Volume 4, Issue 1, January 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Improving Fuzzy Network Profiling for Intrusion Detection System in Cognitive Radio Network

G. HariPriya, G. Kavitha, Vijaya Lekshmi S.B.
PG Scholar
Department of CSE
SNS Coll. of Engineering, India

Abstract— A cognitive radio network is an intelligent system that can be changed vigorously. It detects the available channel in the radio spectrum automatically. According to that it can changes the transmission parameter to allow concurrent communication in a given spectrum.The operational aspects of cognitive radio are being explored and more attention are given to its security aspects.The CRN is based on IEEE wireless regional area network(WRAN). It describe some of the security threats. The attacker may be external users or secondary users. But cognitive network issensitive to security threats . Secondary users in the CRN to quickly detect the attack , by a simple yet effective IDS ispresented.There are different types of attacks created by the malicious users. To overcome these issues we use intrusion detection system (IDS), to find the abnormal behavior of the system due to attacks . It can adopt the anomaly detection approach and use non-parametric cumulative sum(cusum) as a change point detection algorithm to discover the threats in the system. The proposed system is to enhance the detection sensitivity of Intrusion detection system in Fuzzy inference system with low detection latency.

Keywords— Anomaly-IDS, Fuzzy inference system, CRN.

I. INTRODUCTION

The cognitive radio is intelligent radio that can be programmed dynamically. Federal communication commission in the US found the most radio frequency spectrum was inefficiently utilized. So FCC approve in September 2010 new rules to allow unlicensed users to utilize the spectrum that can be reserved for wireless broadband services. But they would not cause any interference to licensed users. It can adapt to changes in their environment to better use of the radio spectrum.CRNs help to solve the spectrum shortage problem. CR network are able to provide the high bandwidth to mobile users via heterogeneous architecture and dynamic spectrum accessing technique. CR network impose unique challenges due to the coexistence with primary networks as well as diverse QOS requirement. Thus new spectrum management functions are required for CR network to meet critical design challenges. Intrusion detection system (IDS) is a device that can monitoring the network or system activities for malicious activities. It inspects all activities in the network and identifies suspicious pattern that may indicate a network or system from someone try to break into or compromise a system. In this paper, anomaly intrusion detection system is used to detect the intrusion in very efficient manner.

II. ANOMALY-BASED INTRUSION DETECTION SYSTEM

Anomaly- IDS is based on defining the network behavior. The network behavior is based on the predefined behavior. Then it is accepted or it triggers the event in the anomaly detection. An anomaly is just an event that is suspicious from the perspective of security. The important in defining the network behavior is the IDS engine capability to cut through the various protocols at all levels. The engine must able to process the protocols and understand its goals. By increasing rule set helps in less false positive alarms. The efficiency of the system depends on how well it is implemented and tested on all protocols. Rule defining process is also affected by various protocols used by various vendors. For detection to occur correctly, the detailed knowledge about the accepted network behavior need to be developed by the administrator.In intrusion detection system, signature –based is another approach is used to detect the intruders in the system or network. Signature- based engines is that novel attack for which a signature does not exist can be detected if it falls out of the normal traffic patterns. But signature-based system does not detect the new attacks. It can able to known attacks and then it compare with previous attacks. In this paper, we proposed anomaly intrusion detection system in fuzzy inference system. It can increase the sensitivity of the network.It can also unknown attacks in the system or network or device. It is an effective IDS technique to detect the intruders. Anomaly-based detectors to estimate the "normal" behavior and abnormal behavior of the system.

III. FUZZY INFERENCE SYSTEM

A fuzzy inference system(FIS) is a system that uses fuzzy set theory to map inputs to outputs. FIS uses a collection of fuzzy membership functions and rules. Instead of using the Boolean logic for the data. Tools for working with fuzzy systems allow more than one conclusion per rule. The set of rules in afuzzy system is called as a knowledge

base. The functional operations in fuzzy system proceed by Fuzzification, Fuzzy inferencing, Aggregation of all outputs and Defuzzification. Fuzzy techniques is used to improve the system performance and sensitivity of the system . It can produce optimal solution.

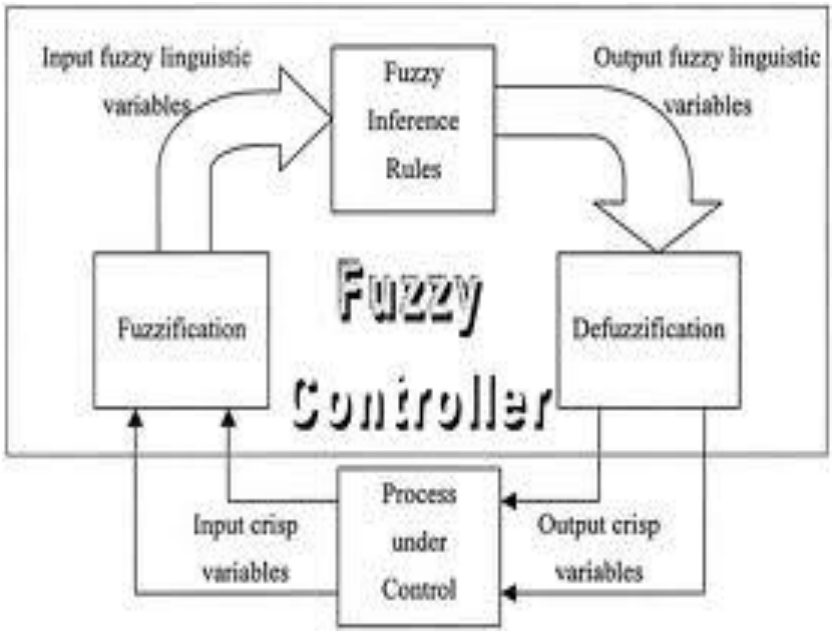

Fig. 1 Fuzzy Inference System with Fuzzy Controller

IV. RELATED WORK

The IEEE 802.22 activity is the first worldwide effort to define a standardized air interface based on CR techniques for the opportunities use of TV bands on interfering basis. An introduction to first wireless standard based upon CRNs is presented in the work by cordreio et al.[1] in 2006. The work demonstrated the prospect of CRN-based wireless communication by using the IEEE 802.22 WRAN technology. The security threats against CRN have been studied by a number of recent researchers. A noteworthy survey on the existing attacks against CRNs was carried out by Olga et al.[3] that analyzes the CRN security problems. R.Nakkeeran et al[] incorporated agents and data mining techniques to prevent anomaly intrusion in mobile adhoc network. The agents monitor the neighboring nodes information and then it collect all information from the agents to determine the correlation among the observed anomalous pattern.Z. M. Fadlullah et al [8] proposed a traffic features via information to build the efficient intrusion detection system model.

V. SYSTEM OVERVIEW

CRN Model is based on the IEEE 802.22 WRAN. The IEEE Specification can allow a number of cells and it can managed by Base station(BS). The network-centric architecture of cognitive radio under consideration is aimed at providing a high-performance platform for experimentation with various adaptive wireless network protocols ranging from simple to more complex ad-hoc collaboration. The design provides for fast RF scanning capability, an RF transceiver working over a range of frequency bands and a software-defined radio modem capable of supporting a variety of waveforms including OFDM and DSSS/QPSKprotocol for packet processing and routing functionality. The general purpose processor for implementation of spectrum policies and algorithms. Primary users is an authorized user in the network. Secondary user is the unauthorized user. White spaces is knows as unused portion of the spectrum in the network. Each Secondary users can use software radio to sense whether the primary users is occupying the channel or not. If the secondary users can have unused spaces means, it can intelligently adapt the unused channel of the radio spectrum of the network.The system combines simple network traffic network traffic metrics with fuzzy rules to determine the likelihood of specific or general network attacks.

The idea of a cognitive radio extends the concepts of a hardware radio and a software defined radio (SDR) from a simple and single function device to a cognitive radio that senses and reacts to its operating environment. A Cognitive Radio take information from multiple sources of todetermines its current operating settings and collaborates with other cognitive radios in awireless network. The cognitive radios is improved use of spectrum resources,reduced planning time, engineering and adaptation to current operating conditions.

Features of cognitive radio networkinclude:

- Sensing the radio frequency spectrum environment
- Policy and configuration databases
- Self-configuration
- Mission-oriented configuration
- Adaptive algorithms
- Distributed collaboration

VI. SUPPORT VECTOR MACHINE

A support vector machine (SVM) is a computer algorithm that learns by assign labels to objects. An SVM can learn to recognize fraudulent credit card activity by examining hundreds or thousands of fraudulent and nonfraudulent credit card activity reports. Alternatively, an SVM can learn torecognize handwritten digits by examining a large collection of scanned images of hand-written zeroes, ones and so forth. SVMs have also been successfully applied to an increasingly wide variety of biological applications. A common biomedical application of support vector machines is the automatic classification of microarray gene expression profiles. Theoretically, an SVM can examine the gene expression profile derived from a tumor sample or from peripheral fluid and arrive at a diagnosis or prognosis. Other biological applications of SVMs involve classifying objects as diverse as protein and DNA sequences, micro-array expression profiles and mass spectra.The general term for astraight line in a high-dimensional space is a hyperplane, and so the separating hyperplaneis, essentially, the line that separates the all samples.define the notion of a separating hyperplane, consider a situation in which the microarray does not contain just two genes. The distance from the separating hyperplane to the nearest expression vector as the margin of the hyperplane, then the SVM selects the maximum margin separating hyperplane.

VII. CONCLUSION

In this paper, the importance of designing appropriate anomaly intrusion detection systems to identify the attack against cognitive radio networks is presented. Also, we use simpleyet effective IDS, which can be easily implemented in the secondary users in the network. Our proposed systemuses a fuzzy network profiling, which can produce an optimal solution. It can able to differentiate the attacker and normal user. Support vector machine is used to separate the users in efficient manner. it can consider all the parameter in cognitive radio network to find the attacker. It can automatically sense the range of the parameter using fuzzy methodology.

REFERENCES

[1] C. Cordeiro, K. Challapali, and D. Birru, "IEEE 802.22: An Introduction to the First Wireless Standard based on Cognitive Radios," *J. Commun.* vol. 1, no. 1, Apr. 2006, pp. 38–47.

[2] R.Nakkeeran et al[]., "A Survey of Routing Attacks in Mobile Ad Hoc Networks," *IEEE Wireless Commun.*, vol. 14, no. 5, Oct. 2007, pp. 85–91.

[3] C.L. Schuba, I.V. Krsul, M.G. Kuhn, E.H. Spafford, A. Sundaram, a nd D. Zamboni, "Analysis of a Denial of Service Attack on TCP," Proc. IEEE Symp. Security and Privacy,May 1997.

[4] O. Leon, R. Roman, and J. H. Serrano, "Towards A Cooperative Intrusion Detection System for Cognitive Radio Networks," *Proc. Wksp. Wireless Cooperative Network Security (WCNS'11)*, Valencia, Spain, May 2011.

[5] W. El-Hajj, H. Safa, and M. Guizani, "Survey of Security Issues in Cognitive Radio Networks," *J. Internet Technology (JIT)*, vol. 12, no. 2, Mar. 2011, pp. 181–98.

[6] K. Ju and K. Chung, "Jamming Attack Detection and Rate Adaptation Scheme for IEEE 802.11 Multi-hop Tactical Networks," *Int'l. J. Security and Its Applications*, vol. 6, no. 2, Apr. 2012, pp. 149–54.

[7] Robert Di Pietro, Gabriele Oligeri, "Jamming Mitigation in Cognitive Radio networks," *J. Comput. Netw., vol. 51, no. 10, pp. 2594–2615, Jul. 2011.*

[8] Z. M. Fadlullah *et al.*, "DTRAB: Combating Against Attacks on Encrypted Protocols Through Traffic-Feature Analysis," *IEEE/ACM Trans. Net.*, vol. 18, no. 4, Aug. 2010, pp. 1234–47.

[9] V. Jyothsna, V. V. Rama Prasad, "A Review of anomaly based intrusion detection system" International journal of computer application, vol-28, no-7,*Aug 2011.*

[10] MunaM.Taherjawhar and Monica Mehrotra "Anomaly Intrusion detection system using Hamming Network Approach," *vol. 1, no. 1, pp. 165–169, jan-jun 2010.*

[11] H. Wang, D. Zhang, and K. G. Shin, "Change-Point Monitoring for Detection of DoS Attacks," *IEEE Trans. Dependable and Secure Computing*, vol. 1, no. 4, Oct. 2004, pp. 193–208.

[12] Y. Hu, D. Johnson, and A. Perrig, "Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks," IEEE Workshop on Mobile Computing Systems and Applications 2002.

[13] A. Yamada, Y. Miyake, K. Takemori, A. Studer, and A. Perrig, "Intrusion detection for encrypted Web accesses," in *Proc. 21st Int. Conf. Adv. Inf. Netw. Appl. Workshops*, Niagara Falls, ON, Canada, May 2007, pp. 569–576.

[14] KaiguiBian and Jung-Min Park, *MAC-Layer Misbehaviors in Multi-hop Cognitive Radio Networks, 2006 US-Korea Conference on Science, Technology, and Entrepreneurship (UKC2006)*, August, 2006.

