RESEARCH REVIEW JOURNALS
Volume-03
Issue-10
October -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

A Study on Analysis of Attacks and Combating Security Issues in Cognitive Radio Networks

[1]Katta Swamy Mergu and [2]Dr. Habibulla Khan

[1]Research Scholar under the faculty of ECE at SSSUTMS, Sehore-MP
[2]Professor and Dean Faculty of ECE at K.L Deemed to be University, Andhra Pradesh

ARTICLE DETAILS

Article History
Published Online: 10 October 2018

Keywords
cognitive, radio, security, attack, network

ABSTRACT

Cognitive radio (CR) is introduced as a solution to improve spectrum utilization by enabling secondary access to licensed spectrum. Discovering spectrum holes is therefore essential. To explore the spectrum opportunities, there are two approaches: spectrum sensing and database-driven. While most examination work in the field of security is based on latent attack detection procedures for example attack detection on signal detection, the goal of this exploration work is to build up a functioning attack detection based security framework for cognitive radio networks. This examination is extension of SMTD (Security Management based on Trust Determination) protocol proposed. In their seminal work, creators have proposed a functioning attack detection component based on trust determination in grouped cognitive radio network.

1. Introduction

Cognitive radio (CR) is introduced as a solution to improve spectrum utilization by enabling secondary access to licensed spectrum. Discovering spectrum holes is therefore essential. To explore the spectrum opportunities, there are two approaches: spectrum sensing and database-driven. In the spectrum sensing approach, the primary users' activity is explored by measuring the spectrum environment, while in the database-driven approach, the information of spectrum usage for CR users is provided by a database server. Compared to the database-driven approach, the spectrum sensing approach is cheaper and more flexible for a wide range of networks. In the past decade, the field of cognitive radio (CR) has grown and matured to the point where it can be considered a feasible demonstrable technology. As such, issues of robustness and security have become more prominent. At this juncture, it is important to assess the challenges faced by cognitive radio networks (CRN) and the current status of solutions to general and CRN-specific security threats. Tremendous demand of wireless network services has increased troubles in its security angle. Albeit due to the idea of CRN and its basic applications, it is defenseless against the vast majority of the security threats. Regardless of such an incredible advantage, ensuring security is a significant test for these networks. According to perceptions, it is seen that CRN has a class of scarcely any weaknesses which can't be effortlessly amended. To determine these kinds of threats CR ought to figure out how to know to the climate. Significant threats on CRN can be ordered based on layers they attack, since cognitive radios are extraordinary instance of adhoc networks, consequently security threats on adhoc networks are additionally appropriate on CRNs.

2. Literature Review

Chen ET. al. (2008) discuss the possibility of cognitive radio system by J. Mitola from programming characterizes radio (SDR) which is initially considered to enhance the spectrum utilization. CR is a smart correspondence framework which knows about the earth. CR finishes two noteworthy destinations which are to a great degree reliable correspondence when and wherever required and successful activity of the radio spectrum. Paper discusses significant three sort of system engineering in CR. 1-Foundation, 2-Include hoc and 3-Work models. The writer utilize pictorial outline which encourages the peruse to effortlessly comprehend the themes the paper portrays. Paper utilized tremendous referencing in his paper. This paper can't finish the entire design of cognitive radio system. More business related to CRN is pending.

Yuan ET al. (2008) said that system layer can use to incorporate Macintosh's and PHY layer for better administration. Also, it discusses the numerical structure for steering trust in CRN. System layer structure can give better administration in Macintosh and PHYs and it coordinate transport and application layer. Paper discusses the area administration handoff administration, security assaults and bad conduct and security administrations. Papers discuss the security benefit which is given in CRN. For every one of those administrations of security convey the security empower condition as contrast with vindictive dangers and troublesomeness. In this paper creator utilized best and refreshed referencing. Paper utilized numerical relational word in trust CRN. Creator can't recreate to his scientific recommendations. The security dangers in CR/CRN the assaults are computerized reasoning conduct dangers and dynamic spectrum gets to dangers. Creator Utilize the best referencing in his short paper. Paper is ordered and mastermind in the proper way. Creator can't propose any model to demonstrate his perspective. The countermeasure of the assaults can't disk.

Ruiliang ET. al. (2010) defends Incumbent emulation assault and SSDF assault. Two system are utilized one is DRT which is remove Proportion Test while the second is DDT which is Separation Diverse Test to dispense with the IE assaults. Creator utilizes two levels in the main all local spectrums' deducting result ought to be approved by the information beneficiary. While second layer of assurance is position of information union plans which are emphatically against assault of SSDF. The creators utilize recreation result to demonstrate his outcome and to demonstrate his

reenactment the creators utilize graphs. No numerical recipe is utilized to demonstrate his recreation.

Shaukat ET. al. (2008) investigated that to kill the DOS assault stream control can be acquainted at Macintosh layer with approve the veritable hubs of the system amid the channel trade off stage. In this stage no significant specialist or solid untouchable gathering is included. The paper proposed an outcome to recognize noxious hub. Refreshed referencing is utilized as a part of this paper. No Check with its examination is discussed in this paper. No reproduction work is done .The creator perspective is extremely uncommon. It portray the security risk and it exhibit two arrangements which is Key administration Foundation and Conveyed key Administration. Graphical Reproduction and pictorial chart utilized. Creator can't finish the contentions of Conceivable DoS Dangers in Cognitive Radio System and their Countermeasure.

Zhang ET. al. (2009) discuss two methodologies which is assurance based layer considering distinctive convention layers and second is identification based layer considering diverse convention layers. Paper discusses security and location on various layers on more detail. Pictorial chart can be utilized. No primary security dangers are discussed in this paper Countermeasures are not full filling the entire security parameters. The dangers to CR and dynamic spectrum get to dangers and proposed Three Moderation procedure strong Tactile, Relief in Singular Radios and Alleviation in System. The paper gives well foundation learning about the CR engineering and pictorial portrayal to elucidate the security issues. Security dangers and arrangements are very much characterized, separately. We didn't found any critical shortcoming in the paper aside from the demonstrated hypothesis might be more approved by recreation in NS-2 or MATLAB. Cures against the disappointments they are arranged steady CR, CCC assaults, inhabitance disappointments by spectrum, strategy, area, and sensor and by transmitter and in addition beneficiary. Paper discusses the primary security dangers and also their countermeasure. Distinctive security can be taken after against the assault. Creator can't demonstrate his countermeasure with any model through recreation. No pictorial chart is utilized as a part of this paper.

3. Proposed Framework for Secure Cognitive Radio Networks

Past part examines about conceivable security threats at each layer of cognitive radio network. Moreover a systematic model for detecting primary user emulation attack has been given. Unmistakably cognitive radios are vulnerable to different security threats that decrease its value. A few analysts have proposed different procedures to relieve these attacks for every class of cognitive radio network. To build up a secure CRN design, these methods ought to be incorporated in same network. Security framework for cognitive radios can be sorted as cryptographic procedures, notoriety based strategies and trust assessment based methods.

To give confirmation, secrecy and unwavering quality, a CRN security design dependent on cryptography. Creator introduced an access control component dependent on 802.1 xs alongside a key distribution place (KDC), changed DHCP workers and terminal identification strategy that will cooperate to offer asset allocation and message confirmation in DHCP exchanges.

Notoriety based design to recognize misbehaving cognitive users in cooperative spectrum sensing algorithm has been introduced. The algorithm begins by selecting some cognitive users as dependable and then classifies the notoriety on every user into three states to be specific disposed of, pending and solid. The algorithm allocates pending state to each cognitive user other than confided in once then their notoriety is aggregated by uniformity test among worldwide and neighborhood sensing results. Cognitive users with notoriety esteem more noteworthy than believed edge are refreshed to solid classification while others will be added to dispose of class.

The creators have introduced trust based cognitive radio network design (TCRN) to help network functions, for example, dynamic spectrum access (DSA) and routing. According to creators there ought to be two significant segments involved in CRN trust model; confided in affiliation and learning algorithms. Believed affiliation involves the initial decision of a cognitive user to either acknowledge or dismiss its neighbor's affiliation demand. Learning algorithm assists with making improved decisions regarding parcel forwarding, routing and trust measures.

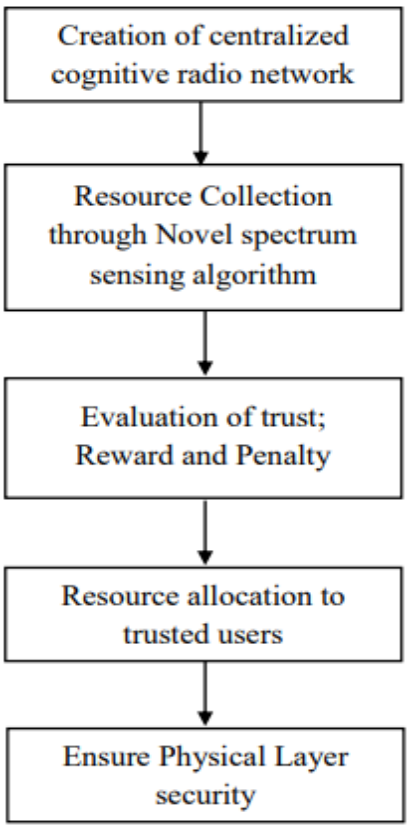

Figure 1: Flow diagram of proposed research work

Figure 1gives stream diagram of proposed research work. The components of this stream graph are portrayed in different sections of this proposition independently. While most examination work in the field of security is based on latent attack detection procedures for example attack detection on signal detection, the goal of this exploration work is to build up a functioning attack detection based security framework for cognitive radio networks. In such manner, this examination is extension of SMTD (Security Management based on Trust

Determination) protocol proposed. In their seminal work, creators have proposed a functioning attack detection component based on trust determination in grouped cognitive radio network. A tale prize and punishment conspire is proposed based on trust determination however they don't consider data transmission security. Mystery limit improvement plot has been applied with hybrid cooperative spectrum sensing algorithm to SMTD way to deal with upgrade physical layer security in cognitive radio networks. Network model and system stream are given as follows:

4. Analytical Model

A Lion attack can corrupt the throughput of a TCP connection, leading in certain situations to the starvation of the TCP source. In this section, we determine a logical expression both for the normal inactivity time of a TCP source and the reduction of the throughput due to the attack. It is important to comment that introduced model is only an approximation that is, neglecting numerous marginal contributions. Its exactness is in any case demonstrated by comparing the outcomes with recreated ones.

Numerical Background:

Let Sk as in expression (1) be the whole of k ∈ N independent and identically distributed (i.i.d.) random factors Xi, i ∈ [1, k] ⊆ N, with likelihood thickness function (pdf) as in (2) and combined distributed function (cdf) as in (3)

$$S_k = X_1 + X_2 + \cdots + X_k = \sum_{i=1}^{k} X_i, \quad (1)$$

$$f_{S_k}(t) = \left(f_{X_1} * f_{X_2} * \cdots * f_{X_k}\right)(t), \quad (2)$$

$$F_{S_k}(t) = \int f_{S_k}(t)dt. \quad (3)$$

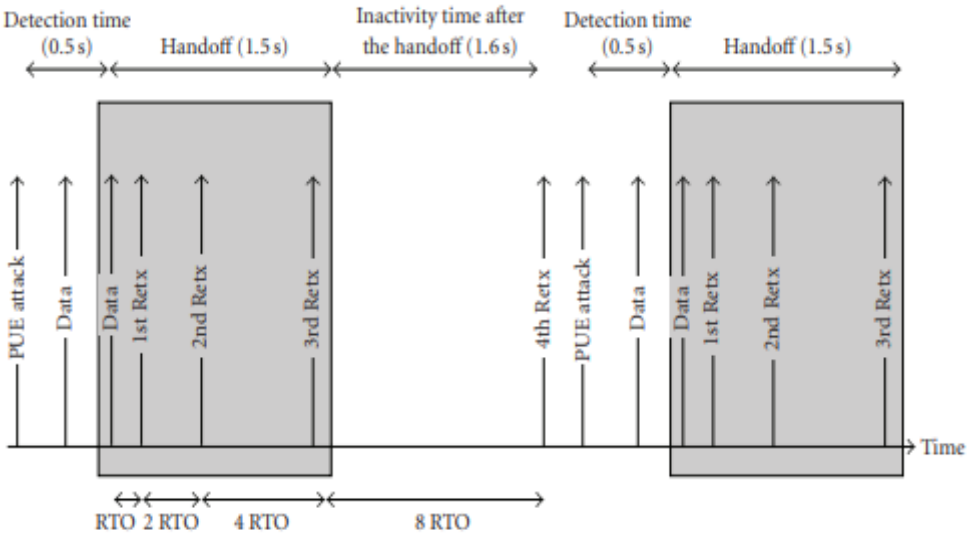

Figure 2: Lion attack

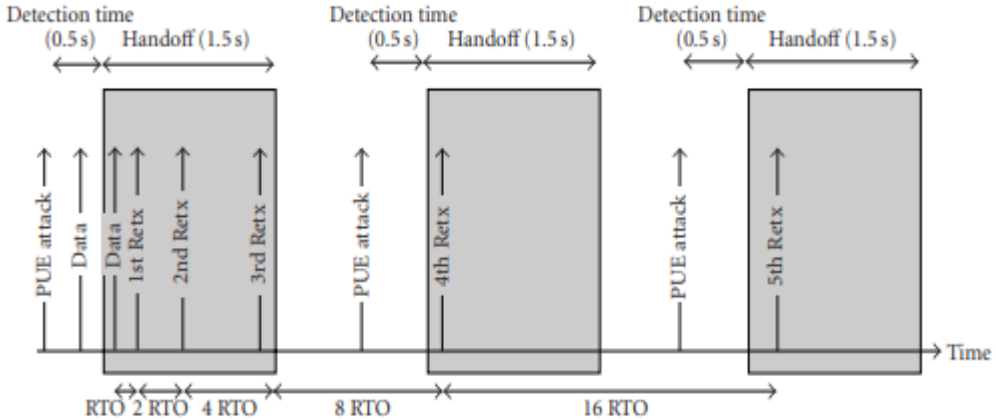

Figure 3: Smart Lion attack

***Lemma 1*:** Given Sk as in (1), the probability of only and no more than k N events occurring within the interval [t, t +τ], t ≥ 0, τ > 0 R is

$$\Pr(k \text{ events in } (t, t+\tau]) = F_{S_k}(\tau) - F_{S_{k+1}}(\tau). \quad (4)$$

***Proof*:** Let us signify by A = {Sk+1 : Sk+1 ≥ τ}, B = {Sk : Sk ≤ τ} and C = {Sk : Sk > τ}. The likelihood of only and close to k N occasions occurring within the interval (t, t + τ] can be communicated as the likelihood of A ∩ B. As A = (A ∩ B) ∪ (A ∩ C), being.

$$\Pr(A) = \Pr(S_{k+1} \geq \tau) = 1 - F_{S_{k+1}}(\tau),$$
$$\Pr(A \cap C) = \Pr(C) = \Pr(S_k > \tau) = 1 - F_{S_k}(\tau), \quad (5)$$

Then

$$\Pr(A \cap B) = \Pr(A) - \Pr(A \cap C) = F_{S_k}(\tau) - F_{S_{k+1}}(\tau). \quad (6)$$

Assumptions

i. In order to build up the model, the following assumptions have been received.
ii. A malicious user performs a few attacks, every one leading to a frequency handoff.
iii. The duration of a handoff, which we mean by tH is fixed.
iv. The time required in order to begin a handoff after the CRN identifies the presence of a primary user (channel detection time) is fixed with value tD.

The time since the finish of a frequency handoff until the attacker performs the following attack is modeled by a random variable. Accordingly, we define Xi as a lot of i.i.d. random factors (see Figure 3) and X I = Xi + tD + tH as i.i.d. random factors that speak to the time since the finish of a handoff until the finish of the following one. Therefore, we can define S k as a random variable being the aggregate of k NX'i as in (7) with pdf and cdf as in (8), being Sk the total of k NXi as in (3.47)

$$S'_k = \sum_{i=1}^{k} X'_i, \quad (7)$$

$$\begin{aligned} f_{S'_k} &= f_{X'_1} * f_{X'_2} * \cdots * f_{X'_k} \\ &= f_{X_1} * f_{X_2} * \cdots * f_{X_k} * \delta(t - k(t_D + t_H)) \\ &= f_{S_k}(t - k(t_D + t_H)), \\ F_{S'_k}(t) &= F_{S_k}(t - k \cdot (t_H + t_D)). \end{aligned} \quad (8)$$

The round trip time is consistently more modest than the minimum RTO of the TCP source RTOmin. As explained this can be expected in CRNs, for example, 802.22 networks. With each ineffective endeavor the RTO value is multiplied until a greatest value RTOmax that it is the RTO by a power of 2. Thus, the value of RTO for the i^{th} retransmission can be communicated as and set of conceivable retransmission instants t_i defined as in

$$\mathrm{RTO}_i = \begin{cases} 2^{i-1} \cdot \mathrm{RTO}_{\min} & \text{if } i \leq i_{\max}, \\ \mathrm{RTO}_{\max} & \text{if } i > i_{\max}, \end{cases}$$
$$i_{\max} = \log_2 \mathrm{RTO}_{\max} + 1,$$
$$\mathrm{RTO}_{\max} = 2^{i_{\max}-1} \cdot \mathrm{RTO}_{\min}, \quad (9)$$

$$t_i = \begin{cases} \mathrm{RTO}_{\min} & \text{if } i = 1, \\ t_{i-1} + \mathrm{RTO}_i & \text{if } i > 1 \end{cases}$$
$$= \begin{cases} (2^i - 1) \cdot \mathrm{RTO}_{\min} & \text{if } i \leq i_{\max}, \\ (i - i_{\max} + 2) \cdot \mathrm{RTO}_{\max} - \mathrm{RTO}_{\min} & \text{if } i > i_{\max}. \end{cases} \quad (10)$$

As appeared in Figure 3.6, we expect that it generally takes place at any rate one (handoff 0). Considering that the principal fragment loss takes place toward the beginning of the handoff 0, the retransmissions endeavors at ti < tH will fall within this handoff and therefore will consistently fizzle, implying Pr(t = ti) = 0. For the sake of clearness, we define a new time hub t' = t−tH, and in this manner we redefine the retransmission instants as tI' = ti −tH being t1' = ts − tH with s the index of the main ti satisfying the condition ti > tH. Accordingly i is defined as i − s + 1 for i ≥ s.

Probability of k Handoffs in Interval (t, t + τ]

The probability pk(τ) that k handoffs happen in the interval (t', t'+ τ] is the probability of k occasions of the random variable X I in interval (t' t'+ τ] (see Figure 3). Therefore, from Lemma 1, pk(τ) can be communicated as in

$$p_k(\tau) = \begin{cases} 1 - F_{S'_1}(\tau + t_H) & \text{if } k = 0, \\ F_{S'_k}(\tau + t_H) - F_{S'_{k+1}}(\tau + t_H) & \text{if } k > 0. \end{cases} \quad (11)$$

5. Conclusion

A Lion attack can corrupt the throughput of a TCP connection, leading in certain situations to the starvation of the TCP source. This part examines about security threats identified with cognitive radio networks. Security threats identified with each layer of CRN are examined. Furthermore, a systematic model for detection of PUE attack has been introduced. Security mechanism identified with cognitive radio networks has been examined and proposed security framework for cognitive radio network has been introduced.

References

1. K.-C Chen, Y.-J Peng, N. Parasad, Y.-C Liang, S. Sun “Cognitive Radio Network Architecture: Part I – General Structure” ACM 2008
2. Mustafa Harun YJlmaz, ErtuLrul Güvenkaya,HajiM. Furqan,Selçuk Köse,and Hüseyin Arslan.”Cognitive Security of Wireless Communication Systems in the Physical Layer”. Wireless Communications and Mobile Computing. Volume 2017.
3. Ruiliang Chen Jung-Min Park Hou, Y.T. Reed (2010), “Toward secure distributed spectrum sensing in cognitive radio networks” Communications Magazine, IEEE Publication.
4. Shaukat, R. Khan, S.A. Ahmed, A. “Augmented Security in IEEE 802.22 MAC layer Protocol” Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th IEEE International Conference.

5. Xueying Zhang, Cheng Li “The security in cognitive radio networks: a survey”ACM 2009 International Conference on Communications and Mobile Computing.
6. E. Wassim, S. Haidar and G. Mohsen, “Survey of Security Issues in Cognitive Radio Networks”, Journal of Internet Technology, 2011, vol. 12 No. 2, pp. 181-198.
7. S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, “Cognitive radio network security: A survey”, Journal of Network and Computer Applications, 2012, vol. 35, pp. 1691–1708.
8. T. R. Newman and T. C. Clancy, “Security threats to cognitive radio signal classifiers”, Proceedings of the Virginia tech wireless personal communications symposium, 2009, pp. 1-9
9. Kresimir Dabcevic, Alejandro Betancourt, Lucio Marcenaro and Carlo S Regazzoni.”Intelligent cognitive radio jamming - agame-theoretical approach”.Dabcevic et al. EURASIP Journal on Advances in Signal Processing 2014, pp.1-18.
10. D. Cabric, S. M. Mishra and R. W. Brodersen, “Implementation Issues in Spectrum Sensing for Cognitive Radios”, 38th Asilomar Conference on Signals, Systems and Computers, 2004, pp. 772-776.

