PATTERN BASED ANOMALOUS USER DETECTION IN COGNITIVE RADIO NETWORKS

Sutharshan Rajasegarar[1], Christopher Leckie[1], Marimuthu Palaniswami[2]

[1]Dept. of Computing and Information Systems, [2] Dept.of Electrical and Electronic Eng.,
[1,2]The University of Melbourne, Australia, [1] National ICT Australia Victoria.
Email: {sraja, caleckie, palani}@unimelb.edu.au

ABSTRACT

Cognitive radio (CR) provides the ability to sense the range of frequencies (spectrum) that are not utilized by the incumbent user (primary user) and to opportunistically use the unoccupied spectrum in a heterogeneous environment. This can use a collaborative spectrum sensing approach to detect the spectrum holes. However, this nature of the collaborative mechanism is vulnerable to security attacks and faulty observations communicated by the opportunistic users (secondary users). Detecting such malicious users in CR networks is challenging as the pattern of malicious behavior is unknown *apriori*. In this paper we present an unsupervised approach to detect those malicious users, utilizing the pattern of their historic behavior. Our evaluation reveals that the proposed scheme effectively detects the malicious data in the system and provides a robust framework for CR to operate in this environment.

1. INTRODUCTION

Cognitive radio (CR) has become an important technology for efficient spectrum utilization. The CR system continuously monitors the spectrum using spectrum sensing and identifies the unused spectrum. Once the spectrum hole is identified, CR operates in those spectra where the primary user (licensed user) radio systems are idle [1]. This provides efficient usage of the spectrum, and has been used in many applications, such as emergency management, disaster recovery and by public safety personal [2].

Collaborative spectrum sensing (CSS) involve multiple secondary users or opportunistic users (SUs) performing spectrum sensing to detect any primary user (PU) present in the spectrum. This can introduce reliability and security vulnerabilities in the CR system due to its collaborative nature [3]. Some of the SUs in the system can report falsified information to the central node or fusion center (FC), where the reported values from each of the SUs, about the presence or absence of the PU in the spectrum in the current time interval are combined to make a decision about the availability of the spectrum. This falsified information can either be a genuine erroneous value or malicious secondary users (MUs) reporting values in order to invoke the FC to make an erroneous decision about the spectrum availability. This process may cause either under utilization of the spectrum (when the malicious FC makes a decision that the spectrum is currently utilized by the PU, when actually not) or leads to a denial of service attack by the MU. The latter occurs when the MUs make the FC believe that the spectrum is not utilized by the PU when actually it is. In this situation, the SUs will start transmitting while the PU is present in the spectrum and cause interference to the communication of the licensed PU, thereby denying his/her legitimate use. Therefore it is important to identify the existence of such MUs in the system and remove or minimize their impact on the FC's decision.

Detecting the existence of malicious data reported by the SUs is challenging. In [4] a pre-filtering method is introduced to identify extreme data based on the mean of the received spectrum sensing data. Weighted averages of all the reported values are used by the FC to detect the presence of PU in the spectrum. The weights are adjusted based on how far the values are from the mean of the observations. However, these statistical measures are not robust against extreme values in the data. Hence they proposed robust alternatives involving median and median absolute deviations. In [5] a statistical moment deviation method is used to detect the anomalous users. In [6] and [7] reputation based frameworks and modified Grubbs tests are used to detect anomalies. In [8], a Goodness-of-fit technique is used by comparing the empirical distribution of the SUs with the expected distribution of the MUs. In [9], largest gap methods utilising Tietjen-Moore and Shapiro-Wilk tests were used for detecting anomalous users. However, all these schemes operate on univariate data and use current or partial (previous time instance) data transmitted by the SUs. History information and the historic pattern of the normal and anomalous behavior is ignored in identifying the MUs. This limits the ability of the system in identifying changing or emerging anomalous patterns in the data.

In this paper, we present a technique that can effectively identify such anomalous data values from the SUs and hence mitigate their effect on the CR system. In particular, we formulate multi-dimensional feature vectors using the history of the (energy) data vectors collected from the SUs over a time period by the FC, and perform unsupervised (without any labeled data) anomaly detection on them. This formulation facilitates modeling the pattern of the (energy) time series behavior over a period, and detecting the anomalies. We map the data from the input space to a higher dimensional space using kernel methods and find a smooth surface in that space to separate the normal data and the anomalies. This smooth surface in the higher dimensional space corresponds to finding non-linear flexible boundaries for the normal pattern of the data in the input space, and hence facilitates accurate detection of complex, non-separable anomalies in the input space.

The rest of the paper is organized as follows. Section 2 introduces cognitive radio and the collaborative spectrum sensing problem in the presence of malicious users. Section 3 provides the unsupervised one-class support vector machine based malicious user detection framework. In Section 4, the proposed framework is evaluated, and followed by the conclusion and future work in Section 5.

2. COGNITIVE RADIO: SYSTEM MODEL

Consider a CR network consisting of K secondary users, a primary user and a common receiver called as a fusion center. Each SU performs spectrum sensing independently based on energy detection and communicates the detected energy values to the fusion center. Note that we use energy detection [10, 11] for spectrum sensing in this work for simplicity; albeit, the proposed mechanism is applicable in the case of any other sensing techniques, such as coherent detection [12] and cyclostationary feature detection [13]. The FC combines all the values collected from the SUs and makes a decision as to whether the PU is present (i.e., actively using the spectrum) or not (i.e., the spectrum is not used). This problem can be formulated as the binary hypothesis testing problem with $\mathscr{H}_0$ as *PU is absent* and $\mathscr{H}_1$ as *PU is in operation*.

Let us consider the spectrum sensing at a SU i. The sensing method decides between the following two hypotheses:

$$x_i(t) = \begin{cases} w_i(t), & \mathscr{H}_0 \\ h_i(t)s(t) + w_i(t), & \mathscr{H}_1 \end{cases} \quad (1)$$

where $x_i(t)$ is the received signal at the ith SU at time t, $s(t)$ is the primary signal, $w_i(t)$ is the additive white Gaussian noise, and $h_i(t)$ is the complex channel gain of the sensing channel between the ith SU and PU. The sensing channel $h_i(t)$ is considered to be a time-invariant channel during the sensing process as the sensing time is considered to be smaller than the coherence time (the time duration within which the channel impulse response is invariant) [10]. The status of PU is assumed to be unchanged during the sensing process. The PU signal and noise process at each CR is assumed to be an identical and independent random process with zero mean and variance σ_s^2 and σ_w^2 respectively. Further, it is assumed that $s(t)$ and $w(t)$ are independent of each other. The received signal to noise ratio (SNR) is given by $\gamma = \mathbb{E}[|h_i|^2]\sigma_s^2/\sigma_w^2$, where $\mathbb{E}[.]$ is the expectation operator.

The test statistic (energy values of the signal) E for the energy detector at each SU is given by [14]

$$E_i = \frac{1}{N}\sum_{j=1}^{N} |x_i(j)|^2 \underset{\mathscr{H}_0}{\overset{\mathscr{H}_1}{\gtrless}} \lambda_i \quad (2)$$

where N is the number of signal samples and λ_i is a predetermined threshold. For large N [14, 15], according to central limit theorem, the test statistic can be approximated by a Gaussian distribution. Assuming $h(t) = 1$, the expression for the probability of false alarm P_{fa}^i and the probability of detection P_d^i can be given as follows [9, 16]:

$$P_{fa}^i = Q\left[\left(\frac{\lambda_i}{\sigma_w^2} - 1\right)\sqrt{N}\right]$$

$$P_d^i = Q\left[\left(\frac{\lambda_i}{\sigma_w^2} - \gamma - 1\right)\frac{\sqrt{N}}{\gamma + 1}\right]$$

where $Q(.)$ is the tail probability of the normalised Gaussian distribution.

Data Fusion

The FC, upon receiving the energy values from SUs, combines them to arrive at a decision as to whether a PU is active in the spectrum or not. FC can use either a majority rule [10] to combine the evidence (i.e., the binary decision) from each SU as to whether the PU is present or not, or a weighted combination of the energy values for the decision. The weights can be assigned to be equal for all the SUs. However, if the presence of MUs in the SUs can be correctly detected, then the weights can be adjusted such that the contribution from the MUs are minimised or nullified in the decision making, hence providing robustness against the anomalous users. In order to identify such malicious users, below we present a mechanism that uses the energy values communicated by the SUs over a period of time.

In order to detect the anomalous users from the normal users, we use the energy values collected over a period from each SU, and denote them as a "energy vector", i.e., a feature vector in terms of machine learning terminology. Hence, an energy vector from the i^{th} SU can be denoted as a vector $y_i = [E_i(1), E_i(2), ..., E_i(m)]'$, where m is the time window of energy measurements considered by the FC for the data analysis. In this work, we use the One-Class Support Vector Machine (One-class SVM) to identify the anomalous data (energy) vectors. Note that the one-class SVM is fundamentally different from the traditional binary or two class SVMs. The one-class SVM is an unsupervised methodology which do not require any pre-labelled data or pre-training for identifying normal and anomalous data, as opposed to the traditional binary SVMs where labelled data are required for pre-training the system before use (supervised method).

3. ONE-CLASS SUPPORT VECTOR MACHINE

A variety of machine learning algorithms exist for anomaly detection in the literature [17–29]. A class of machine learning algorithms, called kernel methods, use *kernel functions* to emulate a mapping of data measurements from the *input space* (the space where the data is collected) to a higher dimensional space called the *feature space* [30–34]. The mapped vectors in the feature space are called *image vectors*. Linear or smooth surfaces in the feature space are used to classify the data as either normal or anomalous. The linear or smooth surfaces in the feature space usually yield nonlinear surfaces in the input space. The advantage of this method is that the dimension of the mapped feature space is hidden by the kernel function and is not explicitly known. This facilitates highly nonlinear and complex learning tasks without excessive algorithmic complexity.

A specific class of algorithms called one-class support vector machines (SVMs) do not require labeled data for training (i.e., an unsupervised scheme). In this scheme a separating smooth surface such as a hypersphere is found in the feature space, such that the surface automatically separates the data vectors into normal and anomalous. In these schemes, the proportion of data vectors considered to be anomalous is controlled by a parameter of the algorithm. Tax et al. [35] formulated the one-class SVM using a hypersphere, called support vector data description (SVDD). In this approach, a minimal radius hypersphere is fixed around the majority of the image vectors in the (higher dimensional) feature space. The data that falls outside the hypersphere are identified as anomalous. Figure 1 shows the geometry of the SVDD. This hypersphere formulation uses quadratic programming optimization [35].

Consider a data (energy) vector y_i in the *input space* from a set of data vectors $Y = \{y_i : i = 1..K\}$ mapped to a the *feature space* by some non-linear mapping function $\phi(.)$, resulting in a mapped vector $\phi(y_i)$ (*image vector*). Note that the K denotes the number of secondary users in the CR system. The aim of fitting a hypersphere with minimal radius R, having a center c and

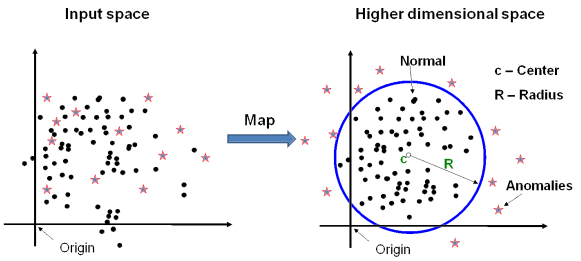

Figure 1: Geometry of the One-Class SVM

encompassing a majority of the image vectors in the feature space yields the following optimisation problem:

$$\begin{aligned} \min_{R\in\Re^+,\xi\in\Re^n} \quad & R^2 + \frac{1}{\nu K}\sum_{i=1}^{K}\xi_i \\ \text{subject to:} \quad & \|\phi(y_i) - c\|^2 \leq R^2 + \xi_i, \\ & \xi_i \geq 0, \ \ \forall i \end{aligned} \tag{3}$$

where $\{\xi_i : i = 1...K\}$ are the slack variables that allow some of the image vectors to lie outside the sphere. The parameter $\nu \in (0, 1]$ is the regularisation parameter which controls the fraction of image vectors that lie outside the sphere, i.e., the fraction of image vectors that can be *outliers* or *anomalies*. Using the Lagrange technique, the above primal problem (3) is converted to a dual problem as follows, which is a quadratic optimisation problem:

$$\begin{aligned} \min_{\alpha\in\Re^n} \quad & \sum_{i,j=1}^{K}\alpha_i\alpha_j k(y_i, y_j) - \sum_{i=1}^{K}\alpha_i k(y_i, y_i) \\ \text{subject to:} \quad & \sum_{i=1}^{K}\alpha_i = 1, \\ & 0 \leq \alpha_i \leq \frac{1}{\nu K}, \quad i = 1...K. \end{aligned} \tag{4}$$

where $k(y_i, y_j) = \phi(y_i).\phi(y_j)$ is the kernel function, and the α_i are the Largrange multipliers. The data vectors with $\alpha_i > 0$ are called the support vectors. Using the solution for α_i, the decision function for a data vector y can be written as

$$\begin{aligned} f(y) = sgn(R^2 - \sum_{i,j=1}^{K}\alpha_i\alpha_j k(y_i, y_j) + \\ 2\sum_{i=1}^{K}\alpha_i k(y_i, y) - k(y, y)). \end{aligned} \tag{5}$$

where $sgn(.)$ is the signum function. *Anomalous* data vectors are those with $\alpha_i = \frac{1}{\nu K}$, which fall outside the sphere. Data vectors with $0 \leq \alpha_i < \frac{1}{\nu K}$ fall inside or on the the sphere, and are considered *normal* [35]. The kernel function that we use in here is the radial basis function given by:

$$k(y_i, y_j) = exp\left(\frac{-\|y_i - y_j\|^2}{\sigma^2}\right) \tag{6}$$

where, σ is the kernel width parameter. A larger value for σ provides a smoother boundary around the data, while a smaller value provides a rugged boundary. It can be shown that ν is an upper bound on the fraction of anomalies and a lower bound for the fraction of support vectors. The ν and σ are the two parameters of this algorithm that need to be tuned depending on the data set [35].

4. EVALUATION

The aim of this evaluation is to asses the proposed scheme for its accuracy in detecting various malicious users in CR networks. We also perform a study on the number of malicious users that can be detected in a given set of SUs. Further, we analyse the effect of the attack strength δ on the detection accuracy (for malicious user detection).

In order to perform the evaluation, we use the following malicious user attack scenarios as identified in [36]. Each malicious user thwarts the system performance by two types of attacks, namely

- Attack-1: reporting an increased energy value $y_i + \delta$ when the PU is inactive, thus increasing the false alarm rate.
- Attack-2: reporting a decreased energy value $y_i - \delta$ when primary user is active, thus increasing the missed detection rate.

We used the following CR system for evaluation. The total number of SUs $K = 50$, $N = 50$, $m = 100$ and the SNR $\gamma = 10dB$. We randomly switch the attacks in the system between Attack-1 and Attack-2 with a probability of 0.5. A real-valued Gaussian Primary User signal is used along with a Gaussian noise with zero mean and unit variance.

In order to analyse the system's performance with the increasing number of malicious users in the CR system, we changed the percentage of MUs in the total number of SUs from 0% to 100% in steps of 5%. The attack strength δ is changed uniformly at random in the range $[4\lambda_i, 8\lambda_i]$, where the λ_i is chosen using $\lambda_i = Q^{-1}(P^i_{fa})/\sqrt{N} + 1$, for a given $P^i_{fa} = 0.1$. The σ is chosen to be 100 after a systematic search that gives the highest detection performance. The simulation is performed with the one-class SVM, and the Receiver Operating Characteristic (ROC) curves are produced with different ν values. The area under the curve (AUC) is computed for each simulation while changing the number of MUs. The simulation is run for 50 iterations of different realisations of the random values, and the mean and the standard deviation of the AUC values are computed. Figure 2 shows the AUC with the number of malicious users present in the system. The proposed scheme detects anomalies with high accuracy for a small number of MUs present in the system. As the number of MUs increase beyond 50% the AUC values go below 0.5, meaning it becomes worse than random guessing. This is expected as the majority of the SUs become MUs, the normal behavior will be masked by the anomalous behavior, and hence becomes undetectable.

In order to analyse the performance of the detector with the strength of attack, we changed the attack strength δ from 0 to 25 in steps of 0.1, while keeping the percentage of MUs fixed at 20%. The AUC values are computed as before. Figure 3 shows the detector's performance with the attack strength δ. It can be observed that when the δ is small, the anomalous energy values fall inside the region of normal energy values, hence become difficult to detect. However, when the strength increases, it becomes easily detectable by the detector. This shows the sensitivity of our detector for the CR system.

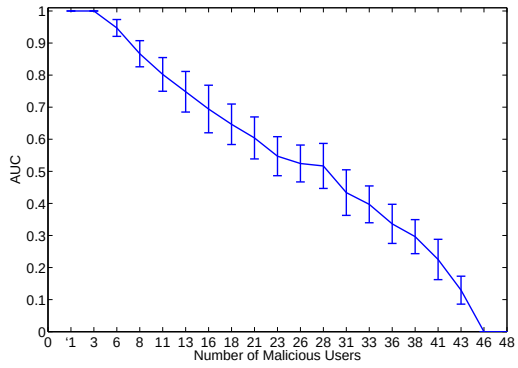

Figure 2: AUC vs Number of Malicious Users

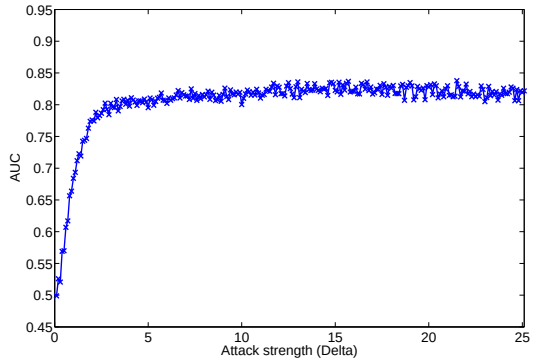

Figure 3: AUC vs Attack strength (Delta)

5. CONCLUSION

Detecting malicious users (MUs) in a cognitive radio network is crucial for robust and secure functioning of the network. In order to correctly identify the malicious users in the CR, we proposed an unsupervised machine learning based scheme that used the history of the energy measurements that the secondary users communicate to the fusion center in order to perform robust spectrum sensing. Further, we analysed the effect of the number of MUs in the system, and the detector's sensitivity in terms of the severity of the attacks. The results reveal that our scheme is capable of detecting MUs with higher detection accuracies, even when it switches between various attack scenarios. In the future, we plan to implement an incremental scheme that can perform on-line detection as new energy vectors become available.

6. ACKNOWLEDGMENT

We thank the support from ARC (LP120100529, LP130101038); University of Melbourne ECR; EU FP7 SocIoTal; and National ICT Australia (NICTA).

7. REFERENCES

[1] "Federal Communications Commission - FCC 03-322," http://web.cs.ucdavis.edu/~liu/289I/Material/FCC-03-322A1.pdf, 2003.

[2] M. Di Felice, A. Trotta, L. Bedogni, L. Bononi, F. Panzieri, G. Ruggeri, V. Loscri, and P. Pace, "Stem-mesh: Self-organizing mobile cognitive radio network for disaster recovery operations," in *9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, July 2013, pp. 602–608.

[3] R. Sharma and D. Rawat, "Advances on security threats and countermeasures for cognitive radio networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. PP, no. 99, pp. 1–1, 2014.

[4] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *IEEE Transactions on Wireless Communications*, vol. 9, no. 8, pp. 2488–2497, August 2010.

[5] A. Javid, S. Rajasegarar, K. Arshad, and K. Moessner, "A statistical moment deviation approach to identify outliers in collaborative spectrum sensing for cognitive radio," in *Proceedings of the Future Network and MobileSummit*, July 2012.

[6] K. Arshad and K. Moessner, "Robust collaborative spectrum sensing in the presence of deleterious users," *IET Communications*, vol. 7, no. 1, pp. 49–56, Jan 2013.

[7] T. Zhang, R. Safavi-Naini, and Z. Li, "Redisen: Reputation-based secure cooperative sensing in distributed cognitive radio networks," in *IEEE International Conference on Communications (IEEE ICC)*, June 2013, pp. 2601–2605.

[8] G. Noh, S. Lim, S. Lee, and D. Hong, "Goodness-of-fit-based malicious user detection in cooperative spectrum sensing," in *IEEE Vehicular Technology Conference (VTC Fall)*, Sept 2012, pp. 1–5.

[9] S. S. Kalamkar, P. K. Singh, and A. Banerjee, "Block outlier methods for malicious user detection in cooperative spectrum sensing," in *IEEE VTC*, South Korea, May 2014.

[10] W. Zhang, R. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5761–5766, December 2009.

[11] D. Cabric, A. Tkachenko, and R. W. Brodersen, "Experimental study of spectrum sensing based on energy detection and network cooperation," in *Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum*, ser. TAPAS '06. New York, NY, USA: ACM, 2006. [Online]. Available: http://doi.acm.org/10.1145/1234388.1234400

[12] F. Moghimi, R. Schober, and R. Mallik, "Hybrid coherent/energy detection for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 10, no. 5, pp. 1594–1605, May 2011.

[13] V. Turunen, M. Kosunen, A. Huttunen, S. Kallioinen, P. Ikonen, A. Parssinen, and J. Ryynanen, "Implementation of cyclostationary feature detector for cognitive radios," in *CROWNCOM*, June 2009, pp. 1–4.

[14] K. Arshad, "Malicious users detection in collaborative spectrum sensing using statistical tests," in *Intl. Conf. on Ubiquitous and Future Networks*, July 2012, pp. 109–113.

[15] P. K. Varshney, *Distributed Detection and Data Fusion*. Secaucus, NJ, USA,: Springer, 1996.

[16] Y.-C. Liang, Y. Zeng, E. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. on Wireless Comms.*, vol. 7, no. 4, pp. 1326–1337, April 2008.

[17] J. Shawe-Taylor and N. Cristianini, *Kernel Methods for Pattern Analysis*, 2004.

[18] C. O. Reilly, A. Gluhak, M. A. Imran, and S. Rajasegarar, "Anomaly detection in wireless sensor networks in a non-stationary environments," *IEEE Comms. Surveys and Tut.*, vol. 16, no. 3, pp. 1413–1432, 2014.

[19] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Anomaly detection in wireless sensor networks," *IEEE Wireless Comms.*, vol. 15, no. 4, pp. 34–40, August 2008.

[20] S. Rajasegarar, C. Leckie, M. Palaniswami, and J. C. Bezdek, "Distributed anomaly detection in wireless sensor networks," in *IEEE ICCS 2006*, Singapore, October 2006.

[21] S. Rajasegarar, A. Gluhak, M. A. Imran, M. Nati, M. Moshtaghi, C. Leckie, and M. Palaniswami, "Ellipsoidal neighbourhood outlier factor for distributed anomaly detection in resource constrained networks," *Pattern Recognition*, vol. 47, no. 9, pp. 2867–2879, 2014.

[22] S. Rajasegarar, C. Leckie, and M. Palaniswami, "Hyperspherical cluster based distributed anomaly detection in wireless sensor networks," *Jnl. of Parallel and Distributed Computing*, vol. 74, no. 1, pp. 1833–1847, 2014.

[23] ——, "Detecting data anomalies in sensor networks," in *Security in Ad-hoc and Sensor Networks*, R. Beyah, J. McNair, and C. Corbett, Eds. World Scientific Publishing, Inc, ISBN: 978-981-4271-08-0, July 2009, pp. 231–260.

[24] S. Rajasegarar, J. C. Bezdek, C. Leckie, and M. Palaniswami, "Elliptical anomalies in wireless sensor networks," *ACM Trans. on Sensor Networks*, vol. 6, no. 1, p. 28, Dec. 2009.

[25] J. C. Bezdek, T. Havens, J. Keller, C. Leckie, L. Park, M. Palaniswami, and S. Rajasegarar, "Clustering elliptical anomalies in sensor networks," in *IEEE WCCI*, 2010.

[26] D. Kumar, M. Palaniswami, S. Rajasegarar, C. Leckie, J. C. Bezdek, and T. C. Havens, "clusivat: A mixed visual/numerical clustering algorithm for big data," in *IEEE BigData*, 2013, pp. 112–117.

[27] M. Moshtaghi, S. Rajasegarar, C. Leckie, and S. Karunasekera, "An efficient hyperellipsoidal clustering algorithm for resource-constrained environments," *Pattern Recog.*, vol. 44, no. 9, pp. 2197–2209, 2011.

[28] M. Moshtaghi, T. Havens, L. Park, J. C. Bezdek, S. Rajasegarar, C. Leckie, M. Palaniswami, and J. Keller, "Clustering ellipses for anomaly detection," *Pattern Recog.*, vol. 44, no. 1, pp. 55–69, 2011.

[29] A. Shilton, S. Rajasegarar, C. Leckie, and M. Palaniswami, "DP1SVM: A dynamic planar one-class support vector machine for internet of things environment," in *Accepted for IEEE ISSNIP*, 2015.

[30] B. Scholkopf and A. Smola, *Learning with Kernels*. MIT Press, 2002.

[31] S. M. Erfani, M. Baktashmotlagh, S. Rajasegarar, S. Karunasekera, and C. Leckie, "R1SVM: a randomised nonlinear approach to large-scale anomaly detection," in *AAAI-15*, Jan. 2015.

[32] A. Shilton, S. Rajasegarar, and M. Palaniswami, "Combined multiclass classification and anomaly detection for large-scale wireless sensor networks," in *IEEE ISSNIP*, 2013, pp. 491–496.

[33] S. Rajasegarar, C. Leckie, J. C. Bezdek, and M. Palaniswami, "Centered hyperspherical and hyperellipsoidal one-class support vector machines for anomaly detection in sensor networks," *IEEE Trans. on Info. Forensics and Sec.*, vol. 5, no. 3, pp. 518–533, 2010.

[34] S. Rajasegarar, A. Shilton, C. Leckie, R. Kotagiri, and M. Palaniswami, "Distributed training of multiclass conic-segmentation support vector machines on communication constrained networks," in *ISSNIP*, 2010, pp. 211–216.

[35] D. M. J. Tax and R. P. W. Duin, "Support vector data description," *Machine Learning*, vol. 54, no. 1, pp. 45–66, 2004.

[36] S. Jana, K. Zeng, and P. Mohapatra, "Trusted collaborative spectrum sensing for mobile cognitive radio networks," in *IEEE INFOCOM*, March 2012, pp. 2621–2625.