Sequential Statistical Analysis-Based Method for Attacks Detection in Cognitive Radio Networks

Vladimir Shakhov
Department of Electrical, Electronic and Computer Engineering
University of Ulsan
Ulsan, Korea
shakhov@mail.ulsan.ac.kr

***Abstract*—This Cognitive radio networks are vulnerable to specific intrusions due to the unique cognitive characteristics of these networks. This DoS attacks are known as the Primary User Emulation Attack and the Spectrum Sensing Data Falsification. If the intruder behavior is not statistically identical to the behavior of the primary users, intrusion detection techniques based on observing the energy of the received signals can be used. Both machine learning-based intrusion detection and sequential statistical analysis can be effectively applied. However, in some cases, statistical sequential analysis has some advantages in dealing with such challenges. This paper discusses aspects of using statistical sequential analysis methods to detect attacks in Cognitive radio networks.**

Keywords— cognitive radio networks, information security, intrusion detection, sequential statistical analysis

I. INTRODUCTION

Cognitive radio is an attractive approach to improve spectrum use by providing opportunistic spectrum access to unlicensed users. The concept of cognitive radio allows a secondary user (SU) to discover and efficiently use any available valid spectrum from primary users (PU) at a given time [1]. Cooperative spectrum sensing can significantly improve the efficiency of cognitive radio networks. The desired effect has to be achieved by merging and processing observations received from spatially located SUs. A set of SUs collaborates to share their sensing information in order to reach the required decision with improved accuracy.

Cognitive radio networks are wireless in nature. Therefore, they are vulnerable to almost all intrusions encountered in traditional wireless networks. These attacks include various types of jamming, MAC address spoofing, eavesdropping, etc. Moreover, cognitive radio networks have created new security challenges due to the unique cognitive characteristics of these networks. The previous literature on cognitive radio dealt with various approaches to spectrum management, and there is a lot of relevant works, but security issues have not been given due attention [2]. The main operation of Cognitive radio is spectral sensing. The priority of PUs is higher, SUs should not interfere. The specific spectrum band used by the PU must be released. Attackers can take advantage of this circumstance and imitate PU transmitters in order to force the system to vacate some spectrum band. This DoS attack is known as the Primary User Emulation Attack (PUEA).

Another attack specific to Cognitive radio is as follows. Intruders influence the overall spectrum assessment and allocation decision by reporting false data. This is known as the spectrum sensing data falsification (SSDF). For example, attacker can initiate an SSDF attack by passing misleading sensor data to a decision center.

Thus, to improve Cognitive radio networks reliability and survivability, the relevant efficient methods of intrusion detection are required.

II. PRELIMINARIES

In general, cooperative spectrum sensing process can be described as follows [3]. There is a control center (also called fusion center). This center control manages cooperative spectrum sensing, being responsible for individually sensing, supporting quality of service for network nodes, combining and processing data, allocating resources, interacting with PUs, and so on. A collaborative cognitive secondary users sense the spectrum status of a PU individually. All cooperating secondary users send their sensing data to the control center. The center combines the SU data to obtain the decision about the PU spectrum, and disseminates information to secondary users. There is feedback between the SU and the control center during which information about the state of the PU spectrum is specified and refined. Cognitive radio technology is based on the premise that SUs do not interfere with PUs. If this does happen, the PU sends a complaint to the control center to report the violation. These complaints are useful for the control center to verify if its decision is correct or if the feedback to SU is adequate. Thus, false sensing data can be detected.

Detection of PU activity based on the observed signal energy is a choice of one of two alternatives as follows:

- Hypothesis H_1 : the channel is idle;
- Hypothesis H_2: existence of the PU signal;

where

$$x(t) = \begin{cases} n(t), & H_1 \\ h(t)s(t) + n(t), & H_2 \end{cases}$$

Here $x(t)$ means the received samples at the sensing node (i.e. the detected signal at SU), $s(t)$ is the transmitted PU signal, $h(t)$ is the channel gain from primary transmitter to sensing node, $n(t)$ is the zero-mean normally distributed random value representing the additive white Gaussian noise, t is the sample index.

The energy of *N* samples are summed. Next, the detection mechanism uses it for local energy detection at each cognitive radio user. The obtained energy of the cognitive radio user can be taken into account in the following ways [4]:

$$E = \sum_{n=1}^{N} (x(t))^2$$

or [5]

$$E = \sum_{n=1}^{N} x(t)$$

Thus, energy detection mechanism adds the energy of *N* samples together. Next, it compares the output with a certain detection threshold d_h as follows:

$$y(E) = \begin{cases} 1, & \text{if } E \geq d_h \\ 0, & \text{else} \end{cases}$$

In some cases, the quality of PU activity accounting has been obtained. For example, in [4] the closed-form expressions for the probabilities of false alarm (P_{fa}) and miss detection rate (P_{lost}) are provided:

$$P_{fa}(y(E) = 1|\mathrm{H}_1) = Q(\frac{d_h - N}{\sqrt{2N}})$$

$$P_{fa}(y(E) = 0|\mathrm{H}_2) = Q(\frac{(N - d_h)\tilde{\gamma}}{\tilde{\gamma}\sqrt{2N}})$$

where Q(*) is the Q-function for standard normal distribution, $\tilde{\gamma}$ is the PU dispersion gain. The local threshold d_h is determined by the target false alarm probability. If the estimated energy of is larger than the decision threshold, the existence of PU would be declared. Otherwise, if the energy of *y*(t) is smaller than the threshold, it is declared that no PU signal. Obviously, an intruder can quite easily affect the received signal or distort information about it. Both PUEA and SSDF attacks exploit these vulnerabilities in spectrum sensing [6].

III. DETECTION TECHNIQUE

If the mobility of nodes in cognitive radio networks is low and the intruder cannot mimic a PU, then the observed signal energy can be described as follows:

$$x(t) = \begin{cases} n(t), \\ a(t) + n(t), \\ h(t)s(t) + n(t), \\ h(t)s(t) + a(t) + n(t) \end{cases}$$

where $a(t)$ is the attacker impact. In this situation, intrusion detection methods based on machine learning can be effectively applied [7]. Also, sequential statistical analysis can be applied for these purposes.

From this point of view the observations of signal energy form a random sequence $X_1, X_1, \ldots, X_k, \ldots$ This sequence at time t_a abruptly changes the properties uniquely determined by the parameter vector ϑ . In other words, $X_1, X_1, \ldots, X_{t_a-1}$ have the cumulative distribution function (CDF) $F(\vartheta_1)$ and the probability density function (pdf) $f(\vartheta_1)$, $X_{t_a}, X_{t_a-1}, \ldots$ have the CDF $F(\vartheta_2)$ and the pdf $f(\vartheta_2)$ i.e. the same distribution law, but the distribution parameter is changed. Observing the sequence, it is necessary to detect the moment of discord. With sequential detection, the observations are processed continuously, and the decision about the presence of a discord must be made in real time with the advent of the next observation.

The change-point detection method is based on the analysis of the behavior of the cumulative sum as follows:

$$S_k = S_{k-1} + \ln\left(\frac{f(X_k|\vartheta_2}{f(X_k|\vartheta_1}\right)$$

Since the sum decreases before the discord, and after it increases, it is possible to calculate the following difference at each step [8]:

$$S_k - \min_{j \leq k} S_j$$

As soon as this value exceeds the threshold value, declare discord. The decision rule is as follows:

$$t_a = \inf\{\, k : d_k > h\}$$

where

$$d_k = S_k - \min_{j \leq k} S_j$$

As applied to the PUEA situation, the observed sequence has a normal distribution, $\mathcal{N}(\vartheta, \sigma^2)$. The parameter ϑ is the mean. In this case, the formula for the cumulative sum is as follows

$$S_k = \frac{\theta_2 - \theta_1}{\sigma^2} \sum_{i=1}^{k} \left(X_i - \frac{k(\theta_2 + \theta_1)}{2}\right)$$

Note that the use of an intrusion detection method based on sequential statistical analysis is preferable than ML-based one, since it is sufficient to detect a statistical anomaly in general. A train data set is not required.

Let us consider a situation where the behavior of attackers is statistically identical to the behavior of PU. In this case, it is impossible to detect an attack based on the observation of signal energy. However, due to the decrease in the number of available channels, the probability of receiving a channel for SUs decreases. The idea of detecting the presence of an intrusion is to cooperatively observe a discrete random variable: the number of successful outcomes when SUs receive channels.

The random number (ξ) of successful SU attempts to get a channel corresponds to the binomial distribution, i.e.

$$p(\xi = k) = C_m^k p_0^k (1 - p_0)^{m-k}$$

here *m* is a number of trial in a session, p_0 is the probability of success in one trial. After activating the intruders, the probability of success in one attempt became p_A,

$$p_A < p_0$$

and now

$$p(\xi = k) = C_m^k p_A^k (1 - p_A)^{m-k}$$

Let C be the number of SUs in an attacked cluster. With cooperation, the number of trials will increase to mC. Taking into account that the sum of binomially distributed quantities is a random variable distributed according to the binomial law,

we obtain the probability mass function (pmf) for the number of sacksful outcomes in a cluster.

$$p(\xi = k) = C_{mC}^{k} p_0^k (1 - p_0)^{mC-k}$$

Let us make the following assumption. In some cases, if the intrusion is detected for some time, then the harm is negligible. Therefore, the delay is acceptable in this case. This assumption gives us a possibility to obtain a closed-form expression for the optimal threshold value in the cumulative sum algorithm. Let the allowable lag be equal to *T* observation units. If the alarm is given at any time after t_a and before $t_a + T$, then the intrusion has been successfully detected. Otherwise, we will get a false alarm or a missed intrusion.

Let us collect cooperative observations and use the following decision rule for the discord detection:

$$\sum_{k=1}^{T} \xi_k < h$$

Thus, the probability that the process will not be interrupted too early equals

$$P\left(\sum_{k=1}^{T} \xi_k > h \mid p_0\right)$$

Fixing the probability of false alarm, α,

$$P\left(\sum_{k=1}^{T} \xi_k < h \mid p_0\right) = \alpha$$

we obtain the optimal threshold value:

$$h_{opt} = \arg\max\left\{\sum_{k=0}^{h} C_{mCT}^{k} p_0^k (1 - p_0)^{mCT-k} \le \alpha\right\}$$

Changing the false alarm rate will affect the probability of disorder detection.

IV. PERFORMANCE ANALYSIS

Let the number of trials in a session be 5 and the number of nodes in a cluster be 10. Assume, $p_0 = 0.5, p_1 = 0.45$. A typical observed process is shown in Figure 1.

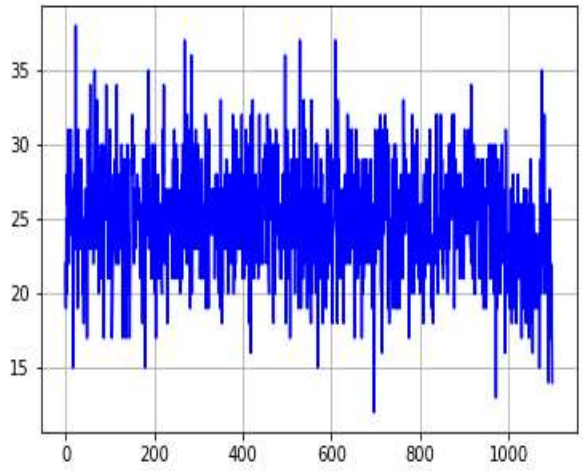

Fig. 1. Example of obsevations.

Here, the change point moment is 1000. Let the admissible lag, *T*, equals 10. Next, we calculate optimal threshold values for various desired false alarm rate (if $\alpha = 0.05$ then $h_{opt} = 231$ etc.) and get the intrusion detection efficiency. The results are shown in Figure 2.

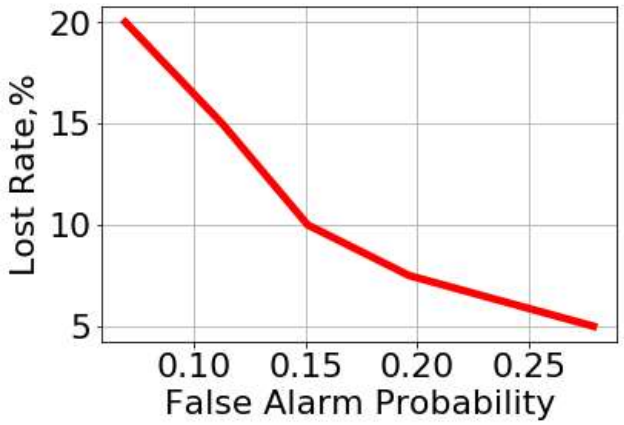

Fig. 2. Intrusion detection efficiency.

Please note that the value of *T* is substantially smaller than the typical size of a train dataset. If *T* is increased, then the false positive rate and the probability of intrusion detection can be greatly improved.

V. CONCLUSIONS

The main function of Cognitive Radio is spectral sounding, which is used to implement the principle: secondary users do not interfere with primary ones. Attackers see this as an opportunity to attack the system and can imitate primary user transmitters to force the system to release some band of spectrum. This leads to DoS attacks specific to Cognitive radio networks, such as Primary User Emulation Attack and the Spectrum Sensing Data Falsification. Based on observations of the energy of the received signal, intrusion detection methods have been developed based on the technique of machine learning and statistical sequential analysis. The use of an intrusion detection method based on sequential statistical analysis can be preferable than machine learning based one, since it is sufficient to detect a statistical anomaly in general. A train data set is not required. In the case when the behavior of intruders is statistically identical to the behavior of the main users, we propose an effective intrusion detection method based on the cumulative sum algorithm.

ACKNOWLEDGMENT

This work was supported by a National Research Foundation of Korea (NRF) grant through the Korean Government (MSIT) under Grant NRF-2020R1I1A1A01065692.

REFERENCES

[1] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, “Cooperative spectrum sensing in cognitive radio networks: A survey,” Phys. Commun., vol. 4, no. 1, pp. 40–62, Feb. 2011.

[2] J. Feng, S. Li, S. Lv, H. Wang and A. Fu, "Securing Cooperative Spectrum Sensing Against Collusive False Feedback Attack in Cognitive Radio Networks," in IEEE Transactions on Vehicular Technology, vol. 67, no. 9, pp. 8276-8287, Sept. 2018.

[3] A. G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 428-445, 2013.

[4] A. A. Sharifi and M. J. Musevi Niya, "Defense Against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach," in IEEE Communications Letters, vol. 20, no. 1, pp. 93-96, Jan. 2016.

[5] A. Attar, H. Tang, A. V. Vasilakos, F. R. Yu and V. C. M. Leung, "A Survey of Security Challenges in Cognitive Radio Networks: Solutions and Future Research Directions," in Proceedings of the IEEE, vol. 100, no. 12, pp. 3172-3186, Dec. 2012.

[6] K. G. Shin, H. Kim, A. W. Min, and A. Kumar, “Cognitive radios for dynamic spectrum access: From concept to reality,” IEEE Wireless Commun. Mag., vol. 17, no. 6, pp. 64–74, Dec. 2010.

[7] M. Camana, C. Garcia, I. Koo and V. Shakhov, "Machine Learning Based Primary User Emulation Attack Detection," 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2022, pp. 244-248.

[8] A. Tartakovsky, I. Nikiforov, M. Basseville. Sequential Analysis: Hypothesis Testing and Changepoint Detection, CRC Press: Boca Raton, FL, USA, 2014.

[9] V. Shakhov and I. Koo, "Depletion-of-battery attack: Specificity modelling and analysis", Sensors, vol. 18, no. 6, pp. 1849, 2018.

[10] V. Shakhov, H. Choo, Y. Bang. Discord model for detecting unexpected demands in mobile networks. J. Future Gen. Comput. Syst. 2004, 20, 181–188.