I J C T A, 9(41), 2016, pp. 443-453 ISSN: 0974-5572

Comparative Study of Security Threats in Cognitive Radio Networks

Rohini Lohia*, Isha* and Arun Malik*

ABSTRACT

Wireless Sensor Networks (WSN) are considered to be posterity of the posterity of networks that will form the intrinsic part of human life. Electromagnetic spectrum is a meagre resource. As the urgency of wireless communication applications is expanding the electromagnetic spectrum band is becoming congested or jam-packed. If we throw light on fixed spectrum there are many frequencies which are not accurately exploited. Here comes the cognitive radio (CR) with a purpose to exercise unused frequency bands which in technical terms is known as" White Spaces". Spectrum Sensing is paramount function of CR. There are many security concerns that are associated with this functionality of CR. Cognitive radio wireless sensor networks (CRWSN) can be compromised by fracturing the dynamic spectrum access (DSA) policy. Most of the security threats arise from the malicious nodes. In simple words, as there are many CR nodes but out them many are malicious nodes. They are the main cause of most of the security threats in CRWSN. Cardinal objective of this paper is to lay emphasis on security issues associated with CRWSN. Primary User Emulation (PUE) Attack and Spectrum Sensing Data Falsification (SSDF) Attack are the two precarious attacks in CR. This paper elucidates the difference between PUE attack and SSDF attack and also gives a detailed explanation of SSDF -attack parameters, how parameters are related to produce different attack models.

Keywords: Cognitive radio (CR), Security issues, Primary User Emulation (PUE) attack and Spectrum Sensing Data Falsification (SSDF) attack.

1. INTRODUCTION

WSN is considered as most fascinated area for research in wireless and mobile computing. WSN are considered to be the posterity of networks that will form the intrinsic part of human life (1). WSN is a fusion of multiple miniature devices called as sensor nodes having the proficiency to sense the environment, performs finite computing and commune in a wireless manner to build WSN. The main function of these sensor nodes is to process, store and sense. Applications of WSN include healthcare, biometrics, automotives, construction and other building industries. The primary difference between wired and the wireless network lies in their decentralized and specialized nature. The paramount purpose of this paper is to lay emphasis on one of the most leading topic in WSN-CR. Here the spotlight is on what CR is and how it is used.

Electromagnetic Spectrum is meagre resource. At present wireless communication has emerged as the most commercial/admired communication. As the urgency of wireless communication applications is expanding the electromagnetic spectrum band is becoming congested or jam-packed (2). If we throw light on fixed spectrum there are many frequencies which are not accurately exploited. Here comes the CR with a purpose to exercise unused frequency bands which in technical terms is known as "White Spaces". Thus the concept of CR is an exclusive approach to boost the employment of radio electromagnetic spectrum. Before going to more details it is important to know that basically there exist two kinds of users. Primary users- these are defined as those users that have liberty to access distinct channels that are issued to them

* Department of Computer Science and Engineering, Lovely Professional University Jalandhar, Punjab, INDIA, *Emails: rohinilohia@yahoo.in, isha.17451@lpu.co.in, arun.17442@lpu.co.in*

(3). Secondary users are those users that are granted to exercise the vacant spectrum of licensed users, simply primary users. These users are having the inferior seniority and thus utilize the spectrum in a manner that it does not purpose interference among the licensed users.

Authors in (4) describes three primary features of CR includes: - intelligent adaptive behaviour, self awareness and reconfigurability. These are the three primary features of utilization and allocation of static spectrum that leads to a spectrum access which in dynamic in nature. To summarize, CR is defined as the radio frequency transmitter/receiver that can wisely sense the surrounding environment and as a result can expose/recognize whether an appropriate segment of the radio spectrum is presently in user. If the unlicensed user feels the existence of licensed user then unlicensed user should immediately switch to temporarily unused spectrum without interference with the primary users. The four important functions performed by CR users' are- Spectrum Management, Spectrum Sharing, Spectrum Mobility and Spectrum Sensing. This paper mainly focuses on spectrum sensing. Table 1. illustrates essential terms of CR. Spectrum holes are those licensed band which can be utilized by cognitive users without causing interference to the primary or secondary users. Basically spectrum holes can be categorised as, spatial and temporal spectrum holes.

Table 1
Essential terms of CR

Terms	*Description*	
White Spaces	White spaces are those spaces that are relieved of interferers, besides noise caused reasoned by natural or artificial sources.	
Gray Spaces	Gray spaces are those spaces that are moderately occupied by interferes and noise.	
Black Spaces	Black spaces are those spaces whose entire volume is due to the existence of communication, noise and interfering signals	
Spectrum Holes	Temporal Spectrum Holes	In case of temporal spectrum holes, at the time of sensing no primary transmission should take place over the spectrum band of interest. And due to this fact cognitive users have the liberty to use this band within current time slot.
	Spatial Spectrum Holes	Spatial spectrum holes are kept engaged by the primary transmissions but only in a defined or restrained area. Thus cognitive users can exercise the particular band outside the restrained area.

Security issues are one of the most important concerns while discussing about CR's. Typical security objectives of CRWSN are availability, confidentiality, access control and integrity. CR wireless network can be compromised by fracturing the DSA policy. Most of the security threats arise from the malicious nodes. In simple words, as there are many CR nodes but out them many are malicious nodes. They are the main cause of most of the security threats in CRWSN. Here we will discuss about all the security threats in CRWSN. Also prevalent attacks in CR are elaborated. Magnificent difference between PUE attack and SSDF attack is shown. Detailed explanation of SSDF attack-attack parameters; how parameters are related to produce different attack models are also elaborated.

2. SPECTRUM SENSING TECHNIQUES

Spectrum Sensing is one of the dominant functions performed by CR. To perform this function, there are many spectrum sensing techniques whose primary function is to identify weak primary user signals. In other words these techniques aim to expose the spectrum holes in a particular spectrum band. Spectrum sensing techniques, are categorised as Cooperative Spectrum Sensing, Non-Cooperative Spectrum Sensing, Interference Based Detection and MIMO based Spectrum Sensing Technique. This paper only covers detail about the Co-operative Spectrum Sensing Technique.

2.1. Cooperative Spectrum Sensing

While discussing about CR, cooperative sensing technique can be defined s a technique in which multiple cognitive users basically share the information which they have sensed. And thus it proffers an idea of spectrum employment in the particular area where CR's are lodged.

Cooperative Sensing Techniques covers the limitations of the non cooperative sensing technique. It is also considered as dominant technique to ignore interference to the licensed users. According to authors in (5) cooperative sensing is a three step technique. Figure 1. shows the working of cooperative spectrum sensing as a three step technique. At last, the final judgement is given by the common receiver regarding the absence or presence of licensed user. Advantages of cooperative sensing techniques includes false alarms also reduced the hidden node problem.

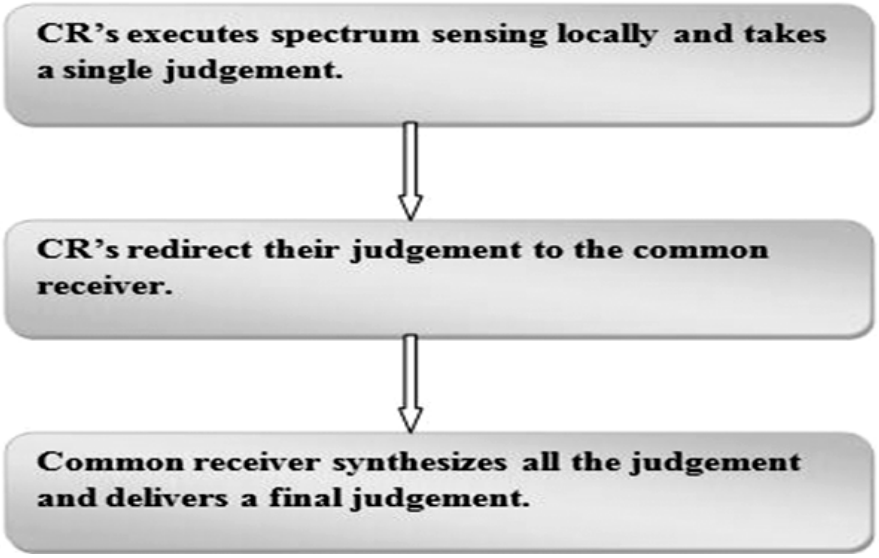


Figure 1: Working of cooperative spectrum sensing as three step technique.

Two approaches for the cooperative spectrum sensing are listed and elaborated below:

- Centralized Approach
- Decentralized Approach

Centralized Approach: Theme of centralized co-operative spectrum sensing is to boost the performance of sensing by making best use of spatial diversity. As the name indicates centralized co-operative spectrum sensing, all the nodes first individually sense the spectrum and afterwards forwards their individual sensing reports to the central head or monitor called "THE FUSION CENTRE". Fusion centre performs the three step procedure in cooperative spectrum sensing. In (6) it has been elucidated that, three step procedure performed by the fusion centre in cooperative spectrum sensing is described as follows:

- Fusion centre chooses the frequency band or channel of interest with the aim to perform spectrum sensing and instructs all the other CR's to sense the spectrum by performing local sensing.
- After performing local sensing, all CR users direct their sensing report to the fusion centre via control channel.
- When all sensing reports reaches the fusion centre, it integrates all the reports or results and decides on the existence of licensed user, and finally reports the judgement back to all CR's.

Distributed Approach:- As the name indicates "distributed", there is no monitor or controller node. Each and every node performs its own sensing function. Basically here in this particular approach, discrete nodes communicate with each other and share the information which they have sensed.

2.2. Fusion Techniques

There are seven elementary elements, Co-operation Models, Control channel and Reporting, Sensing Techniques, Data Fusion, User Selection, Hypothesis Testing and Knowledge Base. This paper accentuate mainly on fusion techniques that are related to "data fusion" which is one of the element of co-operative spectrum sensing. Data Fusion is cardinal process of spectrum sensing. According to the bandwidth of the control channel, all the channels report transmits their sensing report to the fusion centre for hypothesis testing, and finally making judgement on the absence or existence of licensed user. This process of integrating the sensing reports and arriving at the common decision is known as Data fusion. These sensing reports are of different sizes, types and forms.

Fusion Techniques are exercised by the fusion centre. From the above discussion we come to know that, in case of centralized co-operative spectrum sensing each and every individual CR user transmits its sensing reports to the fusion centre. Afterwards, these sensing reports are integrated at the fusion centre. Fusion centre in turn implements fusion techniques by exercising fusion rules on collected sensing reports with an aim to arrive at the perfect decision regarding absence or existence of primary users. Two parameters that are analogous to the data fusion process are: Probability of detection and Probability of false alarm. Probability of detection indicates that how effectively interference with the primary users can be circumvented. Probability of detection is directly proportional to performance of the data fusion. That is, if probability of detection is high then extortionate extent of security of primary signal is achieved (7). Probability of false alarm indicates that, the sensor will detect the primary signal when it is actually absent. Probability of false alarm is inversely proportional to the performance of data fusion. That is, if probability of false alarm is low then the channel is said to be available and it is utilized in an efficient way. Now coming to the fusion techniques, these techniques are of two types (8): Data Fusion and Decision Fusion No doubt these two techniques are utilizing spectrum sensing reports and generates the decision about the absence or existence of primary user signals, but these two techniques differ in the context of information, that they take into consideration. Key difference between these two techniques based on the type of information that is transmitted to the fusion centre.

In case of data fusion, all the CR users transmit their crude sensed information about the spectrum, such as traffic patterns, location, statistical information etc. This is also known as Soft Combination. Whereas in case of decision fusion, every individual CR user transmits its sensing report containing their individual decision about the absence or existence of licensed user. It is also known as hard Combination.

Authors in (9) depicts that decision or sensing reports that is transmitted to the fusion centre is a one bit report. Thirdly, when this one bit decision is submitted to the fusion centre, fusion centre applies any of the three rules, i.e., "AND rule", "OR rule" and "VOTING rule". This one bit decision is a binary in nature. As it is binary in nature, 1 means signal exists and 0 means it doesn't. Table 2. illustrates the rules exercised by fusion centre.

Table 2
Illustration of rules exercised by fusion centre

Rules	*Description*
AND Rule	According to this rule, primary signal is said to be present if each and every CR user has detected a signal, i.e., if each CR user transmit 1 at the fusion centre.
OR-Rule	According to this rule, primary signal is said to be present if single user has detected a signal, i.e., if a single CR user transmits 1 at the fusion centre.
VOTING Rule	According to this rule, primary signal is said to be present if majority of CR users votes that primary user singal is present.

3. SECURITY ISSUES IN CRWSN

Further when the concept of CR came into existence, new security issues came into view. These security issues are related to every aspect of cognitive cycle. CR users exhibit the property of DSA. CRWSN can be compromised by fracturing the DSA policy. DSA policy can be fractured by exercising misuse of spectrum or by behaving selfishly (10). Most of the security threats arise from the malicious nodes. In simple words, as there are many CR nodes but out them many are malicious nodes. They are the main cause of most of the security threats in CRWSN.

Typical security objectives of CRWSN are (11): Confidentiality where unauthorised users don't have the rights to access the network, Integrity which means that data is sent as detected to the recipient. Availability means that the network services should be available when needed and last but not the least Access Control means that only authorized users are restricted to access the resources. In simple words, access control provides access to only restricted users.

3.1. Prevalent Attacks in CRWSN

3.1.1. Attacks on Communication Protocols

As the name indicates communication attacks, in this type of attack attacker tries to destroy the communication between two or more parties. Some of the attacks that come under this category has the highest probability to attack on the communication protocol are: Repay attack and Denial of Service Attack.

In Replay Attack-as the name indicates "replay", in this messages are being replayed by the wicked attacker. Wicked attacker replays the messages from previous conferences. Also this attacker forwards messages to the wrong recipient. Considering this type of attack in CR, if a licensed user replays the packets, then the unlicensed user sometimes makes an erroneous analysis and thus fusion centre makes an incorrect decision.

In Denial of Service (DoS) Attack- services are not available to legitimate users. DoS attacks may be launched in many different ways, i.e., routing disruption attack, jamming attack, flooding attack, collision attack. DoS attacks can be classified as (10): disruption attack, jamming attack, flooding attack and collision attack. Table 3. given below shows the description of various types of attacks under DoS.

Table 3
Description of various types of attacks under DoS

Attack	Description
Jamming Attack	In this type of attack, interference of radio signals with the radio frequencies exists. These radio signals are transmitted by the wicked attacker and radio frequencies are being utilized by the nodes of the network.
Collision Attack	This particular attack, violation of communication protocols takes place.
Disruption Attack	This particular attack, routing messages are not forwarded by wicked attacker. Black hole and grey hole attacks are the examples of such type of attack.
Flooding Attack	In this type of attack, malicious node transmits fraud requests to the target node, as a result of which resources get wasted. Sybil attack comes under this type of attack because in this type of attack, only that particular node will generate the attack which assumes multifarious identities. Basically this type of attack is used to add reputations of malicious nodes.

3.1.2. Masquerading Attack

As the name indicates, in this type of attack an attacker will to masquerade an entity, with the aim to generate malicious results about spectrum sensing. So the entity that an attacker will try to masquerade is licensed or primary user. In simple terms, an attacker will try to mimic the behaviour of primary user because of which unlicensed or cognitive users will get a false idea about the particular spectrum band and

will finally vacate the band. This is just one of the cases of masquerading attack. The other case is of malicious secondary node. In this particular case, an attacker will mimic the behaviour of truthful CR node and hence will destroy the co-operative judgement framing process of all the CR nodes. Finally, resulting in malicious result about the availability of spectrum.

3.1.3. Power Exhaustion attacks on sensor Nodes

As the name indicates "power", indicates that here an attacker will attack on the power of CR sensor node. In simple terms, an attacker will launch multifarious attacks such as sleep deprivation attack etc., or will try to engage CR nodes in useless tasks thus depleting the battery of CR users. As a result of which they are not able to function properly.

3.1.4. Attacks on Cryptographic Protocols and Security Mechanisms

In this type of attacks, wicked attacker will compromise with cryptographic protocols. Main purpose of these types of attacks is to extract or destroy the keys used in hash function calculation; encryption decryption .These attack will try to break the security mechanisms that are being applied for security and privacy purposes. Differential Power Analysis attack is one such example, in which wicked attacker calculates the power of electromagnetic signals that are being emitted out from a victim node with the aim to recognize the encryption and decryption keys and hence breaking the security mechanisms.

3.1.5. Jamming Attack

This is one of the most common attacks in CR. Authors in (10) delineates that there are two types of jamming attacks in CR. Single channel and multi channel jamming attacks are two types of attacks. In case of single channel jamming attack, wicked attacker is responsible for broadcasting high power signals and these signals produces outrageous interference in the communication proceeding between the parties. As the name indicates "single channel", these signals are broadcasted in the single channel only. Whereas in case of multi channel jamming attack wicked attacker plans a policy, distracts the CR nodes from working in their own channel and allows it to move to multifarious channels and jam the channels. Thus the co-operative working of CR nodes is destroyed.

3.1.6. Hidden Node Problem

There are many security issues that arise from this hidden node problem. This is the problem that came into existence when CR node is not able to judge the existence of primary or licensed user and thus similar frequency bands are broadcasted resulting in detrimental interference.

3.1.7. PUE Attack

Authors in (12) states that, this is one of the famous type of malicious attack. In this particular attack emulation takes place. That is, wicked malicious node emulates licensed user and broadcasts signals that are very similar to the one generated by original primary user .As a result of which secondary user gets fallacious idea about the occupied spectrum bands. Unlicensed user maintains the idea that primary user is present and hence will vacate the band, but actually that user is not present. Nodes that are responsible for implementing this type of attack are either greedy or selfish in nature.

3.1.8. SSDF Attack

This type of attack is basically for that environment in which fusion centre is the main hero. As we know that fusion centre is responsible for making judgement about the allocation of any particular channel or band by licensed user. If fusion centre gets false sensing reports as input, then it is but obvious that it will

produce wrong output or judgement. In this type of attack (13) malicious CR nodes provides fallacious sensing reports to the fusion centre, as a result of which it generates false output.

3.2. PUE Attack v/s SSDF Attack

Table 4
Difference between PUE attack and SSDF attack.

Attack	*Relationship*	*Effects*	*Remedies*
PUE Attack	Non Cooperative Spectrum Sensing [14], will affect decision of individual node	Fake signals responsible for generation of false alarms. Also access of the spectrum holes is restricted to the affected secondary users.	Location Determination Schemes and Geo location information about Primary users must be extracted.
SSDF Attack	Cooperative Spectrum Sensing [14] will affect master decision.	If inputs sent to the fusion centre are malicious then the results generated would also be false.	Outlier Detection Schemes, Reputation based schemes, implementation of trust-worthy nodes, authenti-cations, encryption decryption mechanisms etc.

4. SSDF ATTACK

SSDF Attack is also known as Spectrum Sensing Data Falsification Attack. As the name indicates "falsification", the paramount objective of this attack is to falsify the judgement regarding the absence or presence of primary signal (13) as given by fusion centre. According to authors in (15) SSDF is popularly known as Byzantine Attack.Diagrammatic representation of SSDF attack, is shown in Figure 2. shown below.

4.1. Objectives of SSDF Attack

Spectrum Sensing works on two objectives which are defined below:

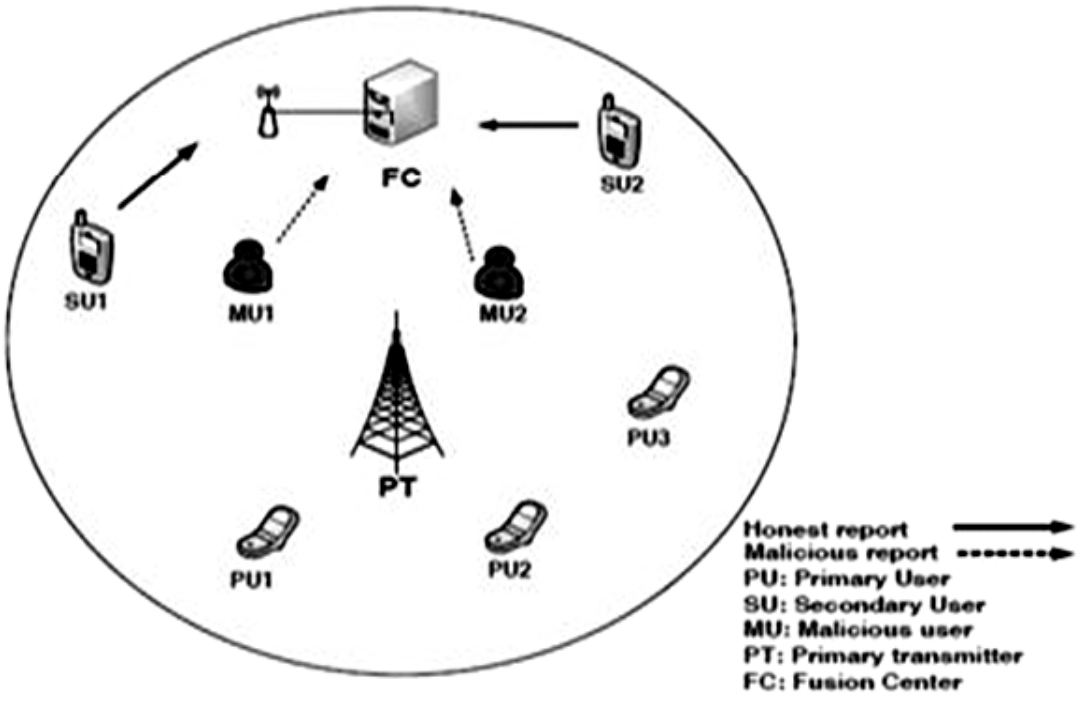


Figure 2: Diagrammatic representation of SSDF attack (11).

- Perniciousness Objective
- Persecution Objective

Perniciousness Objective: This objective deals with interference with primary user systems. In this particular objective class corrupted users indicates that channel is vacant but the sensing results implies that channel is strenuous. Due to the interference issues of secondary users again and again in the licensed bands of primary users, primary users feel uncomfortable and disturbed to share their licensed band with secondary users.

Persecution Objective: This objective of this type of attack is prohibition of free channels. In this particular objective class corrupted users indicates that channel is engaged but sensing results indicates that channel is free. As a result fusion centre which is responsible for making master decision gives wrong judgement that channel is engaged and thus advices all the secondary users to wait for certain time period and switches on to separate channels.

4.2. Attack Parameters

After discussing about the objectives of SSDF attack, in this particular section we will focus on the parameters of attack. Figure 3. shows anatomy of SSDF attack.There are four parameters of SSDF attack (15), which are listed and explained below:-

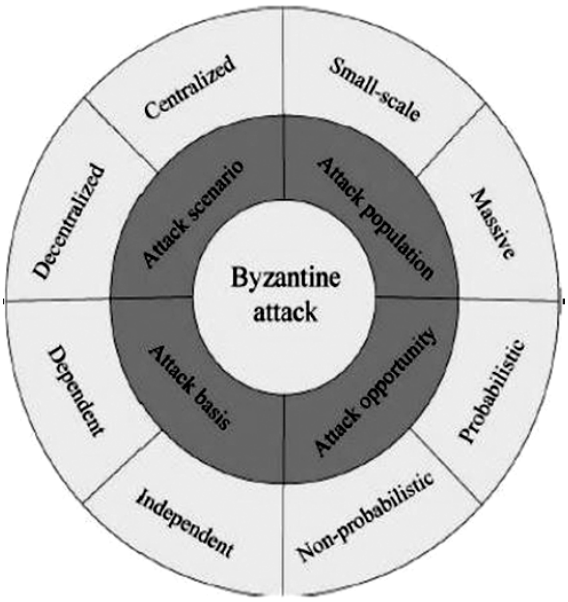
- Scene of attack: Where to Attack?
- Basis of Attack: How to Attack?
- Attack Episode: When to Attack?
- Attack multitude: Who to Attack?

Scene of attack: Attack behaviours are always affected by the management or arrangement of CR. If the nodes are arranged in centralized manner (centralized co-operative spectrum sensing then there must be a fusion centre to make judgement regarding the primary user presence. But if the nodes are arranged in distributed manner (distributed co-operative spectrum sensing) then there is no fusion centre to make the master decision but instead the master decision is taken by all CR users by sharing their sensing results in collaborative manner. Here an attacker is intelligent enough that first it takes into consideration limitations of environment and then plan the strategy in the way that it can take advantage of those limitations in order to gain some profit.

Basis of Attack: Here in this parameter, ground for making an attack is taken into consideration. Basically here the attacker will take into consideration the kind of information it has that is sufficient enough for an attacker to fulfil his strategy of launching attack. Basis of attack can be categorised into two types dependent and independent. Talking about independent attack, wicked attacker has knowledge about its own statistics but has no interpretation about spectrum states, sensing results etc. Whereas in case of dependent attack, wicked attacker has extra knowledge about multifarious parameters and is very useful for the attacker to implement an attack. Dependent attacks are the first option of intelligent wicked attacker.

Attack Episode: As the name depicts “episode”, this parameter depicts the time that the corrupted users should attack. There are three types of attacker (15), one type of attacker is that who can attack at any time, having little knowledge about the environment without taking into consideration whether it will be a successful attack or failure. Second type of attacker is that who makes a probabilistic attack. In probabilistic attack attacker can implements an attack with certain probability. Third type of attack is non-probabilistic attack which is very ore onerous to implement and tough to break.

Attack Multitude: This parameter describes the number of corrupted users present in the company of honest CR users. The more the number of corrupted users the more severe and precarious is the attack which consequently has a great impact on the judgement made by the fusion centre.



4.3. Archetypal Attack Models

After studying the four attack parameters, now we will discuss how these four parameters are interlinked with each other. The relationship of above four parameters describes the typical attack models. As per logic, four parameters can be arranged in sixteen different ways, because each particular parameters has further two types. So there are 16 attack models that describe the various combinations of these parameters. But out of sixteen attack models, only four of them are exclusive and widely used. Description of Paramount attack models are given below:

- Centralized Independent Probabilistic Small Scale Attack Model
- Centralized Dependent Probabilistic Small Scale Attack Model
- Centralized Dependent Non-Probabilistic Small Scale Attack Model
- Decentralized Independent Probabilistic Small Scale attack Model

Centralized Independent Probabilistic Small Scale Attack Model: This model is also known as CIPS attack model. This particular type of attack model has centralized environment in which minute group of wicked attacker attacks in an independent manner with the aim to adulterate the master decision and that too is possible with probabilistic opportunity. This attack model is relatively easy to implement and is considered centrepiece of alternate models.

Centralized Dependent Probabilistic Small Scale Attack Model: This model is also known as CDPS attack. The basic difference between CDPS and CIPS lies in attack basis parameter. CIPS model attacks taking into consideration personally collected information in the particular time period or slot but CDPS attack model attacks taking into consideration supplementary information such as sensing results, defence algorithms, fusion rules, reputation metrics etc. This particular attack model has centralized environment in which minute group of wicked attackers attack in a dependent manner with the aim to adulterate master judgement and that too is possible with probabilistic opportunity.

Centralized Dependent Non-Probabilistic Small Scale Attack Model: This model is also known as CDNS attack model. This particular type of attack model has centralized environment in which minute

group of wicked attacker attacks in dependent manner with the aim to adulterate the master decision and that too is possible with non-probabilistic opportunity.

Decentralized Independent Probabilistic Small Scale attack Model: - This attack model is also known as DIPS model. This particular type of attack model has distributed environment in which minute group of wicked attacker attacks in an independent manner with the aim to adulterate the master decision and that too is possible with probabilistic opportunity. Table 5. illustrates the relationship of attack models and attack parameters.

Table 5
Relationship between Attack Models and Attack Parameters

ATTACK MODELS	ATTACK PARAMETERS							
	Scene of attack-Centralised or Distributed		Basis of attack-Dependent or Independent		Attack Episode-Probabilistic or Non Probabilistic		Attack Multitude-Small or Large	
	C	D	I	D	P	N	S	L
CIPS	√		√		√		√	
CDPS	√			√	√		√	
CDNS	√			√		√	√	
DIPS		√	√		√		√	

ACKNOWLEDGMENT

At first I want to thanks my Almighty God without whom, I wouldn't have reached here. Then I want to express my gratitude towards my mentor Isha Malik of Lovely Professional University for guiding and motivating me at each and every step of my thesis writing. Also I want to thanks my mom who, always stand by my side encouraging and motivating me to learn every new concept with enthusiasm and courage and my father for his moral and timely support.

REFERENCES

[1] Katiyar V, Chand N, Chauhan N. Recent advances and future trends in Wireless Sensor Networks. See Notes. 2010;1(3): 330–42.

[2] Mounika B, Chandra KR, Kumar RR. Spectrum Sensing Techniques and Issues in Cognitive Radio. 2013; 4(April): 695–9.

[3] Abhiraami R. A Perspective of Cognitive Radio in Wireless Sensor Networks–A Survey. 2013; 3(1): 354–7.

[4] Abolarinwa JA, Achonu A. Cognitive Radio-based Wireless Sensor Networks As Next Generation Sensor Network/ : Concept , Problems and Prospects. J Emerg Trends Comput Inf Sci. 2013; 4(8): 642–8.

[5] Yadav N, Rathi S. Spectrum Sensing Techniques: Research, Challenge and Limitations 1 1,2. 2011; 7109: 240–5.

[6] Akyildiz IF, Lo BF, Balakrishnan R. Cooperative spectrum sensing in cognitive radio networks: A survey. Phys Commun [Internet]. Elsevier B.V.; 2011; 4(1): 40–62. Available from: http://linkinghub.elsevier.com/retrieve/pii/S187449071000039X

[7] Rifà-Pous H, Blasco MJ, Garrigues C. Review of Robust Cooperative Spectrum Sensing Techniques for Cognitive Radio Networks. Wirel Pers Commun [Internet]. 2011;67(2): 175–98. Available from: http://link.springer.com/10.1007/s11277-011-0372-x

[8] Meena OP, Somkuwar A. Comparative Analysis of Information Fusion Techniques for Cooperative Spectrum Sensing in Cognitive Radio Networks. 2014; 2–9.

[9] Johnson B, Roller P. Review Article. 2015; 4(3): 845–53.

[10] Sen J. A Survey on Security and Privacy Protocols for Cognitive Wireless Sensor Networks. 2013; 1–31.

[11] Fragkiadakis AG, Tragos EZ, Askoxylakis IG. A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks. IEEE Commun Surv Tutorials [Internet]. 2013;15(1):428–45. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6129369

[12] Alahmadi A, Abdelhakim M, Ren J, Li T. Defense Against Primary User Emulation Attacks in Encryption Standard. 2014;9(5):772–81.

[13] Li J, Feng Z, Wei Z, Feng Z, Zhang P. Security management based on trust determination in cognitive radio networks. 2014; (10): 1–16.

[14] Marinho J, Granjal J, Monteiro E. A survey on security attacks and countermeasures with primary user detection in cognitive radio networks. EURASIP J Inf Secur [Internet]. 2015;2015(1):4. Available from: http://www.scopus.com/inward/record.url?eid=2-s2.0-84928387229&partnerID=tZOtx3y1

[15] Zhang L, Ding G, Wu Q, Zou Y, Han Z, Wang J. Byzantine Attack and Defense in Cognitive Radio Networks: A Survey. IEEE Commun Surv Tutorials [Internet]. 2015;17(c):18. Available from: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7084574