Indian Journal of Science and Technology, *Vol 9(29), DOI: 10.17485/ijst/2016/v9i29/89270, August 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

SVM based Two Level Authentication for Primary user Emulation Attack Detection

S. Arul Selvi* **and M. Sundararajan**

Electronics and Communication Engineering, Bharath University, Chennai – 600 073, Tamil Nadu, India;
arulselvi2003@gmail.com, msrajan69@gmail.com

Abstract

Background/Objectives: Cognitive radio network is the evolutionary network to solve the spectrum scarcity problem. Primary User Emulation Attack is a major security issue that cause to fail the dynamic spectrum access of the cognitive radio network. **Methods/Statistical Analysis:** This paper proposes two level verification of the primary user signal to enhance the security of the spectrum sensing under PUEA attack. Support Vector Machine is used in the two level verification for detector classify the received data in to a location boundary and higher order statics at second level. **Findings:** At first level using the location information of the primary user, the primary user signal is verified for its validity. The SVM is first trained to learn the Primary user Location and with the help of known location of the Primary user it can be verified. Then the trained SVM is used to find the location boundary of the user that transmitted the signal. If the signal boundary is within the primary used location boundary it is concluded that the signal is from the primary user; else it is from the PUEA attacker .After verifying in the first level on the second level higher order statics values are calculated then using that as the feature vector the SVM classifier is used to classify the received signal as two class: one from original primary user and other from the PUEA attacker. This two level verification of the primary user signal will be more accurate method of PUEA attack detection comparing to the single level schemes. **Applications/Improvements:**This two level verification scheme improves the accuracy from 82% at Linear SVM kernel to 100% and also from 77% at RBF SVM kernel to 100%.

Keywords: Cognitive Radio Network, Dynamic Spectrum Access, Primary user Emulation Attack, Support Vector Machines

1. Introduction

Cognitive radios have enabled the full utilization of the underutilized license spectrum by opportunistically transmitting without interference to licensed users. With development of cognitive radios, there are many new security threats have been raised. As per Security threats concern as cognitive radio networks is a type of wireless network, it has all classic threats as in the wireless networks. Apart from that they have a main threat called Primary User Emulation Attack (PUEA) in the spectrum sensing process. Under PUEA attack, the attacker adversaries signal that mimic primary and gives false observations related to spectrum sensing[1,2]. Spectrum sensing uses Energy detection which is the most widely as a method as it has low computational overhead[3,4]. But this detector does not perform well in low SNR case.

PUEAs can be of two types 1)Greedy PUEA : under which, the attacker generate fake incumbent signals which results other users to vacate the band to its exclusive use.2) Malicious attack :under which the attacker mimic incumbent signals which cause Denial of Service (DoS). Furthermore, malicious attack can make DoS attacks to PU networks by harmful interference.

There are many contributions towards security issues for the detection of PUEAs. There are few spectrum sensing approaches which handle the security issues[5]. Cooperative sensing is one of the solution for it[6,7]. A separate sensor network based PUEA detection mechanism is proposed such that the cognitive users need not involve detection duties[8].

*Author for correspondence

This work utilizes both the location information and the *Received Signal Strength* (RSS) . It consists of three phases: verification of signal, received energy estimation, and localization of the transmitter. In another work[9], the channel impulse response is used as the "link signature" to find the PU location. There is a "helper node" which is close to a primary transmitter to get the helper node's link Signatures to verify the primary signal. A multi-channel sensing is given[10,11] to detect PUEA, under which secondary user randomly selects a channel from multiple channel to sense at each time slot, thereby it probabilistically avoiding the PUEA attack. The cooperative spectrum sensing technique is one of the research area where the spectrum sensing accuracy is increased with some level has much research attention. There are very few PUEA detection in the cooperative spectrum sensing. A new cooperative spectrum sensing scheme is presented in the presence of PUEA in cognitive networks. In this work the local sensing information of different secondary users is combined at a fusion center. The combining weights are selected such that it will maximize the detection probability of channels given the constraint of a false alarm probability [12].

Many machine learning algorithms such as Artificial Neural Network, and genetic algorithm are used for attack detection in literature[13]. But that techniques are not suitable for the huge data set. Long training time and accuracy of classification are the two main issues in that approach when the data size are high. So SVM based approach is used in this work.

SVM is first trained to learn the location boundary of the primary user with the help of the known location information .Then the trained SVM is used to classify the received signal whether the received signal location is within the boundary of the primary location or not. Thereby the primary user signal is authenticated. On the second level we used SVM to classify the signal into primary and PUEA by using higher order static data as feature vector[14,15].

The organization of this article is as follow: section 2 presents the theory behind the proposed method using SVM, section 3 gives the results and section 4 concludes the work with the summary of the work.

2. SVM and SVM based PUEA Detection

Machine learning algorithms are widely used in the cognitive radio application to bring out the learning in the cognitive radio. Support Vector Machines (SVM) is a type of supervised learning methods that can be applied to classification or regression application. The working of the SVM consist of two phase .In phase one called training phase a set of training data with marked classes are given as input and a SVM model generated by the SVM training algorithm. In second phase of classification or perdition is used to classify the new set of data in to the trained class. Basically the SVM acts as a non-probabilistic binary linear classifier to classify the data in to two classes. This SVM model maps training data such that the examples of the separate categories are divided by a clear gap that is as wide as possible.

Basically the primary user emulation attack detection is a classification problem, in which we classify the primary user pattern from the primary user emulation attacker pattern. Support Vector Machine (SVM) is a machine learning algorithm used to solve this type of classification problem.

Here in this work SVM based data classification is used to find the boundary of the primary user and also used to classify the higher order static feature of the attacker and primary user. Here two stage verification is done in order to differentiate the primary user signal and the primary user emulation attacker signal .In the first stage using the SVM the boundary of the primary user is fixed on training phase and this boundary values are used to compare the received signal to find out whether the received signal falls within the boundary or not .If the received signal is within this boundary first stage confirmation of the presence of the primary user is done. In second stage of confirmation the higher order statics are used to classify the signal into primary user and attacker.

Figure 1 shows the system model used to study the proposed system .The system model consists of a Primary

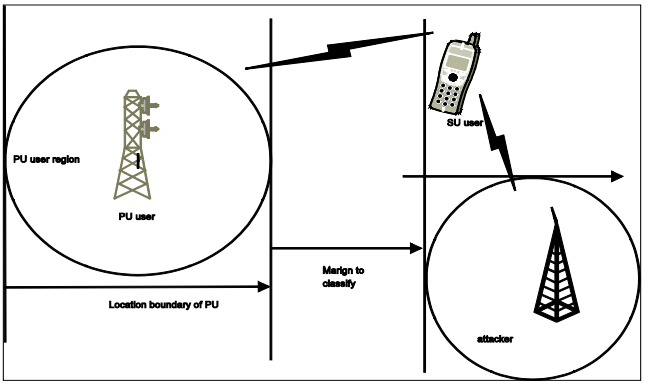

Figure 1. System model for simulation.

user, a secondary user and a PUEA attacker which are located at different places in geographic .It shows the marginal distant boundary between the primary user and PUEA node that will enable us to classify the signal boundary in the first level of authentication of the primary user .The SVM based classification problem for detect the PUEA is stated as below

Suppose we have the training data set where is the feature vector to be classified and is the class vector which has either +1 for class 0 or -1;here in this work the received power is used as the feature vector to classify the two classes i.e. the primary user signal and PUEA attacker signal.

SVM classify the data in to two classes by means of an optimum hyper plane

$$w.x+b=0 \tag{1}$$

The optimal hyper plane to classify the data can be obtained by solving an optimization problem that is given below

$$Min\frac{1}{2}\|w\|^2 \tag{2}$$

$$subjecttoy_i\left(w.x_i+b\right)\geq 1$$

The above the quadratic programming problem can be solved by Introducing Lagrange multipliers, then the optimal decision function can be obtained as follows

$$c(x)=sign\left[\sum_{j=1}^{M}\beta_j y_j\left(x_j,x\right)+b\right] \tag{3}$$

Where is Lagrange multiplier; for nonlinear classification, SVM used a function called kernel function maps the nonlinear training data into a higher-dimensional feature space. If we use such a kernel function then the decision function can be modified as below

$$c(x)=sign\left[\sum_{j=1}^{M}\beta_j y_j G\left(x_j,x\right)+b\right] \tag{4}$$

There are many kernel function available for the SVM classifier .in this work we used linear and radial basis function kernel as our classifier

$$G_{lin}\left(x,y\right)=y^T.x \tag{5}$$

$$G_{rbf}\left(x,y\right)=e^{-\left(\|x-y\|^2/2\sigma^2\right)} \tag{6}$$

2.1 Boundary Detection using SVM

If the received signal power from the PU at secondary user is *Ps*. Consider a predefined power threshold, P_{th}. The boundary of primary is detected by using following algorithms if $Ps < P_{th}$ signal received at secondary will send " + 1" and classified as PUAK signal. Otherwise the signal is from the primary and classified as " –1"

i.e. primary user signal. P_{th} is calculated from the location of the primary by using lognormal channel model. The algorithm of this boundary location based authentication of the primary user is given in Figure2.The algorithm consists of two phases: In phase one the SVM is trained to classify the signal with the help of the location information of the primary user and In phase two the algorithm take the received signal and classify the signal in to two classes 1)primary signal 2) PUEA signal.

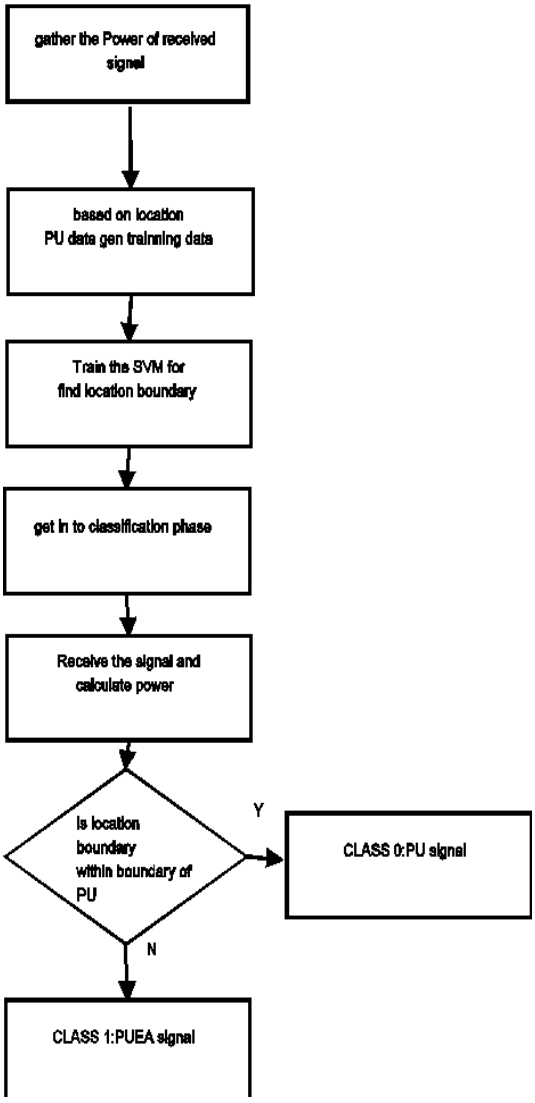

Figure 2. Primary location boundary based SVM classification algorithm.

2.2 Higher order Statics Classification

This second stage verification of primary user signal is developed using the second order and fourth order moments. Figure 3 shows the flow chart of higher order statics based SVM classification

The received signal at the secondary is

$$y_s(n) = h(n) * xp(n) + n(n) \tag{7}$$

Where the xp(n) is the primary transmitted signal ;h(n) is the channel vector between primary and secondary receiver; is modelled as a complex stationary random process due to additive noise.

The second order moments for the above random process is

$$M_{20} = E\left[y^2(n) \right] \tag{8}$$

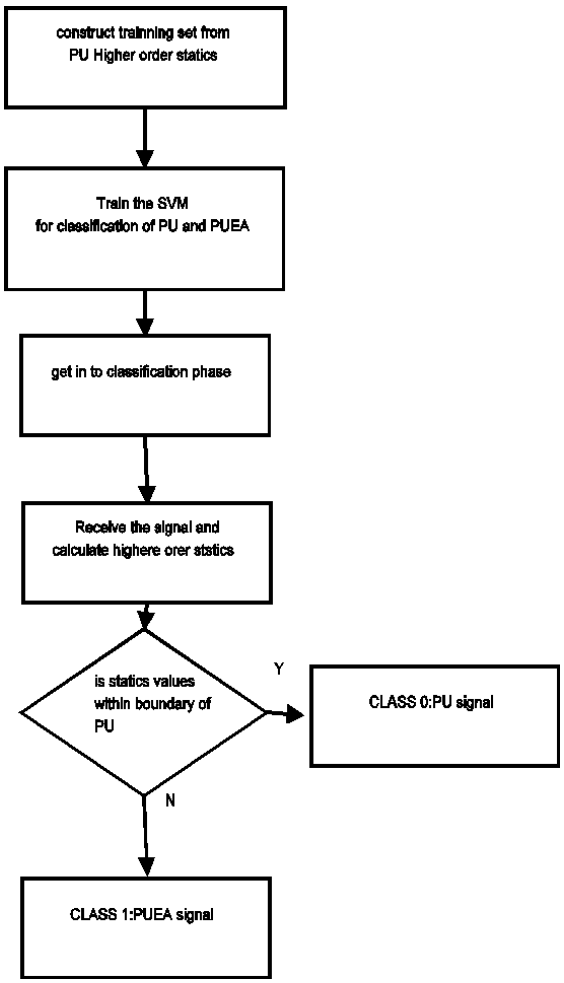

Figure 3. Higher order statics based SVM classification.

$$M_{21} = E\left[\left| y(n) \right|^2 \right] \tag{9}$$

At sample domain the second order moments can be defined as below[13]

$$M_{20} = \frac{1}{N} \Sigma_{n=1}^{N} y^2(n) \tag{10}$$

$$M_{21} = \frac{1}{N} \Sigma_{n=1}^{N} \left| y(n) \right|^2 \tag{11}$$

The fourth order moments and the cumulants at the secondary using the collected sample values is

$$M_{40} = \frac{1}{N} \Sigma_{n=1}^{N} y^4(n) - 3{M_{20}}^2 \tag{12}$$

$$M_{41} = \frac{1}{N} \Sigma_{n=1}^{N} y^3(n) y^*(n) - 3M_{20}M_{21} \tag{13}$$

$$M_{42} = \frac{1}{N} \Sigma_{n=1}^{N} \left| y(n) \right|^4 - \left| M_{20} \right|^2 - 2{M_{21}}^2 \tag{14}$$

The above cumulant values are used as feature vector for the SVM model and used to classify the primary and PUEA signals. The algorithm for this classification is shown in figure. As in the previous section this method consists of training phase where the higher order statics feature are extracted from the primary and PUEA attacker and training vectors are created.

The final decision is made by combining the above two level of classification. If suppose the decision on the first level is the signal from primary userie=-1 and the second level classification also results in primary user signal =-1 then the final decision also =-1;

$$fd(x)_f = \begin{cases} -1, \& c(x)_{lev1} \text{ and} c(x)_{lev2} = -1 \\ +1, else \end{cases} \tag{15}$$

3. Result and Discussion

To study the classification problem we have assumed the following value in the simulation. No of transmission bits used to test the methods N_b =10000; we assumed the distant between the secondary and primary is 10 unit and the between PUEA attacker and secondary is 2 unit .SNR range over which the transmission and reception is done is from 10 to 80 dB.

Figure 4 shows the histogram of the received power of the primary transmitter at the secondary user place and Figure 5 shows the received power of the PUEA attacker on the training phase. From those figure we can conclude that both of them taking different range of power

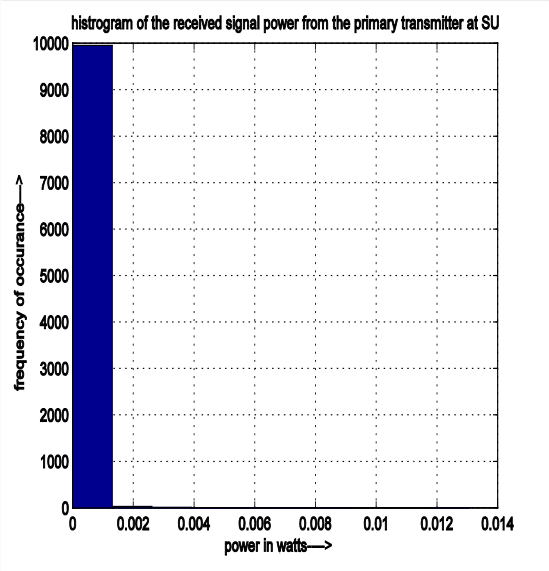

Figure 4. Histrogram of received power of the primary user.

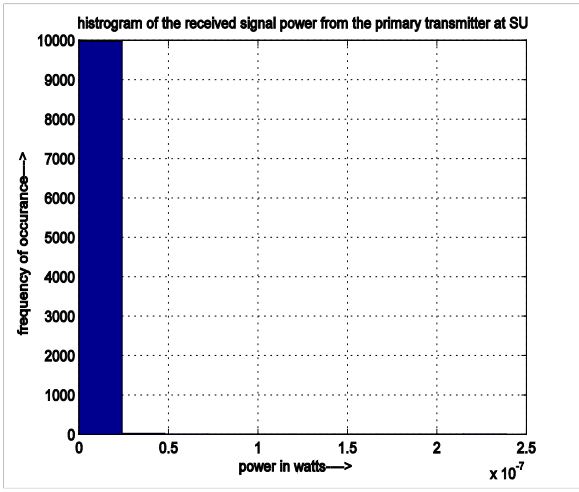

Figure 5. Histrogram of received power of the primary user emulation attacker.

at secondary receiver at different frequency of occurrence this will help us to classify the primary and PUEA attacker signal with some degree of accuracy .On the level one SVM classification the power values of the primary and PUEA attacker is fed as a training vector. Figures 6 and 7 shows the classification diagram with the hyper plane boundary and the associated support vectors for the linear and Radial Basis Function kernel respectively. On the second level of SVM classification the higher order statics values that are computed from the observed signal from the primary user and PUEA.

Table 1. accuracy of correct classification for two different kernel

Kernel	SVM level 1 classification	Level-2-classification	Level-2-classification
Linear	82%	100	100
RBF	77%	100	100

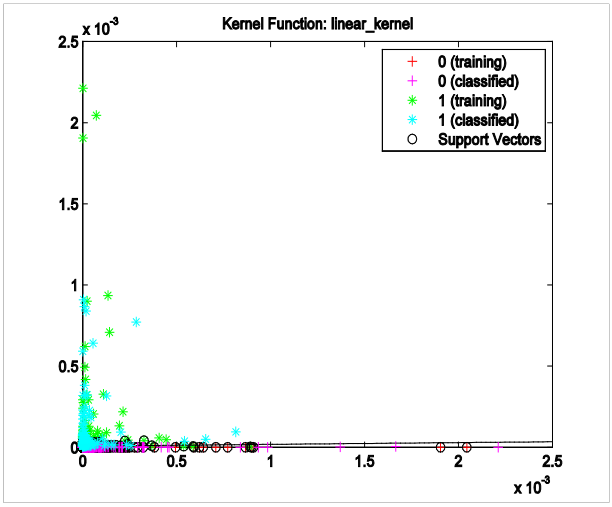

Figure 6. SVM level one classifier with linear kernel.

Attacker is used to train and classification purpose. Here the second order cumulant and fourth order cumulant is used as the feature vector to classify the primary user signal and the PUEA attacker signal. Figures 8 and 9 gives the histogram of the values of the primary user and PUEA attacker signal that is calculated at the secondary user. These figures confirm that both of them taking different band of value that is key enabler to classify these data accurately. Figures 10 and 11 presents the SVM classification with the separating hyper plane and its associated support vector .Those two diagram clearly shows that the two set of the vectors are classifiable with 100% accuracy. Similarly the static M40 is also used as a feature vector in order to classify the primary user and PUEA attacker. Figures 12 and 13 shows the SVM classification diagram using the M40 statistics it is again prove that the two class of data can be classified with 100% accuracy.

As to evaluate the performance of SVM classifier the accuracy of correct classification is calculated in percentage and tabulated in the Table 1. From the table we can observe that one level one of classification on the received signal power to fix the boundary of the transmitter the can only able to achieve 82% accuracy on the linear

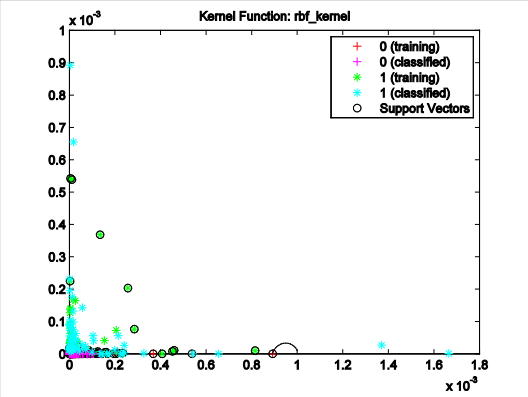

Figure 7. SVM level one classifier with RBF kernel

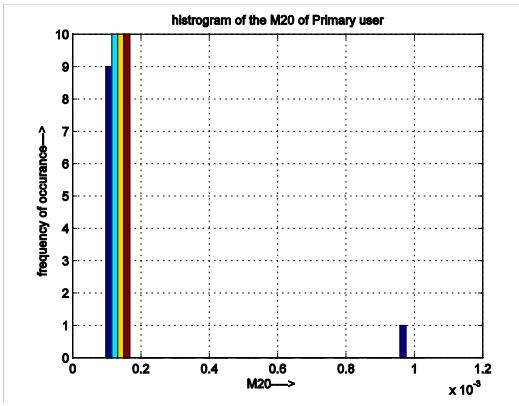

Figure 8. Histrogram of higher order statics M_{20} of the primary user.

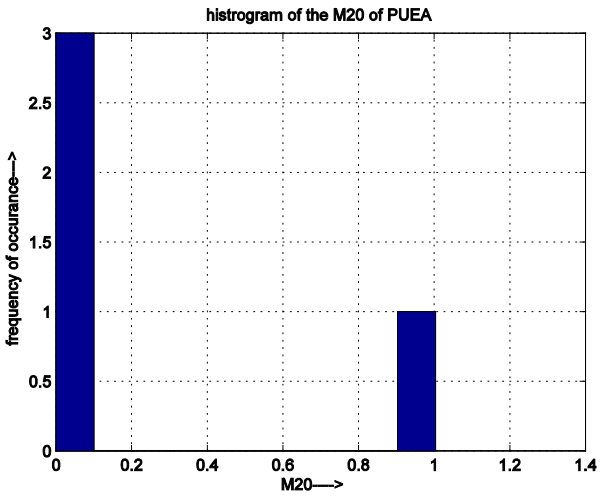

Figure 9. Histogram of higher order statics M_{20} of the primary user emulation attacker.

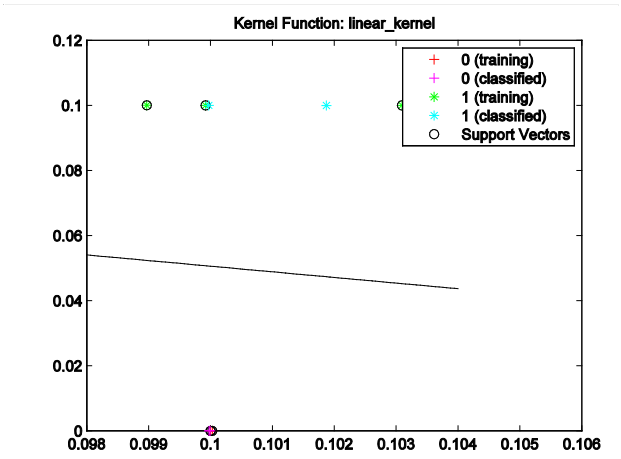

Figure 10. SVM level two classifier with linear kernel for higher order static M_{20}.

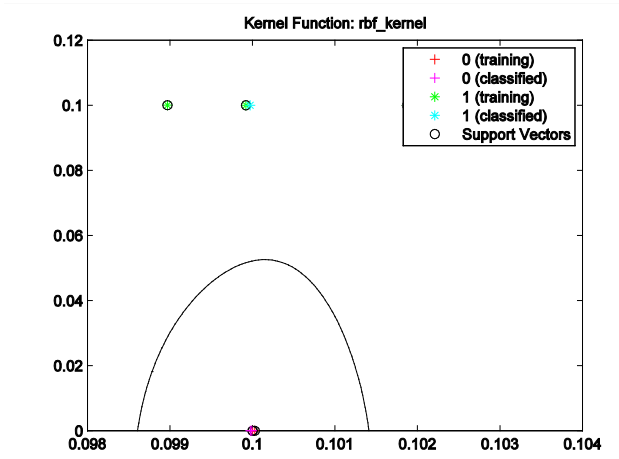

Figure 11. SVM level two classifier with RBF kernel for higher order static M_{20}.

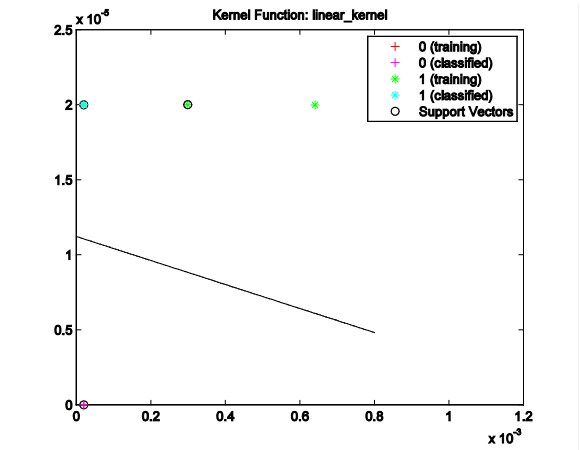

Figure 12. SVM level two classifier with linear kernel for higher order static M_{40}.

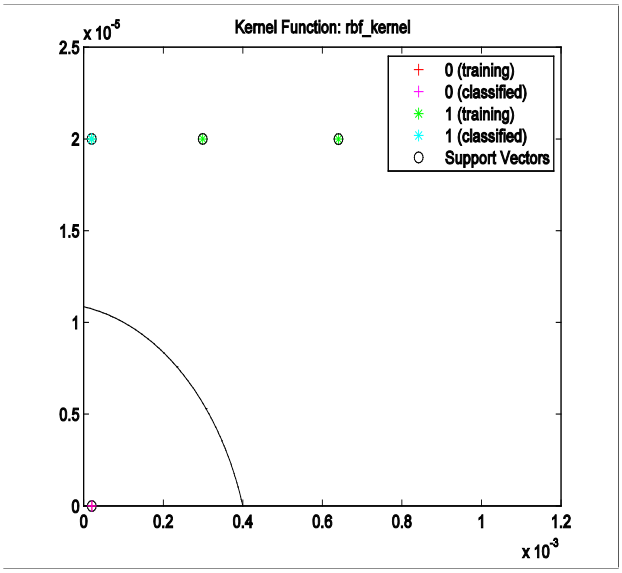

Figure 13. SVM level two classifier with RBF kernel for higher order static M_{40}.

kernel classifier . But in the second level of classification using the higher order statics M20 and M40 we are able to achieve the classification with 100% accuracy. But in order to decide finally whether the received signal is from the primary user signal or PUEA attacker signal we use both level result to combine as given in the equation (15)

4. Conclusion

PUEA attacker detection is the main security threat in the spectrum sensing of the cognitive radio network. There are many location based and received signal power based technique available. But there are only few machine learning based approach availed for this purpose .Here we have provided a SVM based two level confirmation of the primary user signal is presented that will enable more accurate detection of the PUEA attacker signal. The result shows that with 82% accuracy we can able to differentiate the both class of signal on level one to support and increase the accuracy level two classification is used using the higher order cumulant M20 and M40 where in that case we are able to achieve 100% accurate classification .

5. References

1. Vapnik V. The Nature of Statistical Learning Theory, Information Science and Statistics, Springer Science: New York, 2000.
2. Ghosh AK, Schwartzbard A. A study in using neural networks for anomaly and misuse detection, in: Proceedings of the 8th USENIX Security Symposium, Washington, DC, USA. 1999; 141–52.
3. Digham FF, Alouini MS, Simon MK. On the energy detection of unknown signals over fading channels, IEEE International Conference on Communications, ICC '03, 2003; 5. p. 3575–79.
4. Kim H, Shin K. In-Band Spectrum Sensing in IEEE 802.22 WRANs for Incumbent Protection. IEEE Transactions on Mobile Computing. 2008; 9(12):1766–79.
5. Avila J, Thenmozhi K. Upgraded Spectrum Sensing Method in Cognitive Radio Network. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–4.
6. Padmavathi G, Shanmugavel S. Performance analysis of cooperative spectrum sensing technique for low SNR regime over fading channels for cognitive radio networks. Indian Journal of Science and Technology. 2015 Jul; 8(16):1–5.
7. Yang Y, Liu Y, Zhang Q, Ni L. Cooperative boundary detection for spectrum sensing using dedicated wireless sensor networks, 2010. 29th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, San Diego, CA, 2010 Mar. p. 1–9.
8. Chen R, Park JM, Reed JH. Defense against primary user emulation attacks in cognitive radio networks. IEEE Journal on Selected Areas in Communications. 2008 Jan; 26(1):25–37.
9. Mathur CN, Subbalakshmi KP. Digital signatures for centralized DSA networks. Proceedings 4th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, CCNC. 2007. p. 1037–41.
10. Li H, Han Z. Dogfight in spectrum: jamming and anti-jamming in cognitive radio systems, in Proc. IEEE Global Telecommunications Conference, GLOBECOM' 2009, Honolulu, HI. 2009 Nov. p. 1–6.
11. Li H, Han Z. Blind dogfight in spectrum: combating primary user emulation attacks in cognitive radio systems with unknown channel statistics. Proceedings IEEE International Conference on Communications (ICC), Cape Town. 2010 May. p. 1–6.
12. Chen C, Cheng H, Yao YD, Hongbing Cheng CC. Cooperative Spectrum Sensing in Cognitive Radio Networks in the Presence of the Primary User Emulation Attack. IEEE Transactions on Wireless Communications. 2011 Jul; 10(7):2135–41.
13. Mukkamala S, Sung AH, Abraham A. Modeling Intrusion Detection Systems Using Linear Genetic Programming Approach Proceedings of Innovations in Applied Artificial Intelligence. 17th International Conference on Industrial and Engineering Applications of Artificial Intelligence and

Expert Systems (IEA/AIE), Springer: Berlin Heidelberg. 2004 May. p. 634–42.

14. Swami A, Sadler BM. Hierarchical Digital Modulation Classification using Cumulants. IEEE Transactions on Communications. 2000 Mar; 48(3):416–29.
15. Bhagavathy Nanthini S, Hemalatha M, Manivannan D, Devasena L. Attacks in Cognitive Radio Networks (CRN) - A Survey. Indian Journal of Science and Technology. 2014 Jan; 7(4):530–36.