ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st&22ndMarch, Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Identification of Malicious Node by Using Mamdani Method in CRN

P.Amala Grace, B.Padminidevi

PG Scholar, M.Kumarasamy College of Engineering, Karur, India.

Assistant Professor, M.Kumarasamy College of Engineering, Karur, India.

Abstract: A cognitive radio Network is an intelligent system that can be configured dynamically. This network automatically detects the available channels in the radio spectrum. According to that it changes the transmission parameters to allow concurrent communication in a given spectrum. But this cognitive network is sensitive to security threats. So, in order to overcome these issues we use intrusion detection system. Actually in the cognitive radio network the idle channels of the primary users are used by the secondary users. The attackers may be external users or secondary users act as a malicious users. To identify the abnormal behavior due to attacks, we propose non-parametric cumulative sum (cusum) as the change point detection algorithm. There are different types of attacks created by the malicious users in the different types of layers. Like other wireless communication systems, a jamming attack is one of the most difficult threats in CRNs. In order to detect the jamming attack, let us consider a simple observation made by a secondary user involving its PDR and SS. Using the non-parametric cusum algorithm suggests that the mean value of the random sequence should be negative during the normal conditions and becomes positive upon a change. This method detects the malicious users but it is not particularly described whether it is a attacker or not. So, we introduce an innovative approach called Fuzzy Decision making system to recognize the attackers exactly. Fuzzy logic is an approach to computing based on "degrees of truth" rather than the usual "true or false" logic on which the modern computer is based. This fuzzy method uses discrete values to distinguish the attackers. Due to the fuzzy decision making we discover accurate attackers.

General Terms

Cusum Algorithm.

Keywords: Fuzzy Logic(FL), cumulative sum(cusum) , Cognitive Radio Network (CRN), Packet Delivery Rate(PDR),Signal Strength(SS).

I.INTRODUCTION

Cognitive radio is an intelligent radio and its open spectrum sharing that can be programmed and configured dynamically. Its transceiver is designed to use the best wireless channel in its vicinity. Such a radio automatically detects available channels in wireless spectrum. CRN based on IEEE wireless Regional Area Network. Cognitive radio network can be divided into two types. Full cognitive Radio(Mitola radio), in which every possible parameter observable by a wireless node. Spectrum-Sensing Cognitive Radio is using only the radio-frequency spectrum. Cognitive radio (CR) is the enabling technology for supporting dynamic spectrum .The intrusion detection and response model, it is necessary to first introduce the general design of the CRN for a broad view and understanding of the architecture and other relevant components of the concept. The architecture of the CRN below shows the different components of functional and operational hardware, together with the relationship between them. The spectrum band is infinitely renewable, though limited due to high demand by secondary users. The primary user has the legitimate right to a certain spectrum band, whereas the secondary user does not have the license to operate in a choice band. The primary and unlicensed networks consist of some basic elements, which include primary users, primary base-stations, cognitive radio users, cognitive radio base-stations, cognitive radio network access, cognitive radio ad hoc access, and primary network access.

However, the primary user has the license (right) to operate in a specified spectrum band. This access right can only be controlled and monitored by its base-station, and unauthorized users are not allowed to interfere with, or affect, its operations. Consequently, the primary base-station is a fixed wireless infrastructure network component that has a spectrum license but no capability to share the spectrum with other users of cognitive radio. Therefore, the primary base-station may need to have

both the primary and cognitive radio protocols to enable primary network access for cognitive radio users. Moreover, spectrum access is allowed for cognitive radio users only when not occupied by the authorized users, because they do not operate with a spectrum license. Therefore, cognitive radio user capabilities such as spectrum sensing, spectrum decision, spectrum handoff and cognitive radio medium access control, and routing and transport protocols are required to enable communication with the base-station and other cognitive radio network users.

IDSs prepare for and deal with attacks by collecting information from a variety of system and network sources, then analyzing the symptoms of security problems IDSs serve three essential security functions; monitor, detect and respond to unauthorized activity IDS can also response automatically (in real-time) to a security breach event such as logging off a user, disabling a user account and launching of some scripts. There are three type of network approaches used in intrusion detection system are network based, host based and hybrid based network. NIDS uses a passive interface to capture network packets for analyzing. NIDS sensors placed around the globe can be configured to report back to a central site, enabling a small team of security experts to support a large enterprise. NIDS systems scale well for network protection because the number of actual workstations, servers, or user systems on the network is not critical the amount of traffic is what matters .Most network-based IDSs are OS-Independent. Intrusion detection becomes more difficult on modern switched networks. Current network-based monitoring approaches cannot efficiently handle high-speed networks. Most of Network-based systems are based on predefined attack signatures that will always be a step behind the latest underground exploits.

Host based network are works in switched network environments. It operates in encrypted environments and detects and collects the most relevant information in the quickest possible manner. The tracks behavior changes associated with misuse. It requires the use of the resources of a host server – disk space, RAM and CPU time. It does not protect entire infrastructure. Hybrid systems are difficult to manage and deploy. Although the two types of Intrusion Detection Systems differ significantly from each other, but they also complement each other. Such a system can target activity at any or all levels .It is easier to see patterns of attacks over time and across the network space .No proven industry standards with regards to interoperability of intrusion detection components. Hidden Markov Models are convenient and mathematically tractable tools, and useful to describe and analyze the dynamic behavior of complicated random phenomena. In general, a real world process that can or cannot be expressed as a random process produces a sequence of observable symbols or pattern. The symbols or patterns can be discrete or continuous depending on the process of specific applications. If then build a signal model that explains and characterizes the occurrence of the observed symbols or patterns, then it can use that model later to identify or recognize other sequences of observations by choosing most likely model close to obtained model. In an 802.22 network the HMM is a suitable learning technique for classification, detection and possibly channel prediction.A smart antenna is a digital wireless communications antenna system that takes advantage of diversity effect at the source (transmitter), the destination (receiver), or both. Diversity effect involves the transmission and/or reception of multiple Radio Frequency (RF) waves to increase data speed and reduce the error rate. Smart antennas can be classified into three major categories, SIMO (Single Input, Multiple Output) MISO (Multiple Input, Single Output), MIMO(Multiple Input, Multiple Output).There are two main types of smart antennas include switched beam smart antennas and adaptive adaptive array smart antennas.

The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity. Several methods of misuse detection, including a new pattern matching model.This types of approaches used in the cognitive radio network to be find the abnormal behavior of attacks.This type of attack for find the detection threshold attack of detection process. The function of Intrusion Detection System for finding the attacks in cognitive radio networks. It can use non-parametric cumulative sum (cusum) as the change point detection algorithm to discover the abnormal behavior due to attacks. Attacks may be different types of attacks like A “Lion” attack in the transport layer threats usually disrupt the transport control protocol (TCP). The link layer attacks comprise spectrum sensing data fiddling and a denial of service (DoS) attack by saturating the control channel of the CRN. On the other hand, the physical layer attacks against CRNs called jamming attack. Jamming attack is one of the main concern in the wireless communication. To effectively detect anomalies due to various types of attacks, the IDS needs to be designed in such a fashion that it may learn the normal behavior of protocol operation, traffic flow, primary user access time, packet delivery ratio (PDR), signal strength (SS), and so forth. In the non-parametric cumulative sum (Cusum) as the change point detection algorithm there are two phases: Learning phase, Detecting Phase. In the learning phase, specifically to detect the jamming attack, a simple observation made by a secondary user involving its PDR and SS. The PDR of a user indicates the ratio of the number of packets received by the user to that of the packets sent to him.While the SS measured at that secondary user remains high, his PDR usually drops. This happens because the secondary user never receives some/all of the packets sent to him. In the detection phase,an assumption of the non-parametric cusum algorithm suggests that the mean value of the random sequence should be negative during the normal conditions and becomes positive upon a change.

II CRN ARCHITECTURE

The intrusion detection and response model, it is necessary to first introduce the general design of the CRN for a broad view and understanding of the

architecture. Cognitive radio is dynamic and adaptive in nature. The architecture of the CRN below shows the different components of functional and operational hardware, together with the relationship between them. The spectrum band is infinitely renewable, though limited due to high demand by secondary users. The primary user has the legitimate right to a certain spectrum band, whereas the secondary user does not have the license to operate in a choice band. The primary and unlicensed networks consist of some basic elements, which include primary users, primary base-stations, cognitive radio users, cognitive radio base-stations, cognitive radio network access, cognitive radio ad hoc access, and primary network access.

However, the primary user has the license (right) to operate in a specified spectrum band. This access right can only be controlled and monitored by its base-station, and unauthorized users are not allowed to interfere with, or affect, its operations. Consequently, the primary base-station is a fixed wireless infrastructure network component that has a spectrum license but no capability to share the spectrum with other users of cognitive radio. Therefore, the primary base-station may need to have both the primary and cognitive radio protocols to enable primary network access for cognitive radio users. Moreover, spectrum access is allowed for cognitive radio users only when not occupied by the authorized users, because they do not operate with a spectrum license. Therefore, cognitive radio user capabilities such as spectrum sensing, spectrum decision, spectrum handoff and cognitive radio medium access control, and routing and transport protocols are required to enable communication with the base-station and other cognitive radio users. The cognitive radio base-station is a fixed wireless infrastructure component that has cognitive radio capabilities and provides single-hop connection to cognitive radio users without a license for spectrum access. The cognitive radio users communicate with each other either in a multi-hop manner or through a base-station. Consequently, the cognitive radio network architecture consists of three different types of network access, such as cognitive radio network access, cognitive radio ad hoc access, and primary network access with different implementation requirements. However, in cognitive radio network access, secondary users have the capability to access the cognitive radio base-station in both the licensed and unlicensed spectrum bands. In cognitive radio ad hoc access, cognitive radio users communicate with each other on both licensed and unlicensed spectrum bands via ad hoc connection.

In primary network access, when the primary network is dormant, the cognitive radio users are able to access the primary base station via the licensed band. A CR uses the seven ISO/OSI layers to enable communication to other CRs. In order to be dynamically reconfigurable, transmission parameters must be changeable via software commands. Consequently, A CR must be based on Software Defined Radio (SDR) technology. For being able to observe its environment, the CR moreover must be equipped with different kinds of sensors. First of all, there is a need for a spectrum sensing capability. This exceeds the requirements for the PHY and MAC layer in an SDR, in addition to the communications part also the reception of other signals including their analysis must be implemented. An exemplary architecture for this is depicted, derived from an architecture proposal by the Wireless Innovation Forum. Also the user's interactions must be observed and transformed into plans, harmonised with the options derived from the spectral occupation. This harmonization, which conjoins the user input with the spectrum sensing information under consideration of legal conditions, has to be executed in a central entity of the CR, the so-called Cognitive Manager.

Here all incoming information is collected, fused and evaluated. Plans are created, and in a decision process one of those plans is selected and returned to the radio part in form of new transmission parameters.These transmission parameters may have influence on each of the ISO/OSI layers, they must be addressable separately. Consequently, there must be an interface between the Cognitive Manager.The radio part to enable direct access to each layer. The cross layer architecture is achieved, as example information gathered by the PHY layer may result in changes in the networking layer. In order to consider legal conditions, the CR must be aware of where it is allowed to transmit and which frequencies are forbidden, example of due to their use by local security organizations. Such regulations have to be known to the cognitive manager in form of policies, most probably stored in a policy database. As those policies may differ between different locations, the CR must have knowledge about its current location. For this purpose a CR must be equipped with a geo location sensor, ex a GPS device. Gathered knowledge must be stored internally and recallable for any decision. On one hand this requires a storage possibility, like a knowledge database; On other hand the knowledge must be stored in a computer manageable form.

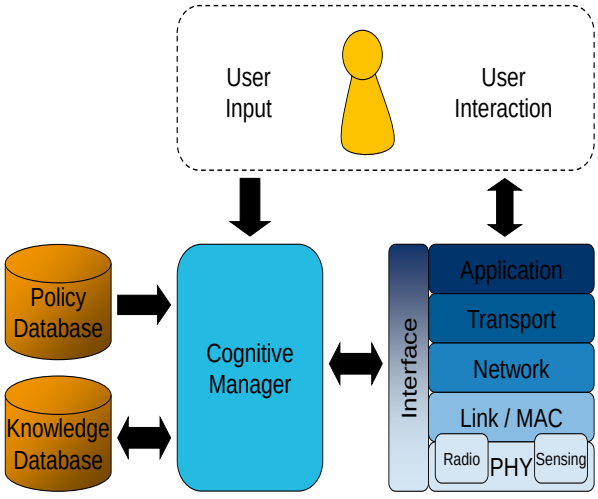


Figure: Cognitive Radio Architecture

III FUZZY LOGIC MODEL

Fuzzy Logic is a form of many valued logic. FL is a problem-solving control system methodology that lends

itself to implementation in systems ranging from simple, small, embedded micro-controllers to large, networked, multi-channel PC or workstation-based data acquisition and control systems.

It can be implemented in hardware, software, or a combination of both. Fuzzy Logic provides a simple way to arrive at a definite conclusion based upon vague, ambiguous, imprecise, noisy, or missing input information. Fuzzy Logic's approach to control problems mimics how a person would make decisions, only much faster. Compared to traditional binary sets fuzzy logic variables may have a true value that ranges in degree between 0 and 1.Fuzzy logic has been extended to handle the concept of partial truth, where the truth value may range between completely true and completely false. Furthermore, when linguistic variables are used, these degrees may be managed by specific functions.

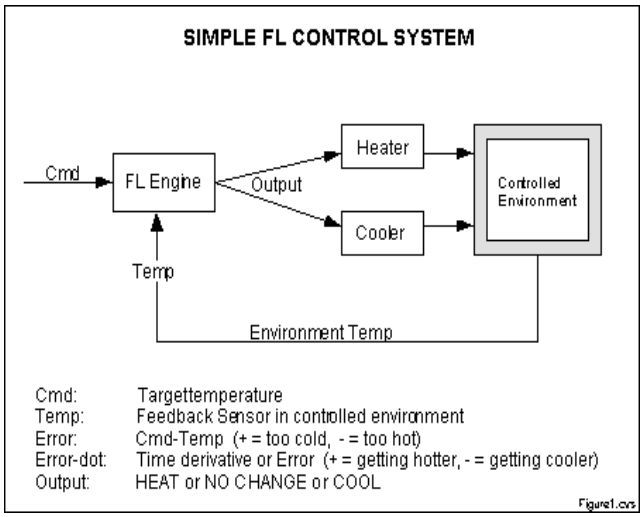


Figure:Fuzzy Logic Control System

Fuzzy logic presents an alternative way to represent linguistic and subjective attributes of the real world in computing. Specifically in the jamming attack, it provides input values as packet delivery ratio and signal strength of the secondary users. The linguistic variable called anomaly and their values are Attacker, Not Attacker, May be Attacker. Linguistic values are defined by using membership functions that depends on the range of values. Due to this differentiate the users and exactly identify the attackers. Fuzzy Logic provides a more efficient and resourceful way to solve the problems. In the fuzzy logic system consists of Fuzzifier, Interference Engine and Defuzzifier.

The Fuzzifier converts the crisp input to a linguistic variable using the membership functions stored in the fuzzy knowledge base. The interference engine converts the fuzzy input to the fuzzy output by using If-Then type fuzzy rules. The Defuzzifier converts the fuzzy output of the inference engine to crisp using membership functions analogous to the ones used by the Fuzzifier. In this method by taking the packet delivery ratio and the signal strength and using the fuzzy system it converts to linguistic variables. After that it can be differentiate the users by If-Then type fuzzy rules. At last it gives the outputs as easily identify the attackers. The advantages of fuzzy logic are detection sensitivity is more and exactly identify the attackers. The centroid method is very popular, in which the center of mass of the result provides the crisp value. Another advance is the altitude method, which take the rate of the main provider .The centroid system favors the regulation by the output of best area, even as the altitude method clearly favors the regulation by the best output rate.

The implementation algorithm and experimental steps:

a. Learning phase

In the learning phase, effectively detect the anomalies due to various types of attacks, the IDS needs to be designed in such a fashion that it may learn the normal behavior of protocol operation, traffic flow, primary user access time, packet delivery ratio (PDR), signal strength (SS), and so forth. The IDS may learn this information by constructing a statistical profile during normal CRN conditions. The PDR of a user indicates the ratio of the number of packets received by the user. The acquired information can facilitate the detection phase of the IDS to discover unknown intrusions or attacks against the targeted CRN.

b. Detection phase

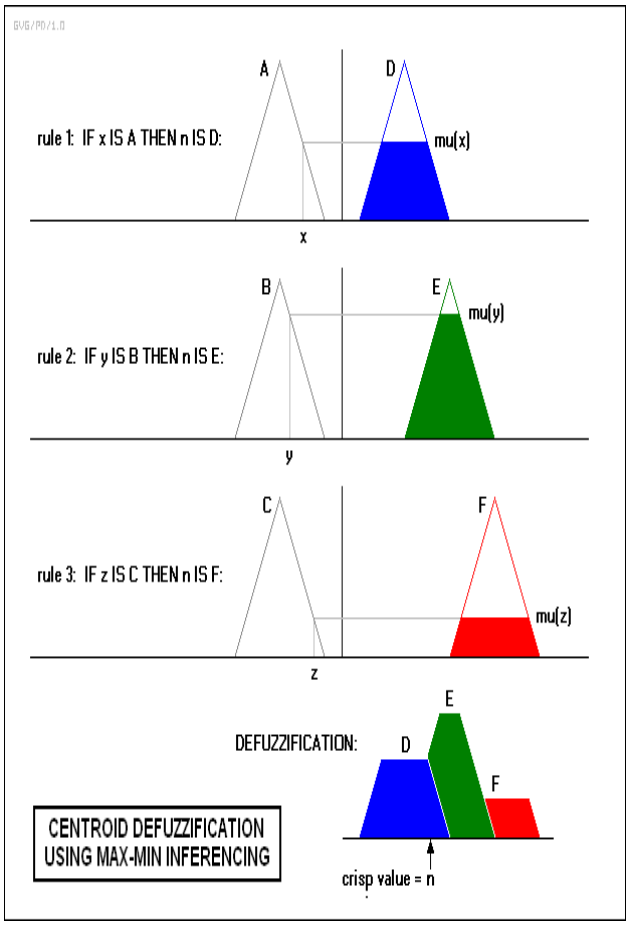
In the detection phase, in order to detect the malicious event the following observations is made. Suppose a malicious user jams a secondary user's connection the SS measured at that secondary user remains high, and the PDR usually drops. Because the secondary user never receives the packets. The intrusion detection system finds the PDR of the secondary user is dropping significantly. The IDS with cusum-based anomaly detection is to solve this problem.

c. Fuzzy Sets

The input variables in a fuzzy control system are in general mapped by sets of membership functions similar to this, known as fuzzy sets. The process of converting a crisp input value to a fuzzy value is called fuzzification. A control system may also have various types of switch, or ON-OFF, analog inputs, and such switch inputs of course resolve forever include a truth value equal to either 1 or 0, however the method preserve transaction by them because simplify fuzzy function to occur towards exist also one value or another. fuzzy logic is the form of appropriate to low-cost implementations based on low-cost sensors, low-decision analog-to-digital converters, and 4-bit or 8-bit one-chip microcontroller chip.

d.Fuzzy logic- Mamdani model

In order to detect the attackers exactly, we use this model. In this method, Mamdani-type uses the technique of defuzzification of a fuzzy output. Here, the two inputs and three outputs are taken. The inputs are packet delivery ratio and signal strength. The outputs are defined as attacker, not attacker and may be attacker. After, that creates the custom membership functions. Membership functions define how each point in the input space is mapped to a membership value between 0 and 1. After, that creates the rule editor that describes the logical relationship between the inputs and the outputs. In addition to that create custom inference functions. It denotes the include AND, OR, implication, aggregation and defuzzification methods. This action generates the output values for the fuzzy system.



IV CONCLUSION

The Cognitive Radio Network is an opportunistic communication technology designed to utilize the maximum available licensed bandwidth for unlicensed users. This radio spectrum sharing policy among the licensed and unlicensed users, however, opens up the possibility of various security threats. So, to overcome this problem we use various security frameworks. The suggestions can be mainly categorized into: cryptography based, reputation based, and trust based. But these methods are less efficient to achieve security. So, we propose a method called non-parametric cumulative sum (Cusum) as the change point detection algorithm to discover the abnormal behavior due to attacks. By learning the normal mode of operations and system parameters of a CRN, the proposed IDS is able to detect suspicious (i.e. anomalous or abnormal) behavior arising from an attack. In order to increase the detection sensitivity we establish a new technique called fuzzy decision making system.. In this method, the Detection Sensitivity is more and exactly identifies the attackers. An Unsupervised Network Intrusion Detection System capable of detecting unknown network attacks without using any kind of signatures, labeled traffic, or training. UNIDS uses a novel unsupervised outliers detection approach based on Sub-Space Clustering and Multiple Evidence Accumulation techniques to pin-point different kinds of network intrusions and attacks such as DoS/DDoS, probing attacks, propagation of worms, buffer overflows, illegal access to network resources, etc. This can be done in future work.

REFERENCES

[1] Zubair Md. Fadlullah, Hiroki Nishiyama, and Nei Kato, Tohoku University Mostafa M. Fouda, Tohoku University and Benha University," Intrusion Detection for Combating Attacks AgainstCognitive Radio Networks Network, IEEE vol.27, May-June 2013.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] B. Kannh vong et al., "A Survey of Routing Attacks in Mobile Ad HocNetworks," IEEE Wireless Commun., vol. 14, no. 5, Oct. 2007, pp.85–91.

[7] S. Kurosawa et al., "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," Int'l. J. Network Security, vol. 5, no. 3, Nov. 2007, pp. 338–46.

[8] O. Leon, J. Hernandez-Serrano, and M. Soriano, "Securing Cognitive Radio Networks," Int'l. J. Commun. Systems, vol. 23, no. 5, May.2010, pp. 633–52.

[9] 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.

[10] 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.

[11] MATLAB,available online at http://www.mathworks.com.