AI based Algorithm & Framework for Efficient PUE Attack Detection using Dual Classification Method in CRN

Sundar Srinivasan
Research Scholar, Department of E&C Engineering,
Mewar University, Chittorgarh, Rajasthan, India

Dr K.B Shivakumar
Professor and HOD, Department of Telecommunication Engineering,
Sri Siddhartha Institute of Technology, Tumkur, Karnataka,

Abstract
Cognitive radio networks are software controlled radios with the ability to allocate and reallocated spectrum depending upon the demand [18]. An extremely optimal use of the spectrum brings selfish attack being most with the challenges of misuse and attacks. Unlicensed Secondary user spectrum pretends to be a primary user by altering characteristics of signal behavior. Robust previous studies have suggested method to overcome many attacks [9,17]. Artificial intelligence detection is most important requirement to detect dynamically [10, 22]. A supervised learning model learns from the past attack patterns and post detecting prevents future attacks by classifying the current transmission spectrum sensing, signaling behaviors [11].Classifier training is one of the important challenging factor training area with supporting information. Such classifiers are extremely difficult to train as signature keeps on changing frequently, due to complex nature of the CR network; attack signature also varies based on the network state [12, 16, 19]. Most of the past works are edge based attack detection; availability state constraint at the edges makes it difficult to run sophisticated attack detection engines at the real time. Cloud advancements now days become possible to connect the edge computing engine to a powerful core cloud which can help to adapt & decide to take quicker decision due to simplification scaling & powerful VM based compute engine[13,14,15]. This paper explorer fullest of technology advancement offering powerful real time Primary user emulation attack detection at the cloud by collaborating the edge computing engines with core compute engine.

Keywords: Cognitive Radio, Primary User attack, Artificial Intelligence, Un Supervised Learning, Cloud Computing.

Introduction
Cognitive Radio offers software controlled spectrum reallocation which enables unutilized spectrum to be distributed amongst non-licensed secondary user and reallocate it back to the primary licensed user when demand surges. Even though the spectrum reallocation is an immensely powerful mechanism to ensure better spectrum utilization, it also leads to primary user emulation (PUE) attack. A PUE attack is one where a secondary user with partial information of the modulation and the underneath spectrum scheme pretends to be a primary user & injects its signal into the primary spectrum. A base station can easily detect an emulated attack. On other hand, intermediate signal spreading enhances the used bandwidth.

[3] Cognitive radio is an intelligent radio that can be programmed and configured dynamically to fully use the frequency resources that are not used by licensed users. It defines the radio devices that are capable of learning and adapting to their transmission to the external radio environment, which means it has some kind of intelligence for monitoring the radio environment, learning the environment and make smart decisions.

[4] Cognitive wireless network are trained via artificial intelligence (AI) and machine learning (ML) algorithms for dynamic processing of spectrum handovers, focuses on learning and reasoning features of cognitive radio (CR) by analyzing primary user (PU) and secondary user (SU) data communication using home location register (HLR) and visitor location register (VLR) database respectively.

[5] To present the proposed AES-assisted system for robust and reliable primary and secondary system operations. In the proposed system, the primary user generates a pseudo-random AES-encrypted reference signal that is used as the segment sync bits. The sync bits in the field sync segments remain unchanged for the channel estimation purposes. At the receiving end, the reference signal is regenerated for the detection of the primary user and malicious user. It should be emphasized that synchronization is still guaranteed in the proposed scheme since the reference bits are also used for synchronization purposes.

[6] The security problems arising from Primary User Emulation (PUE) attacks in CR networks. We present a comprehensive introduction to PUE attacks, from the attacking rationale and its impact on CR networks, to detection and defense approaches.

[7, 21] To solve the spectrum scarcity problem by allocating the spectrum dynamically to unlicensed users. It uses the free spectrum bands which are not being used by the licensed users without causing interference to the incumbent transmission. So spectrum sensing is the essential mechanism on which the entire communication depends.[22] If the spectrum sensing result is violated, the entire networks activities will be disrupted. Primary User Emulation Attack (PUEA) is one of
the major threats in the spectrum sensing, which decreases the spectrum access probability. The objectives are to give the various security issues in cognitive radio networks and then to discuss the PUEA with the existing technique. [8] The crucial features of CRNs are awareness, reliability and adaptability for better communication and preventing the network from threats and malicious intent is equally important and a challenging task. The physical layer is significant in terms of detection of this malicious node. PUEA is one of the security issues in the physical layer of the protocol stack. The defensive system has been proposed.

Methods

The Architectural System of Cognitive Radio Network can be represented in Figure 1 below

![Cognitive Radio overall system](image)

Figure 1: Cognitive Radio overall system

From figure 1, it can be seen that CR network is essentially several software controlled local networks with the ability of spectrum management. These networks are connected to cloud due to information and data management and billing Network state defined as set of unique parameters used to determine attack from unattack scenario.

a) Channel Assignment Matrix\[x\] defined as

\[ A_{n,m} = \begin{cases} 
1, & \text{if SC } n \text{ is assigned to channel } m \\
0, & \text{otherwise} 
\end{cases} \]

Mathematically Interference as below to minimize the overall cost of the Radio Network.

\[ f(x) = \sum_{n=1}^{S} \sum_{m=1}^{C} A_{n,m} \sum_{k=1}^{S} \sum_{j=1}^{C} P_{n,k,d+1} A_{k,j} \]

Where

\[ \sum_{n=1}^{C} A_{n,m} = B_n, \quad \forall n = 1,...,S \]

\[ A_{n,m} \in \{0,1\} \quad \forall n = 1,...,S, \quad \text{and} \quad m = 1,...,C \]

The cost function generated as

\[ P_{n,k,d+1} = \max(0, P_{n,k,d} - 1) \]

\[ P_{n,k,1} = 1_{n,k,m}, \quad \forall n, n \neq k, \quad \text{and} \quad m = 1,...,C \]

\[ P_{n,1,j} = 0, \quad \forall n. \]

The above matrix is used by the spectrum controller (CR Base stations B1 and B2 in proposed method). In non-attacked state, above variables will be homogeneous across the entire controller C (B1, B2 in proposed method).

b) Link bandwidth estimation\[y\] mathematically defined below

\[ \alpha_{i,j,k} = \frac{\sum_{m=0}^{k} B_{i,j,m}}{\prod_{n=0}^{k}(t_m - t_n)} \]

at time \(t_k\), where \(B_{i,j,m}\) is the bandwidth between node \(i\) and node \(j\) at time \(m\).

c) Cyclic Cummulants\[z\] : Assuming signal sequence is \(x(t)\) for time lags \(\tau_1,\ldots,\tau_{k-1}\), signal sequence \(c_{ks}(t;\tau_1,\ldots,\tau_{k-1})\) is expanded into a Fourier series based on variable \(t\):

\[ c_{ks}(t;\tau_1,\ldots,\tau_{k-1}) = \sum_{\alpha \in A_k} C_{ks}^\alpha (t;\tau_1,\ldots,\tau_{k-1}) e^{-j\alpha t} \]

\[ C_{ks}^\alpha (\tau_1,\ldots,\tau_{k-1}) = \lim_{T \to \infty} \frac{1}{T} \sum_{t=0}^{T-1} c_{ks}(t;\tau_1,\ldots,\tau_{k-1}) e^{-j\alpha t} \]

Where cyclic frequency \(K\) th is cyclic Cummulants

d) Energy : Energy sensing model [13] using dynamic spectrum sensing is calculated as below
\[ A_k = \begin{cases} 1, & \text{if } S_{m,k} = 1 \text{ for some } m \\ -1, & \text{if } S_{m,k} = 1 \text{ for all } m \end{cases} \]

\[ Z_{n,k}(i) = \sum_{m=1}^{M} S_{m,k} h_{m,n,k} X_{m,k}(i) + N_{n,k}(i) \]

\[ Y_{n,k} = \frac{2}{\eta_k} \sum_{i=1}^{\alpha} \left| Z_{n,k}(i) \right|^2 \]

\[ Y_k = (Y_{1,k}, ..., Y_{N,k})^T \]

Successful Transmission of Average Secondary Users updated as below

\[ \overline{N}_2 = \left[ k \sum_{j=1}^{2} P_{j,ccc} \right] \]

\[ P_{z,ccc} = \sum_{r=1}^{N_z} \left( \frac{r}{1} \right) P_{p} P_{s} (1-P_{s})^{(r-1)} \left( \frac{1}{k} \right)^r \left( \frac{1-1}{k} \right)^{(N_z-r)} \]

\[ P_{e,ccc} = \sum_{r=1}^{N_e} \left( \frac{r}{1} \right) P_{p} P_{s} (1-P_{s})^{(r-1)} \left( \frac{1}{k} \right)^r \left( \frac{1-1}{k} \right)^{(N_e-r)} \]

The Network State \( N_s \) can be calculated by set of statistical parameters \( N_{sB} \) s network station, \( k \) states of \( N_{sB} = \{ \text{STAT(A), STAT(B), STAT(C4), STAT(P)} \} \) where STAT represents a set of functions \{Min, Max, Average, Standard Deviation, Variance\} \& \( N_{sB} \) represents the network state of a base station B.

**Proposed Framework**

The intelligence adapting process in this proposed framework is distributed in nature comprises of 3 categories of important functional units:

[A] Edge unsupervised bifurcation method

In cognitive networks channel associated with communication channel changes dynamically & unpredictably. Attach Scenario data set is very challenging because communication entities & metrics changes very frequently and hence we propose a novel model Self Organizing map (SOM) based on Edge classifier network model very essential clustered method helps to organize sets of data & map to one set model. Once Information data set is observable and collected at edges of any nodes, data is trained with SOM with \( n \) parameters inputs. Weighted parameters has lattice cell alignment mapping considered to be an independent supervised learning model which we propose in this paper for Cloud based Core.

[B] Core Supervised Learning system method

![Figure 2: Model Core Optimization Methods](image)

Model Core has 4 learning core steps starting with Model Identification phase with unsupervised learning method clustered with 2 model clustering on edge nodes. Iteration started from one node to other node, class to class grouping parameters which are closing located. At beginning there are no PUE attacks hence model training plays a deep learning with validated models building process. Steady state determines that deep learning model is been triggered as explained in Section C

[C] Core Classification of Ns

In Second Phase Deep learning phase of training controlled PUE attacks generated randomly at different edges & core retained model establish primary classes with normal or Abnormal. Hence considered as superset of abnormal categories with a specific type of PUE attack.

In Third phase edges are constructed and model core validated with regular periodic PUE attack and expected to classify right abnormal data from other nodes. Model is repeated is retaining and not 100% classified.

The Classifier validated through suitable test cases and achieved efficiency presented in next section of outcome.

**Conclusion**

A training model is established with 50 Cells & 50 PUA CR Network. By varying number of attackers, error rate, false acceptance and false rejection is calculated. Beside the proposed Deep Learning convolution Neural Network, a rule based classifier based on FFT aggregated end signal at the core and FF neural network at the edge that leverages the same network state as the proposed states. Proposed method results are plotted in Figure 3 & 4
Figure 3: Attacker Accuracy v/s Detection accuracy

Above Figure 3 shows combined framework machine learning performs better than Rule based as technique proposed using supervised and un-supervised model with low error rate.

Figure 4: False Alarm Performance

Above Figure 4 and alarm increase with no of attackers increase as it’s complicated to identify attacker & actual user. Major advantage of proposed framework is more efficient when attacker’s frequency spectrum changes rapidly.

Current work focused on PUE attack detection & prevention in comparison with different techniques rule based & neural network based techniques.

References


Information, and Communications (ICEIC), International Conference on. IEEE, 2016.


About Authors


Dr. K.B. Shiva Kumar received the BE degree in Electronics & Communication Engineering during 1983, ME degree in Electronics during1989, MBA degree during 1998 from Bangalore University, Bangalore and M Phil Degree during 2009 from Dravidian University Kuppam. He obtained Ph.D. during 2012 in Information and Communication Technology from Fakir Mohan University, Balasore, Orissa. He has got 33 years of teaching experience and has over 60 research publications in National and International Conferences and Journals. Currently he is working as Professor, Dept. of TC Engineering, Sri Siddhartha Institute of Technology, Tumkur, Karnataka. His research interests include Signal processing, Image processing, Steganography and Multirate Systems and Filter Banks.