International Journal of Academic Research and Development
ISSN: 2455-4197
Impact Factor: RJIF 5.22
www.academicsjournal.com
Volume 2; Issue 6; November 2017; Page No. 1128-1131

Cognitive radio network security with slow intelligence system

Dr. TS Baskaran
Associate Professor, Department of Computer Science, A.V.V.M. Sri Pushpam College, Poondi, Tamil Nadu, India

Abstract

Now a day's attack on cognitive radio network is common. Insider violence on malicious type of attack is frequently happening one, As Cognitive radio(CR) network is one among the dominant wireless network, solving the above mentioned problem is extremely essential. A new method with an introduction of SIS (Slow Intelligence System) along with fast probe algorithm is proposed to resolve the above issue effectively.

Keywords: radio network, cognitive radio (CR), SIS

1. Introduction

With the fast growth of wireless communication, the last decade has seen an wide demand for wireless radio spectrum. Cognitive (or smart) radio networks are an innovative approach to wireless engineering in which radios are designed with an unprecedented level of intelligence and agility. This advanced technology enables radio devices to use spectrum (i.e., radio frequencies) in entirely new and sophisticated ways [1]. Cognitive radios have the ability to monitor, sense, and detect the conditions of their operating environment. It dynamically reconfigures their own characteristics cognitive radios can identify potential impairments to communications quality, like interference, path loss, shadowing and multipath fading. They can then adjust their transmitting parameters, such as power output, frequency, and modulation to ensure an optimized communications, the use of cognitive radio (CR) technology has led the FCC (Federal Communications Commission) to consider more flexibility in the usage of available spectrum. Partial utilization of the allocated spectrum (inefficient utilization of spectrum) necessitates development of dynamic spectrum access techniques (DSA). The DSA allows users called secondary users (SUs), with no spectrum license, to temporally use the unused licensed spectrum. The priority users have priority in using the spectrum; SUs need to constantly perform real time monitoring of the licensed spectrum which can be used. In doing so the SU should not violate the interference temperature. The SUs should be aware of the PUs reappearance. The technique used for sensing the PUs presence is called spectrum sensing [1]. There are various sensing techniques available such as energy detection, cyclostationary feature detection, matched filter, central cooperative sensing and distributive cooperative sensing. In spectrum sensing the SU constantly senses/checks the transmission channel for the presence of the primary signals in the channel. After sensing the spectrum the CRs allocate the spectrum to the SUs and the SUs need to reconfigure themselves in order to use the newly allocated spectrum.

Cognitive radio is a technique where secondary user looks for a free band to use when primary user not in use of its approved group. It is possible through spectrum sensing. The unoccupied frequency bands are called white space or spectrum holes. Cognitive network is sensitive to security threats. The attackers may be external users or secondary users act as a malicious users. So, in order to overcome CRs security issues, malicious user detection system is used.

Various security problems can occur in a cognitive radio environment [2]. Such as,

- False detection or sensing and misdetection of primary signal May happen due to denial of service or malicious user pretends as the primary signal.
- A malicious user could prevent the cognitive user from using available spectrum.
- A malicious user could access the data in an unauthorized way or modify/inject the false data.
- Environment could be controlled by a malicious user.

CR technology can help in many ways to enhance public safety services include:

- Avoiding spectrum congestion.
- Precedence service to higher priority users temporarily during the peak communications period of an emergency.
- Dynamic spectrum access to improve spectrum efficiency.
- Achieving interoperability among legacy and new devices and systems.

Aim of attack

- Interruption – Interruption is an attack on availability such as a denial of service attack (or DOS). An interruption attacks' aim is to make resources unavailable. Not too long ago, WordPress.com, a popular Blog Hosting Site was faced with a DOS attack taking down the servers so the service was unavailable to its users
- Interception – Interception is an attack to gain unauthorized access to a system. It can be simple eavesdropping on communication such as packet sniffing or just copying of information
- Modification – Modification is an attack that tampers with

a resource. Its aim is to modify information that is being communicated with two or more parties. An example of a modification attack could be sending information that was meant to go to one party but directing it to another.

- Fabrication – A Fabrication attack is also known as counterfeiting. It bypasses authenticity checks, and essential is mimicking or impersonating information. This sort of attack usually inserts new information, or records extra information on a file. It is mainly used to gain access to data or a service.

Security issues of CRN

Table 1: Types of attack on CRN

Attack types	Description
Denial of Service (DoS)	Puts the burden on the resources & to stop the utilization of the resources.
Replay Attack	Capture the packets and resend these packets maliciously
Rogue Base Station Attack	Attacker abuses this information and sends bogus messages.
Incumbent Emulation (IE) Attacks	Actual incumbent signals during the sensing period.

Table 2: Motivation of attack on CRN

Attack types	Description
▪ Selfish Attack	It is access the spectrum the spectrum with high priority.
▪ Malicious attack	Enemy slows down the unlicensed user from spectrum usage and caused DoS
▪ Misbehaving	CR didn’t follow any general rule for sensing and managing of range of the spectrum.
▪ Cheat Attack	The attacker increases his value function as well as at the same time decrease contestant’s profit.

2. Related Work

Malicious attack and Its Description

In general malicious attacks are divided into four different types on show in fig, among it insider attack is the most dominant one.

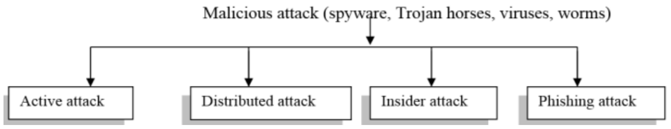

Fig 1: Malicious attack type

An insider attack

It is most difficult to detect and prevent. Because it is caused by someone from the inside (disloyal employee) attacking the network [3]. Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task.

Managing the attacks

Network security affects many organizations, whether they are large, small, or government organizations. If network security is breached an intruder can do all sorts of harm. That is why people need to be aware of and to be educated about network security Systems are required to be modernized regularly as new security flaws are discovered [4]. Without being up to date, it makes it easy for a *hacker* to gain illegal access to the organization.

Security Management

The OSI Security Architecture defines three main areas of security management. These activities are to be preformed System Administrators [5, 6].

- System security management – The management the entire computing environment focusing on the security aspects
- Security service management – The management of particular security services
- Security mechanism management – The management of particular security mechanisms

3. Proposed Approach

3.1 Research Design

Steps of the proposed method are given in fig 2

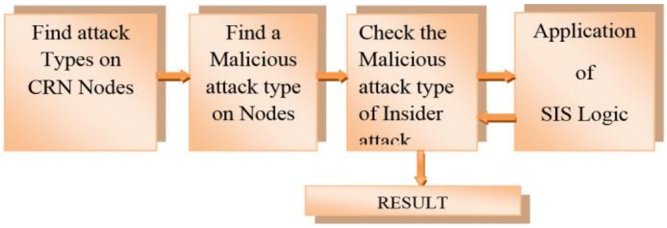
Find attack Types on CRN Nodes
Find a Malicious attack type on Nodes
Check the Malicious attack type of Insider attack
Application of SIS Logic
RESULT

Fig 2: proposed approach design steps

- In the proposed approach initially check whether the CRN has attack if yes its type is detected.
- Identifies detect malicious attack exists or not.
- Extracts the insider attack from the malicious type.
- Finally SIS logic is applied to resolve the problem of Insider’s malicious attack.

3.2 Slow intelligence system

Slow Intelligence Systems (SIS) is a general purpose systems characterized by being able to improve performance over time through a process involving enumeration, propagation, adaptation, elimination and concentration.

A SIS constantly learns, search for new solutions and propagates and shares its familiarity with other peers. A Slow Intelligence System differs from expert systems in it knowledge is not always obvious.

A Slow Intelligence System seems to be a slow learner because it analyzes the environmental changes carefully and gradually before absorbs it into its knowledge base while maintaining synergy with the environment [7].

In general Slow Intelligence System typically exhibits the following characteristics:

Enumeration: different solutions are enumerated, until the appropriate solution or solutions are found.

Propagation: The system is aware of its environment and constantly exchanges information with the environment. Through this constant information exchange, one SIS may propagate information and/or knowledge to other (logically or physically adjacent) SISs.

Adaptation: Solutions are enumerated and adapted to the environment. Sometimes adapted solutions are mutations that transcend enumerated solutions of the past.

Elimination: Unsuitable solutions are eliminated, so that only suitable solutions are further considered.

Concentration: Among the suitable solutions left, resources are further concentrated to only one (or at most a few) of the suitable solutions.

Beside the above mentioned characteristics SIS has one more unique property. SIS possesses at least two decision cycles. The first one, defined as the *quick decision cycle*, provides an instantaneous response to the environment.

The second one, defined as the *slow decision cycle*, tries to follow the gradual changes in the environment and analyze the information acquired by experts and past experiences.

The two decision cycles enable the SIS to both cope with the environment and meet long-term goals. Sophisticated SIS may possess multiple slow decision cycles and multiple quick decision cycles [8, 9].

Most importantly, actions of slow decision cycle(s) may override actions of quick decision cycle(s), resulting in poorer performance in the short run but better performance in the long run. In general a SIS acts according to five main phases, reflecting its five characteristics: Structure and general flow sequence of SIS is given in fig 3.

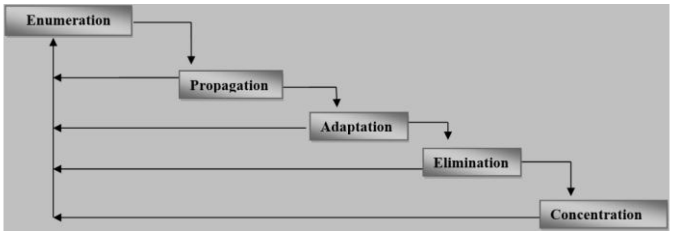

Fig 3: Structure of Slow Intelligence System

3.3 Flow diagram of proposed approach

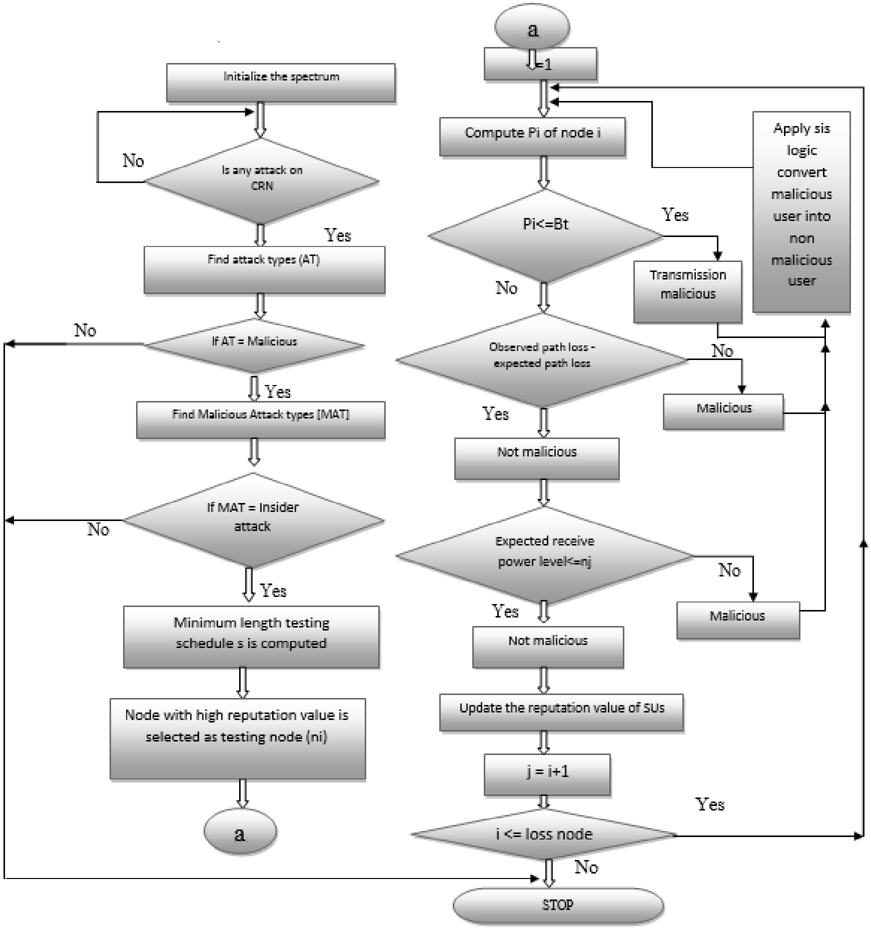
Initialize the spectrum
Is any attack on CRN
No
Yes
Find attack types (AT)
If AT = Malicious
No
Yes
Find Malicious Attack types [MAT]
If MAT = Insider attack
No
Yes
Minimum length testing schedule s is computed
Node with high reputation value is selected as testing node (ni)
a
a
i=1
Compute Pi of node i
Pi<=Bt
Yes
No
Transmission malicious
Apply sis logic convert malicious user into non malicious user
Observed path loss - expected path loss
No
Yes
Malicious
Not malicious
Expected receive power level<=nj
No
Yes
Malicious
Not malicious
Update the reputation value of SUs
j = i+1
Yes
i <= loss node
No
STOP

Fig 4: flow diagram

Flow sequence of the proposed work is given in fig 4

3.4 Algorithm

Step by step procedure of the proposed approach is given below.

- **Step 1:** Initialize the spectrum. [First initialize the spectrum for Cognitive Radio Networks. It is important to analyze the spectrum environment in which cognitive radio will operate.]
- **Step 2:** Test is it any attack on CRN. If 'NO' test again
- **Step 3:** If attack exists, find the attack types (AT)
- **Step 4:** Check the condition if AT=Malicious. The 'yes' go to next step. Otherwise stop the process.
- **Step 5:** find malicious attack types [MAT].
- **Step 6:** If MAT is not equal to Insider attacks stop the process.
- **Step 7:** Compute s (minimum length testing schedule).
- **Step 8:** Identify testing node nj (node with high reputation value).
- **Step 9:** Compute probability (p) of node i.
- **Step 10**: If Pi (probability of node i) is less than or equal to Bt (set of testing node)
- **Step 11:** test is expected path loss equal to observed path loss continues else correct the malicious attack with SIS logic.
- **Step 12:** Test is the node is malicious with Received power level. If power level is less than or equal to ni continue else invoke SIS logic.
- **Step13:** Update the reputation value.
- **Step14:** Go to step9 to perform the operation on in different node.
- **Step15:** If i value is less than or equal to loss then invoke SIS logic else STOP.

4. Conclusion

With the introduction of (SIS) fast probe algorithm's efficiency is drastically enhanced without any compromise. CRN's malicious attacks, Insider type is effectively managed with the help of Slow Intelligence System and also conclude that SIS logic can be applied in future to handle all the kinds of attack on CRN.

5. References

1. Chen K-C, Peng Y-J, Neeli Prasad, Liang Y-C, Sumei Sun. Cognitive radio network architecture: part I--general structure. In Proceedings of the 2nd international conference on Ubiquitous information management and communication, ACM, 2008, 114-119.
2. Clancy Charles T, Nathan Goergen. Security in cognitive radio networks: Threats and mitigation. In 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (Crown Com 2008). IEEE, 2008, 1-8.
3. Fragkiadakis, Alexandros G, Elias Tragos Z, Ioannis Askoxylakis G. A survey on security threats and detection techniques in cognitive radio networks. IEEE Communications Surveys & Tutorials. 2013; 15(1):428-445.
4. Bhattacharjee, Shameek, Shamik Sengupta, Mainak Chatterjee. Vulnerabilities in cognitive radio networks: A survey. Computer Communications. 2013; 36(13):1387-1398.
5. Shazly, Hagar O, Asmaa Saafan, Hesham El Badawy, Hadia El Hennawy M. Performance of Analysis Cognitive Radio with Cooperative Sensing under Malicious Attacks over Nakagami Faded Channels. Wireless Engineering and Technology. 2016; 7(02):67.
6. Bhattacharjee, Suchismita, Raiping Keitangnao, Ningrinla Marchang. Association rule mining for detection of colluding SSDF attack in Cognitive Radio Networks. In 2016 International Conference on Computer Communication and Informatics (ICCCI). IEEE, 2016, 1-6.
7. Baskaran TS, Sivakumar R. Slow Intelligence System Framework to Network Management Problems for Attaining Feasible Solution. International Journal of Engineering and Technology (IJET). 2013; 5(1):398-402.
8. Baskaran TS, Sivakumar R. Slow Intelligence Based Learner Centric Information Discovery System.
9. Baskaran TS, Sivakumar R. Slow Intelligence System Framework to Network Management Problems for Attaining Feasible Solution.