Int. j. inf. tecnol. (March 2020) 12(1):71–75
https://doi.org/10.1007/s41870-018-0183-3

ORIGINAL RESEARCH

Security enhancement technique in cognitive networks

Natasha Saini[1] · **Nitin Pandey**[1] · **Ajeet Pal Singh**[2]

Received: 6 July 2017 / Accepted: 13 April 2018 / Published online: 20 April 2018

Abstract Networking provides the main infrastructure for different recent applications. These applications are targets for various types of attacks. This research mainly focuses on evaluating the techniques used within cognitive system specifically CRN to ensure the security of the data as well as securing the communication. This will include the development of safety technologies in wireless communication in CRNs and also within wired exchanges in the core network. The study will also incorporate security mechanisms into cognitive network fundamentals as well as designing of monitoring framework (Spec Monitor) to monitor the system and detect malicious and abnormal behaviors. The research will evaluate security development techniques such as spectrum sensing in the cognitive network and non-parametric passive traffic monitoring in cognitive systems. A detailed technique is proposed to overcome the increasing complexity threats in Cognitive networks. The major focus of this technique is on host based approach and network based approach. Henceforth, there has been a comparative study on various attributes of information security.

✉ Natasha Saini
natashaaaa21@gmail.com

Nitin Pandey
npandey@amity.edu

Ajeet Pal Singh
drajeetpalsingh@gmail.com

[1] Amity Institute of Information Technology, Noida, India

[2] Raj Kumar Goel Institute of Technology, Ghaziabad, India

Keywords Cognitive network · Cognitive radio network · Network security · Wired communication · Wireless communication · Monitoring framework

1 Introduction

With the broad current range of data services as well as applications in cognitive systems, there is a need to manage the increasing complexity of threats [7]. The cognitive system is a new paradigm that addresses the challenge of growing number of and network devices. The cognitive network technology incorporates the capability of reasoning, learning, and planning by use of cutting edge techniques such as knowledge representation, context awareness, optimization and machine learning [3]. The cognitive network is a multidimensional aspect, and therefore this research will specifically focus on the Cognitive Radio Network (CRN). This is a part of the cognitive network over the wireless links that manages the utilization of spectrum resources within the network system [12].

The system networking area is among the fastest changing areas, which has various applications and services with enormous impact on modern world aspects such as economic growth, scientific development, education as well as entertainment [4]. However, the development of secure, robust and reliable network infrastructure is crucial to ensure effective human-to-human communication and human-to-machine communications in providing services such as e-banking, e-learning, e-payment, and e-health. The future cognitive system is expected to be more complex and will incorporate different connections such as wearable devices, mobile devices, as well as smart home appliances [21]. The cognitive network provides secure and optimized end-to-end communications for future

networking paradigm [17]. This research paper presents the definition of cognitive systems, security challenges as well as other research related to this study.

1.1 What is cognitive network?

The term cognitive incorporates conscious intellectual activities such as reasoning, thinking, remembering as well as the capability of reduced empirical factual knowledge [2]. However, the cognitive network is a type of network that possesses knowledge representation about the systems, events, devices and networks, which uses cognitive process (a cycle that perceives network conditions, and plan, decide and act on those conditions [9]. The Fig. 1 below shows the concept of cognitive network.

The cognitive cycle and knowledge presentation are two elements of cognitive systems. The cognitive cycle allows for the adjustment of functions perceived in their environment [21], while knowledge presentation acts as a prerequisite of self-awareness achievement.

2 Existing framework

The available work on how to secure cooperative spectrum mainly focus on the centralized network model. Contrary, this paper employs adaptive cognitive network techniques with learning capability. The attackers can adjust their strategies based on their local environments as well as the sensing algorithm. The article focused on the consensus-based spectrum as a sensing algorithm. On the other hand, the passive monitoring in the cognitive network is active in the study area. Initially, sniffers were introduced to measure the Wi-Fi network, as well as for the identification of malicious and anomalies WLAN usages. Later, large-scale monitoring infrastructure (Jigsaw) was submitted by Cheng to collect wireless traffic for network diagnosis to a great Wi-Fi network [6].

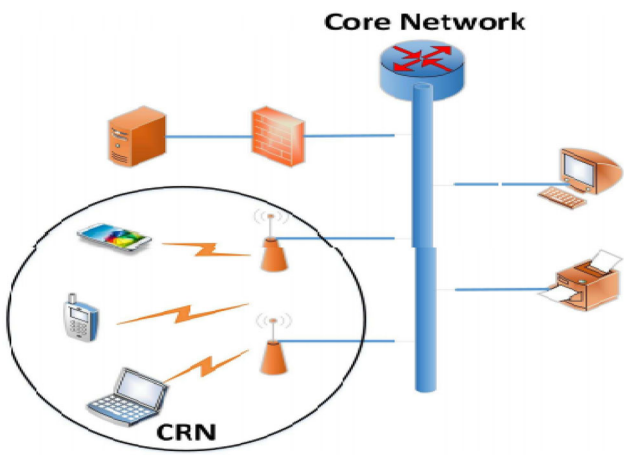

Fig. 1 Concept of cognitive network

Moreover, Zhang et al. [21] articulated that the mainstream jamming defense mechanisms focus on FHSS and DSSS to pre-shared secret keys are communicate without secret keys. The current powerful jamming aroused the interest of many researchers. Some demonstrated the feasibility of reactive jamming by use of software-defines radios. However, recent studies suggest the methods to secure the network against powerful wideband as well as high power jamming attacks [1]. The mechanisms only work for best for a conventional wireless network that is not based on OFDM. Significantly, the growing popularity of P2P botnets attracted a vast amount of research that focuses on tracking and removing them.

3 Proposed framework

The available work can be classified into two categories namely, hosted-based approaches and network-based methods. Zhang also proposed track the stealthy malicious activities by use of triggering relation network events discovery.

3.1 Secure consensus-based spectrum sensing

The spectrum sensing is fundamental to the success of the cognitive system, specifically, CRNs [8]. The fully cooperative spectrum sensing was proposed to ensure high-performance benefits in cognitive systems. The protocols are characterized by increased vulnerability to malicious attack, hence making defense mechanisms tight [18]. In this technique, the network model will be described as well as the review of spectrum sensing algorithm.

3.2 Network model

In this technique, we consider a cognitive system where PUs and SUs depend on each other. The PUs is located far from the secondary system. The different PUs is separated to reduce interference, and each SU requires sensing All PUs. In this case, the energy detection spectrum sensing technique is adopted [18]. The sensing output of each SU is regarded as the received PU power, Pi, expressed by the propagation model below:

$$\mathrm{Pi} = \mathrm{P0} - (10\alpha\log 10\,(\mathrm{di}/\mathrm{d0}) + \mathrm{Si} + \mathrm{Mi})\,(\mathrm{dB})$$

where P0 is the PU transit power, α is the path-loss exponent, d0 is the distance reference (1 m), di represents the distance from the SU to the Measured PU, Si is the power loss as a result of shadowing fading, while Mi represents the path fading effect. Notably, SUs exchange

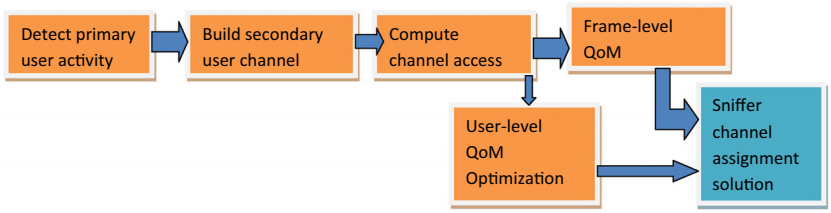

Fig. 2 Spec monitor system overview

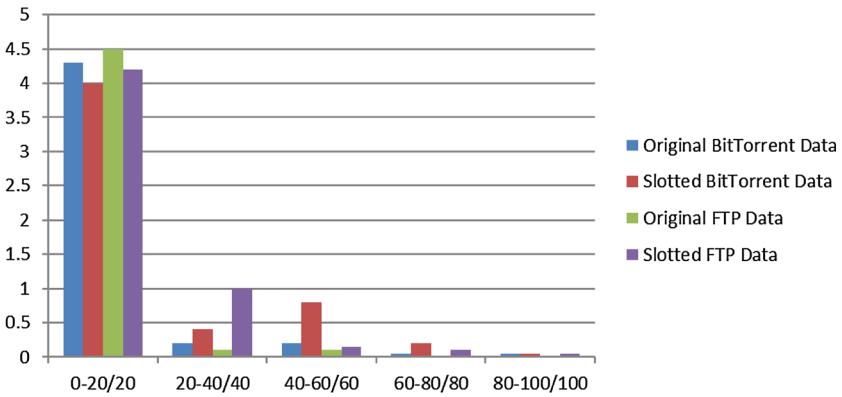

Fig. 3 Frame/active slot interval time distribution

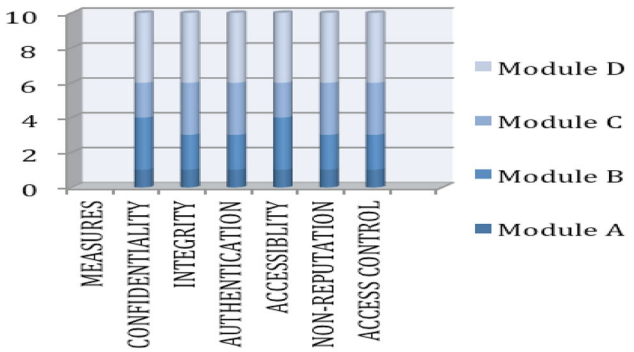

Fig. 4 Comparison on various attributes on information security

the local sensing measurements with the direct neighbors. After receiving the updates, each SU updates the sensing state based on the state update algorithm. According to Tang et al. [18] the consensus-based spectrum-sensing algorithm is expressed by use of discrete-time state equation shown below:

$$\text{xi}\ (\text{k}\ +1) = \text{xi}\ (\text{k}) + \text{€} \sum \text{j}\ \text{€Ni}\ (\text{xj}\ (\text{k}) - \text{xi}\ (\text{k})),$$

where xi (0) is the initial state of sensing a measurement of node ni, and xi (k) is the updated state at time k, where k = 0, 1, 2…. for each local node. € is the constraints on network parameter and connectivity [15].

3.3 Blocking attack

Blocking an attack is to prevent information transmission from an SU [10]. This can be expressed in the following Theorem: Let A € Mn × n be an adjacency matrix of the secondary network. However, after the blockage of several users by the attackers, the remaining system should satisfy:

$$(\text{I}\ +\ \text{A})\text{n} - 1 > 0.$$

In this case, the attackers would not achieve more benefit rather than defeating the secondary users [5]. Else, the entire secondary network is segmented to prevent attainment of the global decision.'

4 Non-parametric passive traffic monitoring technique

Passive motoring has been used by wireless sniffers to capture traffic strategically within the network [4]. This technique would employ the use of Spec Monitor, for the collection of the traffic by use of few sniffers in Wi-Fi such as CRNs [18]. This method utilizes the non-parametric density estimation to model SU's channel [16]. However, the approach does not make any assumption on Unknown channel access pattern distribution, for this reason, it offers a flexible design with little complexity that can be updated online [20]. The Spec Monitor constructs near-optimal security monitoring strategies by taking inputs from SUs' channel [19].

In this case, PU's networks are monitored and regulated by the service providers or specific wireless microphones (WMs) [14]. The sniffers are used to sense channels and gain the channel usage statistics, while the operational sniffers capture information. The sniffers are connected to a sniffer center to centralize the decision-making process

[20]. Every inspection sniffer is assigned multiple channels to scan through a sensing slot.It is been demonstrated in Figs. 2 and 3 respectively.

The sequential data × k (k = 1, 2, ….) is used to get the actual slot interarrival time for each channel; this is referred to as the time interval between two adjacent active slots [11]. For instance given n independent realizations represented as Xi (I = 1, 2, …, n) generated from unknown density function, the Gaussian KDE with bandwidth α is represented as:

$$F\ (x;\ \alpha) := 1/n\ \sum i = 1\ KG\ (x,\ Xi,\ \alpha),\ x \in R.$$

The Gaussian KDE is centered at the location Xi with a similar bandwidth of α. The KDE collects data of the active slots time that is measured by the inspection sniffers to generate the density estimate [20]. The above formula is used to identify the malicious as well as misbehaved cognitive network activities.

5 Results and conclusion

In this research, the key points of cognitive network security development have been explored and identified. The study designed efficient and effective security monitoring mechanisms to defend the cognitive network against sophisticated attackers that exploit vulnerabilities of CRNs [1]. The non-parametric passive traffic monitoring was also evaluated as the core technique used to protect the cognitive network from security threats. The methods for the calculation of safety loopholes were also identified together with other system defending mechanisms [13]. The evaluation incorporated mathematical formula, prototypes, and tested techniques. From the study, it is apparently believed that the cognitive networks defense mechanism play a critical role in guarding the system. The formula used for monitoring cognitive networks include Gaussian KDE with bandwidth $\alpha\{F(x;\ \alpha):\ = 1/n\sum i = 1\ KG\ (x,\ Xi,\ \alpha),\ x \in R\}$ and the propagation model $\{Pi = P0 - (10\alpha\log10\ (di/d0) + Si + Mi)\ (dB)\}$.

The performance evaluation has been done on basis of attributes of network security, which has been achieved for confidentiality, integrity, authentication, accessibility, non-repudiation and access control.

Module A: Secure Consensus-based Spectrum Sensing

Module B: Network Model

Module C: Blocking Attack

Module D: Non-Parametric Passive Traffic Monitoring Technique.

There has been analysis of various modules over various level of information security, which has been analyzed, and comparative analysis has been done for the same in Fig. 4 where the data has been compared and analyzed.

6 Future study

This study can be further advanced by use of open problems for the robust, reliable spectrum attack sensing based on the distributed detection outlier. Regardless of the presence of various researchers on robustness as well as fault tolerance of different outlier detection mechanisms, their impacts to the distributed protocols are not yet determined [2]. Theoretical and experimental study can be initiated on the relationship between the malicious nodes in cognitive networks and the detection performance.

Acknowledgment The authors would like to thank Amity Institute of Information Technology, Noida for providing specifications about the application scenario.

References

1. Avila LF, Souza AD (2015) Cognitive optical networks cognitive optical networks, elastic networks, dynamic networks. Anais Congr Iniciaç Cient Unicamp. https://doi.org/10.19146/pibic-2015-36979
2. Battu D (2014) Communication techniques. New Telecom Netw Enterp Secur. https://doi.org/10.1002/9781119004912.ch2
3. Chakraborty T, Misra IS (2013) VoIP based two-tier cognitive radio network: developing implementation techniques. In: 2013 IEEE international conference on communication, networks and satellite (COMNETSAT). IEEE, Indonesia. https://doi.org/10.1109/comnetsat.2013.6870853
4. Chehelcheshmeh SB, Hosseinzadeh M (2016) Quantum-resistance authentication in centralized cognitive radio networks. Secur Commun Netw 9(10):1158–1172. https://doi.org/10.1002/sec.1408
5. Dubey R, Sharma S, Chouhan L (2011) Security for cognitive radio networks. Cogn Radio Interf Manag Technol Strategy. https://doi.org/10.4018/978-1-4666-2005-6.ch013
6. Fragkiadakis AG, Tragos EZ, Askoxylakis IG (2013) A survey on security threats and detection techniques in cognitive radio networks. IEEE Commun Surv Tutor 15(1):428–445
7. Garcia-Alfaro J, Herrera-Joancomartí J, Melià-Seguí J (2014) Security and privacy concerns about the RFID layer of EPC Gen2 networks. Stud Comput Intell Adv Res Data Priv. https://doi.org/10.1007/978-3-319-09885-2_17
8. Hein D, Morozov S, Saiedian H (2011) A survey of client-side Web threats and counter-threat measures. Secur Commun Netw 5(5):535–544. https://doi.org/10.1002/sec.349
9. Kumar M, Dutta K (2014) A survey of security concerns in various data aggregation techniques in wireless sensor networks. Adv Intell Syst Comput Intell Comput Commun Dev. https://doi.org/10.1007/978-81-322-2009-1_1
10. Kumar S, Singhal D, Murthy GR (2014) Doubly cognitive architecture based cognitive wireless sensor networks. Secur Des Arch Broadband Wirel Netw Technol. https://doi.org/10.4018/978-1-4666-3902-7.ch009

11. Mathur CN, Subbalakshmi KP (2012) Security issues in cognitive radio networks. Cogn Netw. https://doi.org/10.1002/9780470515143.ch11
12. Michael M (2012) Physical security threats and measures. Handbook of computer networks distributed networks, network planning, control, management, and new trends and applications, vol 3, pp 596–631. https://doi.org/10.1002/9781118256107.ch38
13. Peres M, Chalouf MA, Krief F (2014) PHY/MAC signalling protocols for resilient cognitive radio networks. In: 2014 22nd international conference on software, telecommunications and computer networks (SoftCOM). Croatia. https://doi.org/10.1109/softcom.2014.7039116
14. Rafe V, Hosseinpouri R (2015) A security framework for developing service-oriented software architectures. Secur Commun Netw 8(17):2957–2972. https://doi.org/10.1002/sec.1222
15. Sen J (2013) Security and privacy challenges in cognitive wireless sensor networks. Cogn Radio Technol Appl Wirel Mob Ad Hoc Netw. https://doi.org/10.4018/978-1-4666-4221-8.ch011
16. Sengupta S, Anand S, Chandramouli R (2010) Pricing for security and QoS in cognitive radio networks. Cogn Radio Netw Wirel Netw Mob Commun Arch Protoc Stand. https://doi.org/10.1201/ebk1420077759-c11
17. Strassner J (2012) The role of autonomic networking in cognitive networks. Cogn Netw. https://doi.org/10.1002/9780470515143.ch2
18. Tang H, Yu FR, Huang M, Li Z (2012) Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks. IET Commun 6(8):974–983
19. Wei W (2011) The research of cognitive communication networks. In: 2011 IEEE 3rd international conference on communication software and networks. IEEE, China. https://doi.org/10.1109/iccsn.2011.6013533
20. Yan Q, Li M, Chen F, Jiang T, Lou W, Hou YT, Lu CT (2013) Non-parametric passive traffic monitoring in cognitive radio networks. In: INFOCOM, 2013 proceedings IEEE. IEEE, Italy, pp 1240–1248
21. Zhang Y, Zheng J, Chen HH (eds) (2016) Cognitive radio networks: architectures, protocols, and standards. CRC Press, Boca Raton