the increase in data usage of 5000% in next three years, Yankee group predicts from 2009 to 2015, the 29-folds increase in USA mobile traffic. There is a need of minimum 800MHz spectrum for US estimated by the CTIA. Wi-Fi increases the demand and need of unlicensed bandwidth for applications like safety, entertainment systems, embedded wireless devices, home sensors, medical and smart grid control.

This is a very crucial challenge to meet the need of bandwidth increase since suitable bands are already allocated. After getting through the studies, this could be deduced that the 90% of spectrums are not utilized properly and that means in near future there may be a dime need of unallocated spectrums to host and make communication and network technologies. Nowadays static spectrum allocation is used by spectrum policies which produces more efficient infrastructure but that doesn't mean that frequency bands can be restricted to some area. This flaw attracts more attention of researchers in favor to remove it. To avoid this flaw, Dynamic Spectrum Access (DSA) is used to allocate the spectrum bands more dynamically. It requires advances in new policies, technologies and economic models.

Cognitive Radios are radically improves the efficiency and utilization of spectrum as the disruptive technology. The basic features of cognitive radios includes efficient spectrum use, adapting transmission waveform dynamically, channel access methods, networking

© 2016, IJARIIT All Rights Reserved

protocols as required for better network transmission and performance of application. The key application of cognitive radios is more efficient, aggressive dynamic spectrum access and flexibility. The community of researchers has made progress in addressing the many research challenges faced by the cognitive radio cognitive networks (CRCN) and DSA. The main gaps deduced by studying the literature are effective block building, dynamically optimize spectrum use over large-scale deployment of network. Recent developments such as the FCC TV white space ruling, an example of DSA based on a primary-secondary user model, and LTE-A, which relies on flexible spectrum use, offer great opportunities to demonstrate the potential value of cognitive networks and DSA. Failure to act on these opportunities could delay commercial deployment for many years.

After mentioning the research gaps like identifying both the long term and short term research challenges. Now, policy researchers are exploring the new and novel techniques to improve the potential use of CRCN and commercializing it in near future. A more detailed discussion on the above topics can be found in the popular model CRN1's documentation. The breakout session didn't work on elaborating the complex structure of above topics despite of focused on complex topics interaction. The mentioned challenges are need to be addressed before deployment of cognitive radios. Some key point's needs to be elaborated are: interaction between policy, moving from components to networks, evaluation of cognitive networks and cognitive networking beyond DSA.

II. LITERATURE REVIEW

Yu, Rong et. al. [1] has worked towards securing cognitive radio networks against primary user emulation attacks. In this paper the authors have focused on security problems arising from Primary User Emulation (PUE) attacks in CR networks. They have presented the comprehensive introduction to PUE attacks, from the attacking rationale and its impact on CR networks, to detection and defense approaches. The security of the CR networks during the PUE attacks is protect by the two-level authentication mechanisms proposed in this research. For fast and reliable detection both energy detection and location verification are combined. An admission control based defense approach is proposed to mitigate the performance degradation of a CR network under a PUE attack. Zhao, Nan et. al. [6] has proposed the energy-efficient cooperative spectrum sensing schemes for cognitive radio networks. Proposed model have two stages in spectrum sensing using time saving one-bit cooperative spectrum sensing and energy efficient. They have addressed the issue of blind signals and worked to eliminate or minimize the data drop by proposing new technique based on sensing. The proposed sensing technique is considered energy efficient by the authors and they have justified it with the various performance evaluations. They have added only one-bit decision is sent by each secondary user to minimize the overhead. The second proposed algorithm for the local decisions of the coarse detection can be fully utilized, and energy consumption can be reduced with its sensing performance near to the first algorithm. To ensure the results, plenty of simulations are performed, and the results show that the sensing time and energy consumption are both reduced significantly in the proposed schemes.

Umar, Raza et. al. [2] has performed the comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks. The authors have discussed the functionality of the cognitive radios. They have also performed an in-depth comparative survey of various spectrum awareness techniques under this survey. Specifically, to remove the key challenges in SS are discussed and their possible solution. A SS classification is represented to address the selection criteria for sensing method. To identify the future research problems occurred to be removed by the researcher for both cooperative and non-cooperative sensing schemes are reviewed. Ren, Wei et. al. [3] proposes a model to work on temporal traffic dynamics to improve the connectivity of adhoc CRCN. In this paper, the authors have worked with the cognitive radio networks for ad-hoc networks. Instantaneously connection is computed to evaluate the scaling of the multihop delay which is critically dependent on secondary network. We establish the scaling law of the minimum multihop delay with respect to the source-destination distance when the propagation delay is negligible. Rebeiz, Eric et. al. [4] has developed energy-Efficient Processor for Blind Signal Classification in Cognitive Radio Networks.

III. FINDINGS OF LITERATURE REVIEW

The existing model protects the CRCN from the primary user emulation attack (PUEA) and also they evaluated the performance of system against the PUEA attack. The solution provided by the existing systems uses the propoer weight in order to reduce the effect of PUEA. The existing solution is framed to build security mechanism against the PUEA and when is not effective against the multi-purpose PUEA attack. The existing solution does not offer the message data encryption. The existing solution is not effective against multi-purpose PUEA, and does carry the higher probability of being exposed. The existing solution also does not authenticate the attackers (malicious users) which may be utilized to overturn the PUEA attacks over the secure channel. In the proposed model, we have made efforts to mitigate all of the shortcomings of the existing model.

IV. METHODOLOGY

© 2016, IJARIIT All Rights Reserved

The proposed model is designed to mitigate the problem of existing system to provide the security against the PUEA with malicious injection to take on authentication channel. We are proposing a security framework in the cognitive radio to protect against the multi-purpose PUEA attacks. The proposed work will include a secure authentication model for the purpose of initial setup security and secure data exchange afterwards. The PUEA attack is launched to take the authority of the computing resources and to act as the controller farther than the existing users. The PUEA is launched from hacker's device/s to the target device. In the PUEA attack, the attacker uses the direct channel to discover the node information of the target node and establishes the connection with the other node, which can be prevented by using the stronger authentication mechanism. The proposed solution authenticates the node before receiving any kind of packet streams sent from them. The proposed solution will be using the secure key exchange scheme for authentication. In the research, we are proposing the lightweight solution to mitigate the shadow fading using the one-bit padding factor with the data packets or acknowledgements exchanged between the two cognitive ends. The proposed model relies upon the bit-information exchange which is extracted and sequenced on the other end, and analyzed for the spectrum availability pattern. The data scheduling is done according to the fading channel once the fading pattern is found and sequenced in the time-domain. The frequency domain is designed according to the spectrum availability factor. The proposed model is expected to return the performance parameters of data delivery ratio, probability of detection, probability of false alarm, data drop ratio, etc.

V. CONCLUSION

The cognitive radio channels are the intelligent radio based data propagation channels which are established to transfer the heavy loads of data over the microwave channels prominently. The cognitive radio models are capable of understanding the spectrum engagement and available in the frequency spread. All of the spectrum frequencies are analyzed by using the spectrum sensing methods, which are further utilized to prepare the aggregate channels for data propagation over the distance wireless ends. The requirement of the security model arises with the emergence of the various types of the security attacks over the cognitive radio networks. The security practices and authentication methods are the must have techniques to protect the cognitive radio channels from the various types of attacks, which includes the masquerading, jamming, snooping, etc. In this paper, the robust tunneling mechanism has been proposed for the imposition of the secure wireless channel across the cognitive radio ends. The proposed model is aimed to solving the issues of security robustness, security system overhead, and authentication delay and communication efficiency.

REFERENCES

[1] Yu, Rong, Yan Zhang, Yi Liu, Stein Gjessing, and Mohsen Guizani. "Securing cognitive radio networks against primary user emulation attacks."*Network, IEEE* 29, no. 4 (2015): 68-74.

[2] Umar, Raza, and Asrar UH Sheikh. "A comparative study of spectrum awareness techniques for cognitive radio oriented wireless networks." *Physical Communication* 9 (2013): 148-170.

[3] Ren, Wei, Qing Zhao, and Ananthram Swami. "Temporal traffic dynamics improve the connectivity of ad hoc cognitive radio networks." *IEEE/ACM Transactions on Networking (TON)* 22, no. 1 (2014): 124-136.

[4] Rebeiz, Eric, F-L. Yuan, Paulo Urriza, Dejan Markovic, and Danijela Cabric. "Energy-Efficient Processor for Blind Signal Classification in Cognitive Radio Networks." (2014): 1-13.

[5] Incebacak, Davut, Ruken Zilan, Bulent Tavli, Jose M. Barcelo-Ordinas, and Jorge Garcia-Vidal. "Optimal data compression for lifetime maximization in wireless sensor networks operating in stealth mode." *Ad Hoc Networks* (2014).

[6] Zhao, Nan, Fei Richard Yu, Hongjian Sun, and Arumugam Nallanathan. "Energy-efficient cooperative spectrum sensing schemes for cognitive radio networks." *EURASIP Journal on Wireless Communications and Networking*2013, no. 1 (2013): 1-13.

[7] Fragkiadakis, Alexandros G., Elias Z. Tragos, and Ioannis G. Askoxylakis. "A survey on security threats and detection techniques in cognitive radio networks." *Communications Surveys & Tutorials, IEEE* 15, no. 1 (2013): 428-445.

[8] Zou, Yulong, Xianbin Wang, and Weiming Shen. "Physical-layer security with multiuser scheduling in cognitive radio networks." *Communications, IEEE Transactions on* 61, no. 12 (2013): 5103-5113.

[9] Attar, Alireza, Helen Tang, Athanasios V. Vasilakos, F. Richard Yu, and Victor Leung. "A survey of security challenges in cognitive radio networks: Solutions and future research directions." *Proceedings of the IEEE* 100, no. 12 (2012): 3172-3186.

[10] Shu, Zhihui, Yi Qian, and Song Ci. "On physical layer security for cognitive radio networks." *Network, IEEE* 27, no. 3 (2013): 28-33.

[11] Baldini, Gianmarco, Taj Sturman, Abdur Rahim Biswas, Ruediger Leschhorn, Gyözö Gódor, and Michael Street. "Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead."*Communications Surveys & Tutorials, IEEE* 14, no. 2 (2012): 355-379.

[12] Elkashlan, Maged, Lifeng Wang, Trung Q. Duong, George K. Karagiannidis, and Arumugam Nallanathan. "On the security of cognitive radio networks."*Vehicular Technology, IEEE Transactions on* 64, no. 8 (2015): 3790-3795.

© 2016, IJARIIT All Rights Reserved