Security Analysis in Cognitive Radio

Project report submitted in partcontentment of the necessity for the degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

By

Kanwar Singh (161116) **Bhaashit Agarwal (161834)**

UNDER THE GUIDANCE OF

Mr. Alok Kumar

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
ELECTRONICS AND COMMUNICATION ENGINEERING

May 2020

TABLE OF CONTENTS

DECLARATION

We hereby declare that the work reported in the B. Tech Project Report entitled **“Security Analysis in Cognitive Radio”** submitted at **Jaypee University of Information Technology, Waknaghat, India** is an authenticrecordofourworkcarriedoutunderthesupervisionofMr.AlokKumar**.**Wehavenotsubmittedthis work elsewhere for any other degree ordiploma.

Kanwar Singh

Bhaashit Agarwal

Kanwar Singh
161116

BhaashitAgarwal
161834

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Alok Kumar

Mr. Alok Kumar

Date:

ACKNOWLEDGEMENT

We write this acknowledgment with the utmost admiration, proudly acknowledging our admiration to all who have unswervingly or circuitously allowed us to complete this project. We would like to express our gratefulness to our Supervisor Mr. Alok Kumar for being a continuous source of motivation, valuable leadership and encouragement to all of us expressly in resolving difficulties we come across while working on this project.

LIST OF ACRONYMS AND ABBREVIATIONS

CR	Cognitive Radio
PU	Primary User
SU	Secondary User
QoS	Quality of Service
DoS	Denial of Service
SR	Software Radio
PDA	Personal Digital Associate
SDR	Software Defined Radio
DSA	Dynamic Spectrum Access

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

In wireless communication system Cognitive Radio (CR) staysanedifice that can gives an intelligent honor to interconnect over internet. Cognitive Radio (CR) shrewdlyconsents user to use unrestricted spectrum. It is with dynamismconstituted and it permits more user in wireless system. Due tospectrum sensing, sharing, mobility there is aproblem in safety. Guaranteeing security and consuming spectrum resourcefully is stimulating. In this venture, the safetycoercions of cognitive radio systemstancemomentarilydiscoursed. Afterwardelucidationroughly of probable attack, we have accentuated on some actualattacks. Per the predominantarrangementprototypical the likelihoods of false alarm and miss detection partakesremainedpremeditated.

CHAPTER-1

1.1 INTRODUCTION

By means ofpresent’s craving for more wireless devices and systems, the requirement for indistinct resources to house these systems cultivates every day, but the lingering spectrum resources seems to be running out. Cognitive radio expertise offers a pioneeringresolution to this predicament by looking at thespectrum in an eccentric method as a multi-dimensional space. The modern-day wireless communication systems are administrated by static spectrum taskstrategy, which was documented by measurement to be inept. Cognitive radio qualifiesexciting spectrum exploitation proficiency through practical access to in code unutilized portions of array. This report boons an over-all framework to cognitive radio technology;itprovidesajustificationofitsbasics,structure,andcontests.Itconversedthechiefideas, notions and connotations aimed at this technology, and it explicates its foremost tasks, functions, apparatuses and building. Moreover, it pronounces the cross-layer cooperation of separately cognitive occupation. Finally, it gifts some palpable ideas projected for the thoughtful of cognitive radio purposes.

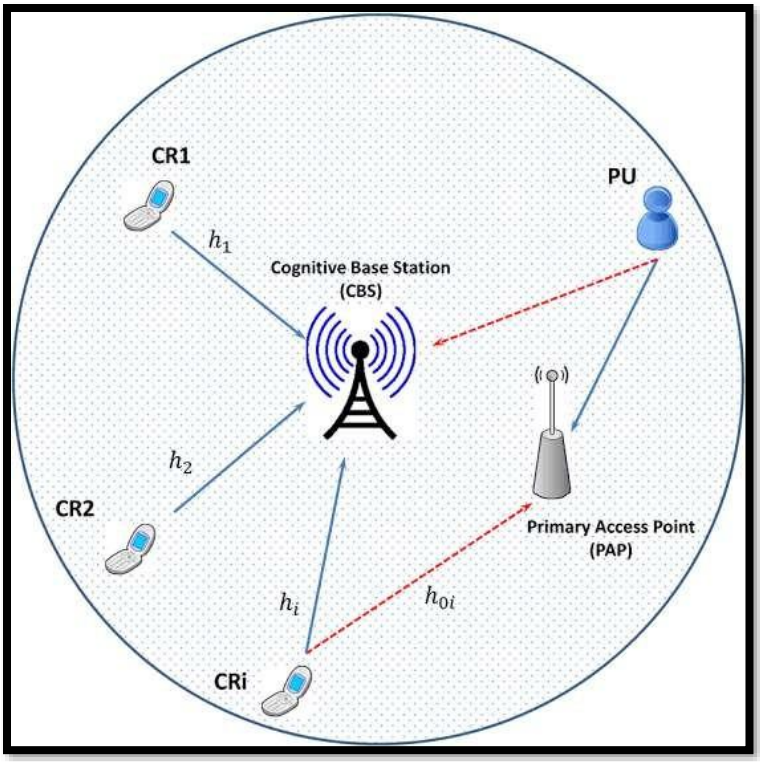


Figure 1.1: Basic Cognitive radio System

1.2 Motivation

The wireless infrastructuresfruition followed in current years has an inherent problem: the buddingdearth of spectrum. With the Cognitive Radio (CR) characterization, it is endeavored to crack this delinquent by using the spectrum animatedly. CR toleratescompetent use of presented spectrum by essential of two types of users in wireless systems: certified and uncertified users. An uncertified user (also called Secondary User (SU)) can habit the band if it is not being used at that period by certified users (also called Primary User (PU)). When the certified user seems to habit the spectrum, uncertified user must find alternative spectrum to use. In spite of cognitive radio is alively field of study,securityfacetshavenotyetbeenwhollyrevealedeventhoughsecuritywillto be anticipatedplayavitalpart in the long-standingmarketablepracticability of the technology. The security architypes are often inbred from typicalsysteming and do not right with the provisions of cognitive radio systems. Granting there is not lot of fiction about this subject, lately, scholars have seen that cognitive radio has unusualphysiognomies that makes its own safetyathought-provokingexamine field, afterward more stakes are given to assailants by cognitive radio expertiserelated to inclusiveradiosystem. At this extantperiod, no such secure structureoccurs for cognitive radiosystems.

1.3 THE STRUCTURE OF COGNITIVERADIO

A cognitive radio is principally a session of software radios (SR's) with superfluousassistances and functionalities such as etheridentifying, facts, and supervisory, which empower it to scope the obligatoryvigorouspresentation. On software program level, cognitive radio aidsseriatim of elevated application software to rival a personal digital associate (PDA). In command to recognize the structure of a cognitive radio, we have to reconnoiter software transistors and their real-world form; the software-defined radios (SDR's), afterward they characterize the focalmodule of a cognitive radio. The respite of this segmentoffersanephemeralsummary of software radios in additionto software defined radios. A software radio (SR) is distinct as a transceiver whose communiquéresolves are comprehended as agendasseriatim on anapt processor. Henceforth, a SR encompasseswholly the protocol load coats of a communiqué system. Founded on the similar hardware, variation of spreader/receiver algorithms can be completed on software to contestunalike broadcast canons. A wide-band antenna steadfast to the hardware authorizations its progression over unalike bands. A software radio is hence, decidedlymobile and modifiable, whichlights the lifeforce of the cognitive radio backgrounds. Asupreme SR directly illustrations the antenna harvest and renovates these models to digital expanse, and then the perfect base band signal dispensation is done in ordinalfield.

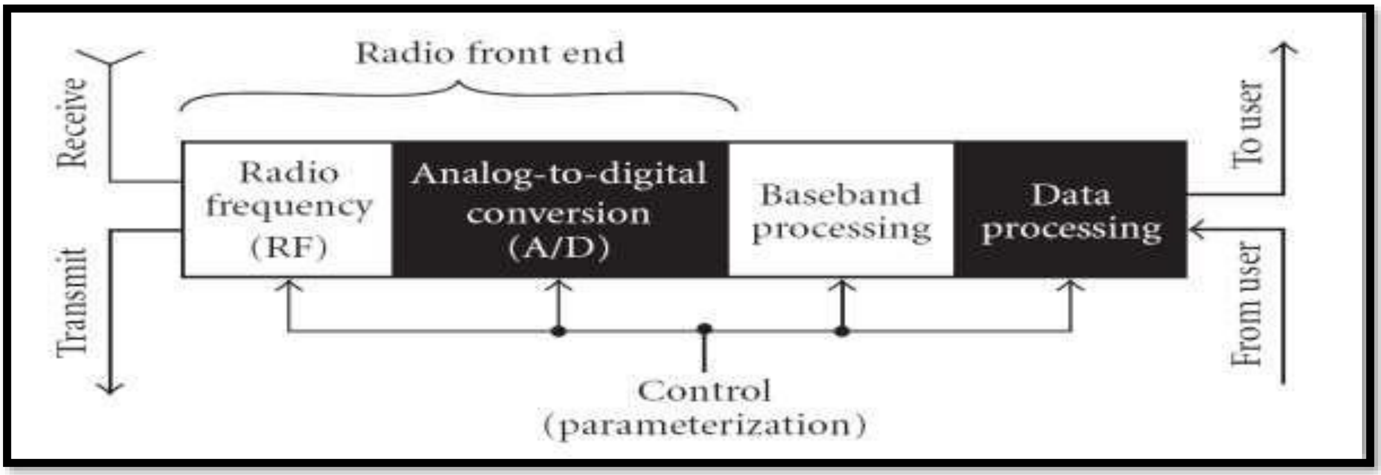


Figure 1.2: Basic structure of CRN

1.4 CONCEPTS AND DEFINITIONS INTRODUCED FOR COGNITIVE RADIOTECHNOLOGY

The espousal of the cognitive radio technology as the technology for the ensuing cohort wireless systemsoccasioned in the advent of groundbreakingperceptions, newfangledcharacterizations and innovativestatistics. In the ensuingsub-sections,weconfersomeofthefocalimpressionsandexplanationsfamiliarizedbycognitive radio expertise in directive to variety it relaxed to grasp and précis the ponderings in the succeedingsectors:

1.4.1 PRIMARY/SECONDARYUSERS/SYSTEMS

The presence of cognitive radio diplomaciesseparations the wireless spectrum manipulators into two categories or defenses, i.e., Primary (certified) users, and Secondary (uncertified/cognitive) users. Afterward, two systems shall segment; primary system, which encompasses all primary users through their precisecertified communication systems, and a tributary autonomous system that comprehends secondary unrestricted cognitive operators. Primary users are the original incumbent users that can have bequest entrée to their devoted spectrum bands unreservedly at any stretch or room. Secondary users standthe cognitive radio operators that entrée spectrum in acorruptcustom. Primary users do not parade anycognitivecomportmentandtheirevolutionordesignessentialnotbeexaggeratedbytheoccurrence ofcognitive manipulators. The absolute reputation for spectrum access incessantly goes to the primary manipulator. Even if the secondary user is by nowcollaborating over a confident channel, it must hollow this channel unswervingly if a main user was distinguished to be trying to entrée thischannel.

1.4.2 SPECTRUMHOLES

Thistenurewasfirstdefiniteinas“abandofoccurrencesowedtoaprimaryuser,but,ataspecific time and unambiguousstructural location, the band is not actualityrummage-sale by that operator”. As, spectrum hole explanation can swell to have countlessmagnitudes. A spectrum shack can be a band of consistencies unutilized by the chief user at a confidentperiod, or at a stable position, or discrepancy, or code, or can be anassortment of roughly or wholly of these. In, a spectrum shacks were classified into threecategories:

1. Black spaces, which are entirelybetrothed by primary users roughly of thetime
2. Greyspaces,whicharepartiallyemployedbylow-powerinterfererssuchasshort-rangeUWBdevices.
3. Whitespaces,whicharefreeofRFmeddlesomeexcludingforambientnoise.Theprincipleofacognitive radio operation is mainly based on tracing these shacks and carrying data over them.Yet, this involves addedcompound and progressive resolutions as will be deliberated in the rest of thisaccount.

1.4.3 SPECTRUMPOOLING

Spectrum pooling is a term that epitomizes the cohabitation of dual autonomous radio systems; the primary and secondary systems exclusive the matching frequency array. It empowers unscrupulous usage of previouslyproficient frequency bands by the secondary (cognitive) system. It chieflyepitomizes the impression of consolidation spectral ranges sinceunalike spectrum possessors (military, trunked radio, etc.) into a joint pool. The unbiassed of spectrum pooling is to progress spectral efficacy by casinga new radio system (cognitive radio system) on a predominant one shorn ofnecessitatingsomewhatvagaries to the factualproficientsystem.

1.4.4 INTERFERENCE TEMPERATURE

TheinterferencetemperatureisprecisetobetheRFpowerrestrainedatareceiptantennaper unitbandwidth.Itepitomizesainnovativeschemefortotalingintrusion,somewherethe stimulusofalowlevelcommunicationsystemsuchasshort-rangeUWBisimplicittobejustaddednoisesourcethat is encompassed in a link budget. All in all, of these sources are summed organized to arrangementof anewfangled noise floor. The noise level in a prearrangedmilieu can be alleged to be unruffled of three foremostmechanisms:

1. Natural thermal noise(KTB).
2. Unintentional man-madenoise.
3. Intentional man-made noise (e.g. short-range UWBdevices).

To some extentbudding the noise level by consenting a trivial amount of unhurried man-made noise can afford us with a great juncture for truncated power systems to activate below this meddling cap. Short- range UWB devices, for illustrationtake a very truncated transmission power, unbiassed one or two dB overhead the inventive noise floor, subsequently in utmost wireless systems, the link budget proposal takes into interpretationroughly link margin, so, the exhibition of these systems practically will not be exaggerated by the manifestation oftheUWBdevices.As perwecanperceiveinthefigureunderneath,theintrusiontriggeredbytheUWBdevices isitemizedbythepeaksovertheuniquenoisefloor,inthefoulestcase,thenewfangledinquisitivecapmolded by the UWB devices to some extentdiminishes the range of course of the primary proficient system. Nevertheless, this small supportvintages a massive spectrum chance for innumerable systems to activate in the UWB range.

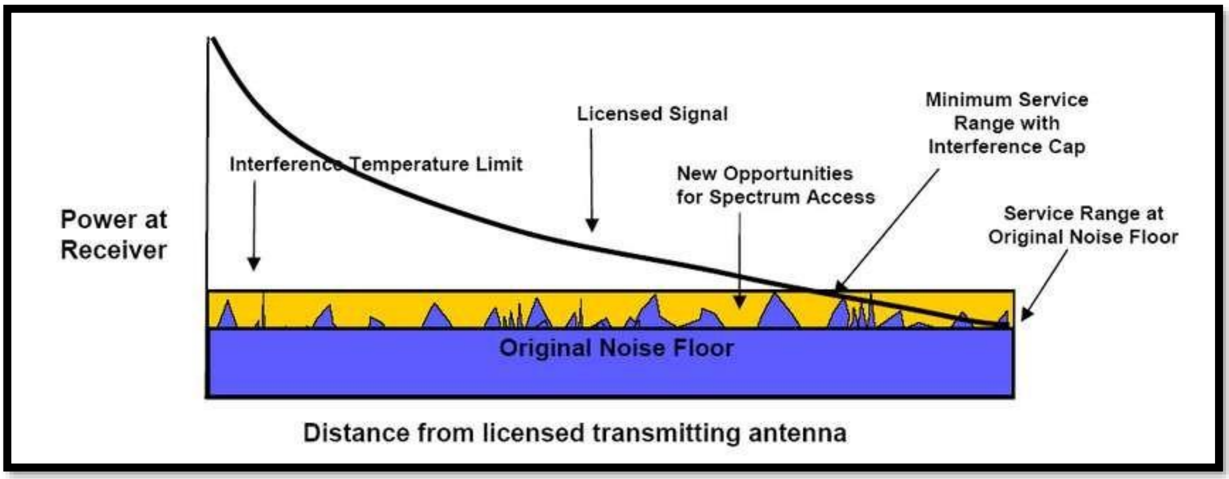

Power at Receiver
Interference Temperature Limit
Licensed Signal
New Opportunities for Spectrum Access
Minimum Service Range with Interference Cap
Service Range at Original Noise Floor
Original Noise Floor
Distance from licensed transmitting antenna

Figure1.3: Effect of Temperature

Interference temperature limit (interference cap) is the static limit for the volume of intrusion that secondary users are tolerable to cause to the primary users, henceforth low power devices are acceptable to activate as long as their transmission do not overdo the intrusion cap. The occurrence of this intrusion cap would affirm that the proficientmaneuver would not understanding any further deprivation or cost of service from innovativenosiness, and so provide proficient systems superior certainty regarding the thoroughgoingacceptable level of prying RF energy in the bands in which theyactivate.Thiswillconsentanaddedunswervinglinkbudgetdesign.Twowayswereanticipatedfor steadfastinterfering temperature assessment:

1. By means of the multi-taper structure to conjecture the supremacyrange of the intrusive temperature billed to the snowballingdispersal of mutuallycorefoundations of noise then external causes of RFenergy.
2. By means ofdisseminatedinstruments that can competentlysnuffle the RF milieu, heftyquantity of instruments can be secondhandtowardremunerationaimed at the altitudinaldiscrepancies of inquisitive temperature as ofonlydwelling to additional.

1.4.5 Spectrum Decision

Subsequentlydistinguishing the frequency rangethendiagnosing the “white spaces” cognitive radio handleroughtespousewhich frequency band is the incomparable to convention (Alahmadi etal., 2014).

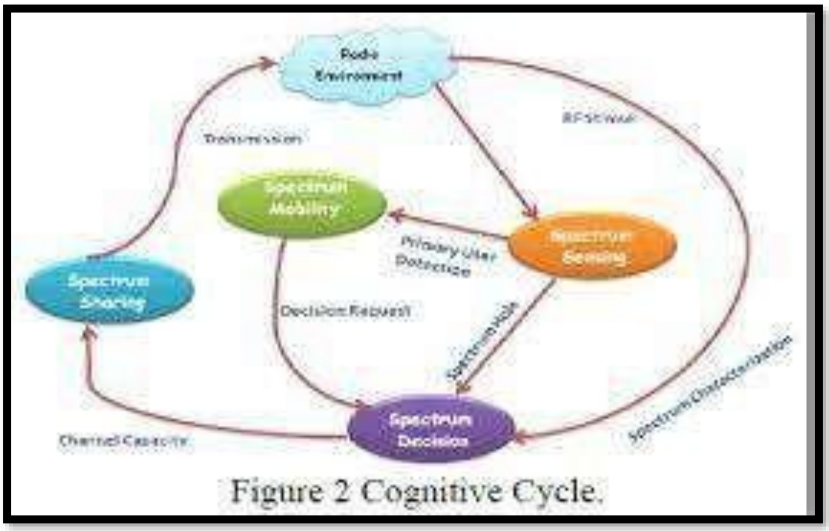


Figure1.4: Cognitive Cycle

1.4.6 Spectrum Mobility

How the person using the radio changes the frequency of the process. Radio programs that do not choose to participate in a transparent way by allowing radio stations to focus on the band are often very accessible, supporting the communication needs of one business to change the spectrum (Liu, Ning, and Dai, 2010). So, which often has a clear, shared look and experience to save the way for CR users, it's also amazing to write about a non-aggressive user who wishes to use more. When a second unsecured user is returned to a given youth, the malicious user [MU] is not accepted into the CR program. A malicious user may raise a primary user signal to expose and cause a false alarm to another secondary user. After receiving a false alarm, the second user cannot detect that the signal was directed by the malicious user. Therefore, SU cannot carry out the act of adoption. A good test to discourage malicious user attacks. In this paper, we discussed the same for certain attacks. We can break security threats into the information radio system in two ways: threats to the user to understand and impose a rule on the primary user. We can break the security of a virtual radio program in two ways: forcing the user to monitor and threaten the primary user.

1.5 INTRODUCTION TO SECURITY IN COGNITIVERADIO

The radio spectrum is ainadequatereserveat presentenduring marvelous intensification in mandate and, subsequently, budding in scarcity. This trend will linger in the forthcoming as the volume of arrayed wireless technologies in accumulation devices intensification, the same smearing to the bandwidth provisions. As well, the few predominant license-free radio frequencies, such as the industrial, scientific, and medical (ISM) bands, are recurrentlyteeming, exclusively in solidlycolonizedzones. This stategrades in quarrel and nosey, and, consequently, in imperative performance lack. In the face of such geographies, we can correspondinglywitness that the conventional of the proficient radio spectrum relics idle or underutilized self-sufficiently of time and location, consequential in countlessvoid spectrum bands. This bunglingpractice of the spectrum outcomesunswervingly from the current spectrum rule guiding principle, which scrappy the spectrum into static certified and Uncertified frequencies. The import of supplementarystretchyguidelinepoliciesandtheextensionofcorrelatedandground-breakingtechnologieswillalteration this model, with cognitive radio (CR) unindustrialized as single of the vital enablers in thisoutline.

Table 1.1: Chāracterization of attacks against the standardworking of CR

systemsIncentives	AttackGoals	AttackApproaches	AttackEffects
Avaricious/Selfish	Make the most ofthe communiquépresentation ofassailants	Make the SU's Trust that emptyareas of band are full (i.e. encouragewrong alarms) and entrée them completely.	A worldwidereductionarrangedrange allocationproficiencythenconventionimpartiality.
Malevolent	Dislocate the presentationthenactions of SUs and/or PUs	Make the additional SUs trust that unoccupiedshares of the bandremainfull.	Adiminution in rangepracticecompetencebesides, so, in the presentation of exaggerated SUs.
		Make the SUs trust that demandingshares of the range are perfect (missed detections).	A cut in the defense of the pretentiousExcretionin contrast tointerferingproducedby (inaccurate) SUs spreads

The CR device is expected to highlight the power of sight and fullness as its ether, and prepare with enthusiasm and ownership to deal with transmission problems such as quantum and Communique operations, in order to review its transformed power without interruption. Of particular importance in the CR model is the integration of software-defined radios (SDR), Equipmentag's radiagommunication systems that are very sensitive to software limited hardware. We previously supported free access to SDR platforms, which are in the process of creating new platforms and testing proposals in the CR area. Through dynamic visualization (DSA), CR users, and even special users (in Ephesus), are able to deceive and expose nail holes in a clear way to operators (red) and deepen the onset of harmful cleaning. The position of some sharp holes gives the impression that as an interesting and prominent subject in the CR area.

Table 1.2: Defense Against Attacks

Attack	**Behavior**	**Targeted Layer inthe protocol Stack**	**Planned Solution**
Denial of service Attack[2]	An assailantpains to avoidsincerehandlerssinceopeninginfo or amenities	System Layer, Application Layer	Digital signature implementation of trust metrics, WPKI securityin CRN
Incumbent Emulation Attack [7]	In an incumbent emulation (IE) outbreak, a malevolent secondary user tries to gain priority over other secondary's by transmitting signals that emulate the characteristics of an incumbent	Physical /Mac Layer, Application Layer	End to End Authentication, Implementation of trust metrics, WPKI securityin CRN
Spectrum Sensing Data Falsification Attack [3]	An attacker may send false local spectrum sensing information to the cognitive radio user and cause interference and inefficiency in spectrum band	Physical/Mac layer, Application Layer	Misbehaving user detection, Attack proof Collaborative spectrum sensing
Byzantine Attack [2]	Cooperated medicate node or set of compromised medicate nodes woks in collusion and carries out attackssuchascreatingroutinghop,routingpacketson non-optimal paths, and selectively dropping packets.	Physical/Mac Layer	Misbehaving user detection, Attack proof Collaborativespectrum sensing
False Feedback Attack [5]	Malicious User hides the truth about the occurrence of certified users, and other nodes cannot sense the information due to signal fading or long distances	Physical/Mac Layer	Misbehaving user detection, Attack proof Collaborativespectrum sensing
Biased Utility Based [5]	Selfish user changes utility function parameters to get more bandwidths, so the bandwidths of other uncertified users are decreased.	Physical/Mac Layer	Misbehaving user detection, Attack proof Collaborativespectrum sensing

Wormhole Attack [6]	Malicious user receives a signal from the transmitter in the system and tunnels them to another location inthe system.Inthisattackresentthesignalintothe system.	System Layer	Authenticated Routing ForCRN
Blackhole Attack [6]	The intention of the malicious user could be to hinder the path finding process to interpret all the transmission process.	System Layer	Authenticated Routing ForCRN

Routing Attack [6]	Malicious aim to disrupting the operation of the system and perform routing table overflow, routing table poisoning, packet replication, route cache poisoning routing attack	System Layer	Authenticated Routing ForCRN
Session Hijacking Attack[4]	Malicious node take control over a session between two nodes, the malicious node in a squerades as one of the end nodes of the session and hijack the session.	Transport Layer	Co-operative security mechanism
Repudiation Attack [9]	It refers to the denial or attemptable denial by a node convoluted in a communication of having participates in all or part of communication	Application Layer	End to End Authentication

It is well integrated into everything that allows bandwidth to be completely limited to local hiring and provides the right results. The main reasons are the unavailability of alarms and false alarms, which are separated by a small type of computer sensors and can affect the disruption of broadcast structures such as frequency of cracks and emissions. This indicates that by preparing any special screen it must respond to multiple sources of information. For example, the rule of law may apply to our interest reports and location data, if possible. In this framework, false data assembly is a high risk that can result in incorrect validation and, in the case of partial protection of PUs (e.g., due to missing data) or failure, layer, or assembly due to alarm violations. CR ether is temporarily inactive in programs designed to achieve thigh analysis and resolution of SUs. The purpose of a simple local solution is to allow SUs to be driven but by practice they can be issued da-di-da by mistake or false information. Predicting Broadband readiness data due to hardware imperfections and increasing conflicting results or, on the other hand, to security attacks, excessive data compression and PU simulation, as we discuss all these tests. Well-intentioned attackers can say that they are not in line with what they have seen with the removal of the CR system (e.g. reduction of PUs or spectrum performance). On the other hand, attackers with greedy or ambitious motives may misinterpret these work events to gain private access to the spectrum. Around the world, malicious attackers and investigators have no public basis for doing creation (DoS) on official SUs

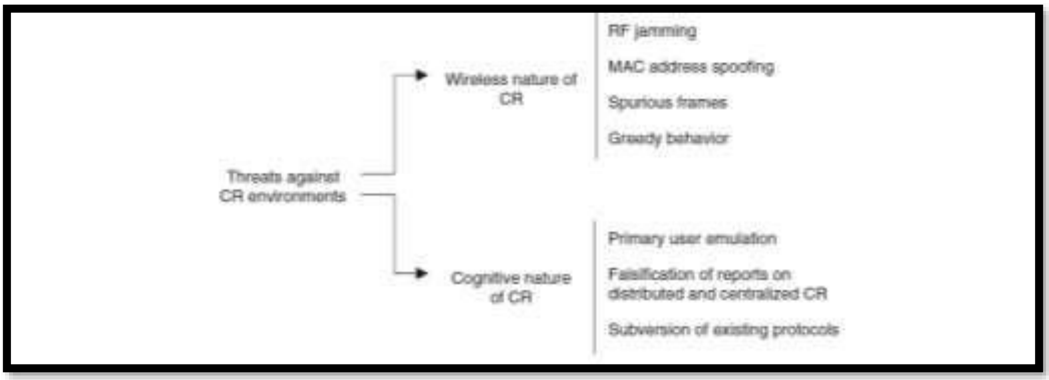
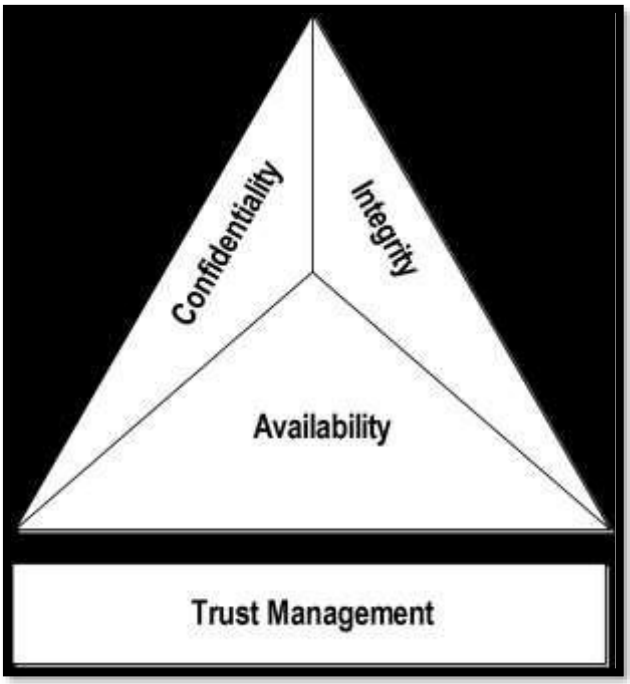


Figure1.5: Threats against CRN

The argument for strengthening the theoretical relationship with the availability of PU is of particular importance to CR linkages and focuses our discussions on research. In addition, any threats against the normal operation of the equipment used to detect PU activity or the presence of a mirror interfere with the normal operation of the CR. Our need to provide how such teaching is taught in the decisions of modern technology and to distinguish open issues in this framework. Aside from the presence of a few available services for CR-related security issues, no one has deliberately provided a comprehensive and clear app for security threats compared to the general disclosure on CR sites, organized by existing framework and open integration. in this study. Our discussions seek to provide a never-ending debate about threats such as these in Andon about how he wants to deal with them, both in relation to mathematics and the encounter where he has to deal with trying to learn. The investigation continues as follows. Section 1.2 outlines the limitations of CR which transform our insecurity into paper. Section 1.3 discusses the basic security and threats that apply to Milieus, and in Section 2.1, we discuss the potential risks of PU exposure and the potential research implications of this behavior.



<u>Figure1.6</u>: Cognitive Radio Security Factor

CHAPTER-2

LITERATURE SURVEY

2.1 ATTACK ON DIFFERENT LAYERS

2.1.1 BLACK HOLE ATTACK ON SYSTEMLAYER

Black Attack will be a powerful offensive set of marches on a program deal's visual message (PRRE). The hostile environment dominates the RREP reports investigated in its table by substituting for trinus. The RREP monument is in a vacant lot, which is the first place to be seen below. So far, the main platform has installed its new routing table on Terminus nodes and includes any other RREP connections from the trusted terminus location to adjacent or unchanged locations. When it comes to the original source route, tweaks and transfers that store data packets on the original hosting company will certainly be distributed to the original deminus. However, the lone node (which works by attacking the black hole) is packed with packets of information rather than speed. Providing a variety of studies focusing on reducing the property of malicious attacks on the system, preliminary results show that black hole attacks are more sophisticated than computer integration.

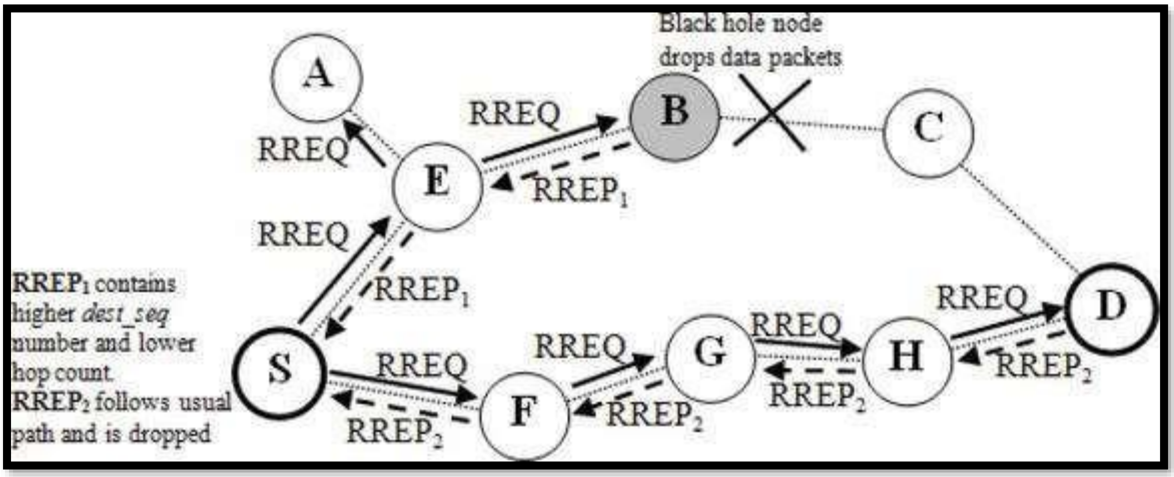


Fig 2.1: Black hole attack illustration

2.1.2 WORMHOLE ATTACK ON SYSTEMLAYER

The wormhole attack, anauthoritative attack that can have solemnsignificances on many anticipated ad hocsystemroutingprotocols;thewormholeattackmayalsobebrowbeateninothercategoriesofsystems andsubmissions,suchaswirelessaccesscontrolsystemsgroundedoncorporealjuxtaposition.Toperceiveand preservein contradiction of the wormhole attack, we familiarized packet strings, which may be what's more geographic orchronologicaltethers,toconfinethethoroughgoingbroadcastdetachmentofapacket.Finally,tocontrivanceprogressivetethers, we obtainable the project and recitalscrutiny of a novel, competent protocol, called TIK, which likewiseaffordspromptsubstantiation of acknowledgedpackets.

- **Proposed Solution**

TIK requires just n communal keys in a system with n nodes, and has comparativelydiffident storage, per packetsize,andtotalingoutgoings.Inspecific,anoderequeststoaccomplishonlyamongst3and6 hash function estimations per time interlude to sustain up-to-date key evidence for the aforementioned, and jaggedly 30 hash functions for apiececonventional packet. With product hardware such as 11 Mbps wirelesslinks,TIKhascomputationalandreminiscencenecessitiesthatareeffortlesslysatisfiabletoday;2.6 megabytes for hash tree stowingepitomizes, for example, less than 3% of the averagereminiscence on an Compaq iPAQ 3870 with no peripheral memory cards, and meanwhile the Strongarm CPU on the iPAQ is accomplishedofexecution222,000symmetriccryptographicmaneuverspersecond,TIKenforcesno more thanan18%loadonCPUtime,unfluctuatingwhenswampedwithpackagesatthethoroughgoingspeedofthewireless system, and customarily uses less CPU load than that in regularprocess.

2.1.3 SESSION HIJACKING ATTACK ON TRANSPORTLAYER

When the linking is recognizedamongst the nodes, the attacker parodies the victim’s discourse and pieces like the victim. He dismisses or postponements the communiqué which has been by nowrecognized and takes away the linking. Then, the connection is recognizedamongst the source and the attacker. The TCP session commandeering attacks are throwing by the attacker after expressive the preparation number in the TCP handclasp and founding the communication with the source by substituting existing linking with the terminus. The source uninformed of this directs the data unceasingly to an attacker in its place of the real client. The source ignorant of this directs the data unceasingly to an attackerin its placeoftheactualclient.Thesubsequentcategorizationofhierarchiesstayssupportedoutformerlyac onstruction is predictable.

Step 1: The userguides a SYN entreatyper I by way of the categorizationamount.

Step 2: The server declares it by means of i+1 laterallyby means of j per the succeedingcategorizationfigure.

Step 3:Patronat that timedirectsaheading to j per j+1 via incrementing the categorizationfigure.

- **Proposed Solution**
  - TRANSPORT LAYER DEFENCE METHOD (TLDMETHOD)

The greatest way to handle the three-session commandeering attack is to avert the manifestation of the attacks.

I. Active attacksdefense

It takes time to work by catching a deer after receiving the partition number sent with the options of the SYN. The partition number can be updated by a multimedia source to avoid numerical computation. For example, one number can be subtracted from the rest. In SYN with number 1, it is enabled for the client to access the mode. Length has been assigned to pipeline 2 with the new SYN 5 based on the source location. The guard accepts the transfer as a string serial number. Using the identification process, partition number 1 is moved to the left and multiplied where the third crop is.

II. Passive attacksdefense

Attack of the passive session attack can be performed on a veto by passing queries periodically to the source protector over time. The answer to a question can only be made by the recipient. The number of frames will be reconstructed using the inversion concept. Forunaffected node

Step 1: Despatcher node stimulates the enquiry

Step 2: Correspondent node augments time imprint and leads the inquiry

Step 3: Dispatcher node vicissitudes the basesystemfigure S(n)=S(n’) Wherever n’ embodies the arrangementfigure of the settransformed by any measuredworkuseful on S(n).

Step 4: Basiswithstands the intermediate node totals in a bench and formsonce the communicationspermitcompletes them through the aid of Period to LivingRate.

Step 5:Terminusreceives the inquiry with periodimprint

Step 6: Patronripostes with precisereaction to the inquiryinside the period If the assailant is contemporary in theschemeandtakeoversthesittingpredictablewiththequarryformerlytheassailantcouldnotrealize andresponsetheinquiry.

Theassailantpossibly willnotunderstandtheborderorganizationsmoothifitattemptstodisplay the circulation. Uncertainty the assailantattempts to interruption the communiqué the period stamp drivedivulgesthat.

III. Hybrid attacks-defense

The communicationsremainautomatedby means ofanimportantas, M=E(m) on the basis side. The patron decrypts it by means of M=D(m), The encryption techniquerummage-sale is itemized by the foundation to the usernowadays.

2.1.4 SPECTRUM SENSING DATA FALSIFICATION ATTACK ON APPLICATION AND PHYSICALLAYER

Spectrum Sensing Data Falsification (SSDF) or Byzantine attacks. In one of these attacks, a user who has added a third-party fix or a second user and who can start broadcasting to see the PS results is converted. In this way, the attacker attempts to reset the BS in the malicious transmission of the network region. Workplaces can work independently or work together to weaken the use of envelopes and make the implementation of the world system difficult.

Creating a policy-making plan to track the removal of these types of attackers will mean access to CRNs as they become more widespread. By deliberately integrating the original channel with malicious users or order managers, contractors will be awarded as CRNs and will pursue such systematic transactions. Finally, potential business users can withdraw money through the regular CRN Radio Training Workshop.Proposedsolution

- REPUTATION BASED APPROACHES

Wang et al. Propose to use an onion-based strategy based on Bayesian statistics to create a suspicious quantity of all the nodes in the system. If the inadequacy of any node violates a certain line, it is clearly sensible and they do not believe in decision making. They also reaffirmed the basis for detecting false alarm attacks, detection attacks, and their coordination. Also, they think that the site is full of facts about the experience of anonymous attackers. Such details have been removed, the thresholds are close, and the result of misdiagnosis by the attackers.

Chen et al. Propose a Weighted Sequence Rate Test (WSPRT) for dye and ground testing to identify hazardous or damaged materials. This process transcends normal coordination systems and relates to AU, FU, and SPRT responses for missing signal processing and uses the right amount of audio. However, the WSPRT was confirmed only when challenged by attackers who submitted a wrong or consistent response. Such a possibility refers to a relatively inexpensive type of attack, which can be expected to retaliate against the attack. This process also includes a large number of secondary users who may see uninstall reports filed by the union, which may prevent the system from being reinstalled as a result of malicious user corruption. Recently, Rawat et al. Al. Independently and socially in scouting attacks. They find powerful tactics to attack a particular invader somewhere that the local center can distinguish loyal and attacking CRs. Challenge detection was obtained using the Kullback-Leipler (KLT) deviation. To deliver its conclusion, in the expression of 50% of private attackers, the Integration Center cannot include a switch between trusted users and attackers. So far, in a joint attack, this rate has been reduced to 35%. In addition, they were looking for a surefire way to build the reputation of the invaders. Focusing on process ships in the wake of the invaders' misbehavior has taken the form of ownership. The upcoming process works through a window to identify the smallest amount of decorations reported to identify the attackers. Under such restrictions, temporary access errors for legitimate users ensure their signatures are out of permission. As more loyal users are removed from the voting process, the machine leaves the final decision-making burden to only a few users. In such cases, the system is left very weak. Any attack on the remaining users can infect the entire cell. In addition, the probability of route error increased significantly when 35% of the sites collided with the attack.

➢ DATA MINING APPROACHES

The new design introduced in the K-Area Distance Algorithm is available to users of sorts. 158 C.S. Haider, B. The Phenomenon. Previous details of Grabber and X Xiao's rotational attack and manufacturers' rotation do not require style. However, when attackers join forces and gain a second user experience, they can make better use of that expression. Additional work has begun with the end of the trading system. In particular, specific descriptive information is used to verify the user base assigned to each second user. Details of PU employment and loss of a third-party user can prove your input.

The overall collection of visual information was considered a total and complete deviation from the quantitative analysis, which is inextricably linked to the classification of attackers. The expected process is dramatically enhanced by negative feedback when generated by negative static parameters. Failed supervised users can be included in the decision-making process, resulting in the PU signal being ignored. Finally, the right kind of adoption guidelines can be uniquely identified with the information of the attackers. Also, the details are amazing to find.

- ARTIFICAL INTELLIGENCE APPROACHES

Clancy et al. Focus daily on CRNs, on physical safety planning, and on CRs. After doing those programs, CRs are at greater risk for short and long-term data generated by understanding data, altered calculations and algorithms. This article proposes a competitive series on the categorization of these weak areas by embedding them, creating social elements, and planning to redefine selected values to avoid invaders' exploitation. They provide the use of group actions to define the global preference for the authentication signal generated by the primary user and then by a credibility-based program. Tenders for how CRSs work in the wild are reduced by verification information. They do not see how to add new information to the existing 802.22 system. Today's study space is limited to this intuitive job description. Repeating these policies strengthens the effectiveness of future approaches. In addition, publicly disclosing attackers may have a negative impact on policy performance. Responsibility for such decisions must be informed by the development of a truly strong organization. Ultimately, methods can be critical in detecting real attacks when creating valid values. In this study, we will explore strategies to classify these organisms without being criticized by any government policy or attack policy.

2.2 SECURITY MECHANISM

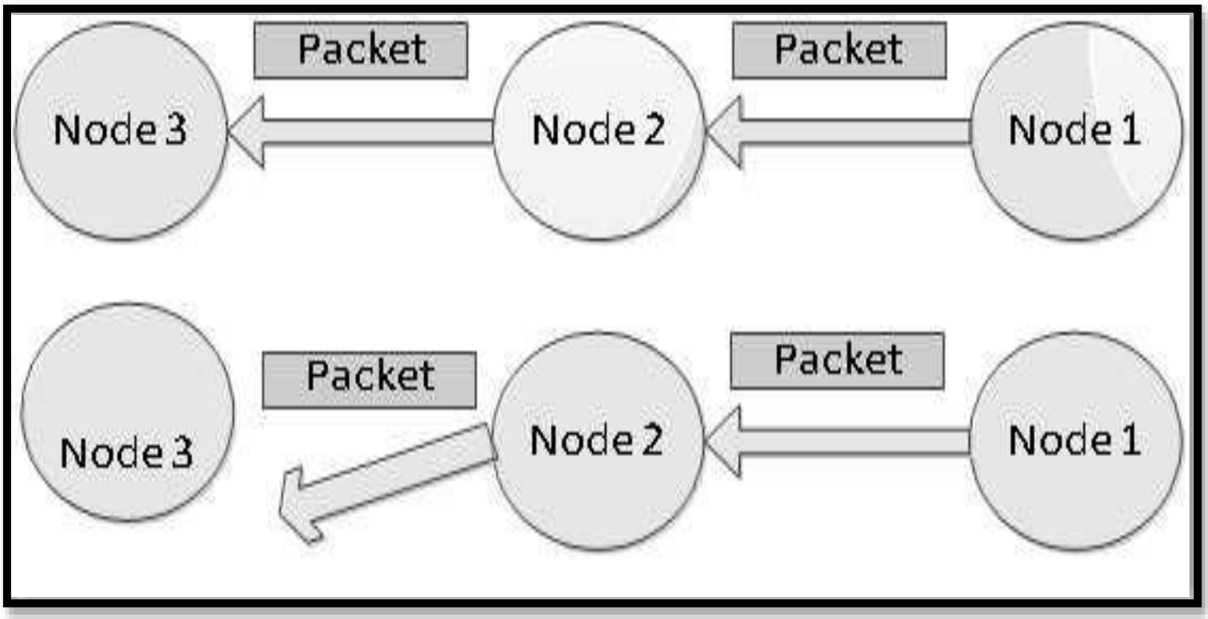
In this section we describe the security mechanisms and the architecture at different protocol layers.

2.2.1 Physical Layer

Security issues are often in the listening system. Features such as the distribution point, the received signal strength, can be used to detect attackers in this layer. Localization techniques can be used to determine the location of CR users in the system. There are many different ways to do things in this area. To the level used to calculate the position change during the signal transit from the source. Start counting the total number of hops in the free home repair system and change the body distance. The same applies to determining whether it transmits the received signal strength. Knowledge and signal strength are used together to find a helper in practice. Two RSS developed schemes are used to find the originator: the default measurement (TRT), the difference difference (DDT) The host MAC address is visible in this layer. Each channel has its own distribution system. The impact of additional actions if the enemy does not follow their plan. Also, the package size is taken into account. If the packet rate is high and long, there are opportunities for some extraordinary work.

2.2.2 SystemLayer

Path details can be encrypted using cryptographic names and authentication to verify the validity of routing tables and local identifiers. A watchdog program can be used to track data packets passing through the system (Zhang and Li, 2010). For example, fig. 3.5 shows normal and abnormal behavior in the system layer. In the context of normal behavior, the packet is routed to node 1 and node 3. In an abnormal behavior, node 2 acts as a malicious environment, that is, it changes the contents of the packet or frees the packet. Clock is used to enter illegal food packets at the time of clock feedback 1. After receiving the package, node 3 compares it to a buffer. If there is a difference, it is considered an undesirable task and limited to the development of the concept



<u>Figure 2.2</u>: Intrusion Detection at system layer

2.2.2 TransportLayer

Cycle time and transfer number are considered. If there is a high likelihood of a return or if the return period exceeds the normal value, we can say that there is something unusual in the system. An access control system based on the availability of RSS and RTT can be used to detect attacks in this framework

2.2.3 Application Layer

Since the function of some ethical layers affects each other, many of the layers of ethics in this layer can be viewed or explored. For example, if an application makes a lot of connections without actual functionality, such an unusual functionality is straightforwardly institute in the application layer

2.3 System Model ofCRN

The following considerations have been made for this computer model. The program contains malicious users and is powered by PowerPa. The distance between the main exchange and all users is DP and Power Bandit. The second user level is in the middle. Risk users are evenly distributed in the R-shaped region and are statistically independent. All users know and resolve the original referral links (RT,) (pt). Transmitters and bad users will damage the transmission line and use it normally. The preferred part of the conversion from the primary transfer is Part 2 and Bad Users 4. Radius Circle R0 is not a malicious user, it is called the private radius of the second user. There is no relationship between the secondary users.

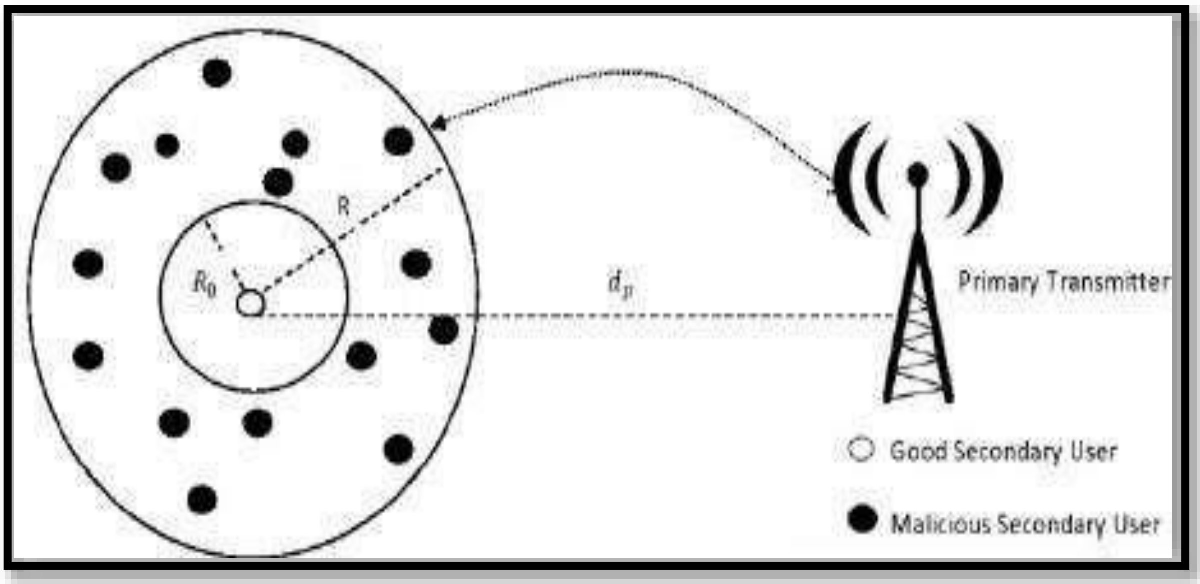


Figure 2.3: System model

2.3.1 LogicalArchetypal

The design of the conventionalsign at the subordinateoperatorowing to broadcast by the prime and the malevolentoperator is completedtowardsdiscovery out likelihoodconcentration function. We ponder, M malevolentoperators at (rj, θj). 1≤ j ≤M. The PDF of ri is assumedas per

$$P(r_j)=\frac{2r_j}{R^2-R^2_{0}}$$

θj remainsconsistentlydispersed in (π, π)). The control that the subordinateoperatorsacceptaftermainspreaderstands,

$$P^P_r = P_t d^{-2}_P G^2_P$$

where,

$$G^2_{□}=10^{\frac{sp}{10}}$$

Meanwhile P_t and $d_p$are secure the chance density function of p is r

$$P_{pr}y = \frac{1}{yA\sigma p\ (2\pi^{0.5})}$$

$$\frac{\mathbf{exp\ (10\ log\ 10}\ \gamma-\ \mu p\mathbf{)}^{2}}{{}^{2}_{P}}$$

2 σ

where A = $\frac{ln^{10}}{10}$ **and**

$\mu_p = 10 \log_{10} P_t - 20 \log_{10} d_p$

The wholeestablished power at the subordinatemanipulator from all the malevolent users is assumed by,

$Pm = P_r\, d_j{-}4G_j^2$

D_j stands the aloofnessamid the jth malevolentoperatorbesides the subordinateoperator.
G_j^2 is the scrutinyamongst the jth malevolentoperator and the subordinatemanipulator.

2.4 SECURITY IN WIRLESS SENSOR SYSTEMS USINGLIGHTWEIGHT CRYPTOGRAPHY

Lightweight Cryptography (LWC) is an emerging field that combines computer science, cryptography and electrical engineering with the goal of providing the environment with the required level of protection with limited power and computational capabilities.
Below, we review the type of attacks that occur on WSNs.

i. **Eavesdropping:** Passive attack that violates user privacy by attackers looking at confidential data. WSNs are vulnerable to this because most communication channels transmit data through sensor systems

ii. **Compromised-key attack:** An invader accesses a private key known as a compromise key to isolate information sent to the computer to encrypt and transfer personal data. Debug using the key to get the key.

iii. **Man-in-the-MiddleMITMAttack:**Direct and aggressive attack, which threatens the stability of WSNs by blocking data flows transmitted across communication channels and tampering with messages sent to the operator.

iv. **Jamming Attack**is when wireless communiquéconduits that conductinformationas ofinstruments to the supervisor are congested to depreciateorganizationcompetencethen operability thoughpermittingextraoccurrencesnear slip overbesidesoriginsupplementaryturbulences andmutilation.

v. **Replay Attack**is aorganizationoutbreak in which adequate and actualstatistics are retransmitted recurrently or overdueaimed atmalevolentdrives

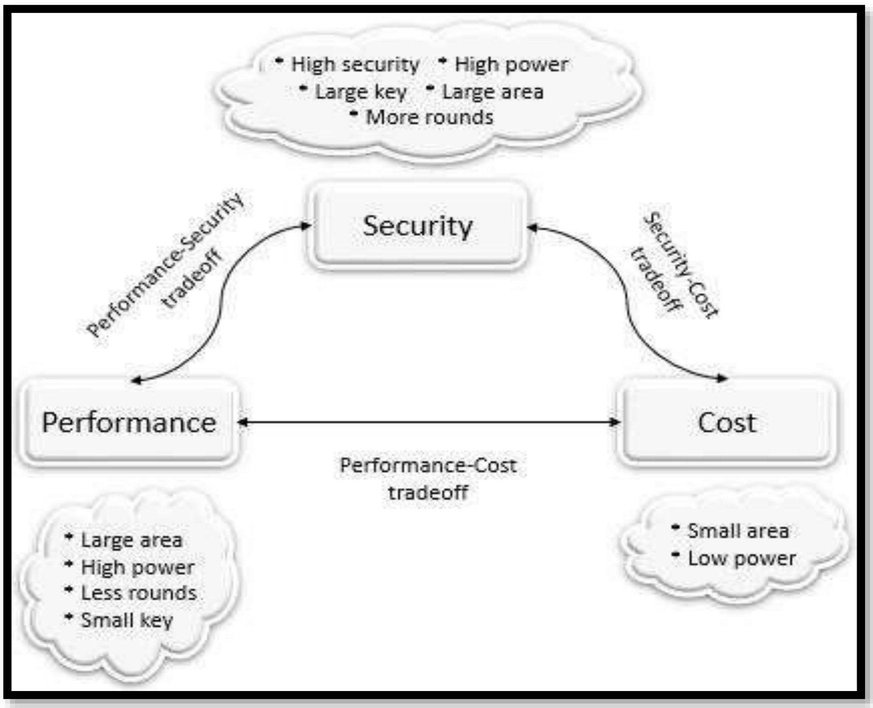


Figure 2.4: Illustration of Playback Attack

Light cryptography denotestoward a conventional of cryptographic symmetric besidesunequalproceduresintended to safeguardpassablesafety in schemesbyexactlimits to the setting and vigorskills such by way of WNS. Cryptography's light mass is attainedon the ironwarethensoftware programequal, anywheremark size, ironware level, cypherscope, thenpackagedifficultyleftoverscast-off to amount the equal of optimization attainedthroughapplying LWC.

Unalike Encryption Methods:

- **AdvancedEncryptionStandard(AES):**It is a standard NIST module that uses 128 volumes and usage 256 bits, 192 bits or 128 bits of key size. You can write in 10, 12 or 14 cycles depending on the size of the installation. Each AES cycle takes four basic positions: SubBytes, Shift Arrays, Integrated Columns, and AddRoundKey. The arrival of bytes is assumed to be 4 x 4 metrics. The AES 128 light launch requires 3100 GE (correspondentgateway) and provides power up to 80 kb / s at 100 Hz. Though, the Man-in-the-Middle (MIDM) outbreak is motionless a slight AES.

- **DESLX:**There is a lightweight DES (Light Encryption Standard) operating on 64 volumes using 184-bit keys. Encryption by means of DESLX is done in 16 cycles. Important modifications in the standard DES are used to achieve the appearance of a lightweight DESLX, that is, use an S box in its dwelling of eight S cases, and a white gate to enter double XOR gateways in the structure: one for the road and one for the members. This modest DES execution requires 2168 GE (correspondentgateway) and provides 44.4 Kb / s of power at 100 KHz. DES attacks are not a threat to DESLX because the S-box features rummage-sale in DSLX are unalikeafter the DES S-Box geographies.

- **High Security and Lightweight HIGHT:** Light Block Cipher activates on a 64 -bit block by means of a 128-bit key, engendered by encryption and decryption, and using the GFS architecture. Encryption is completedby 32 rounds by means of HIGHT. This lightweight implementation requires 3048 GE (gate equivalent) and provides 18 kb / s throughput on 100 kHz supremacy. This block staysdefenseless to cipher inundation.

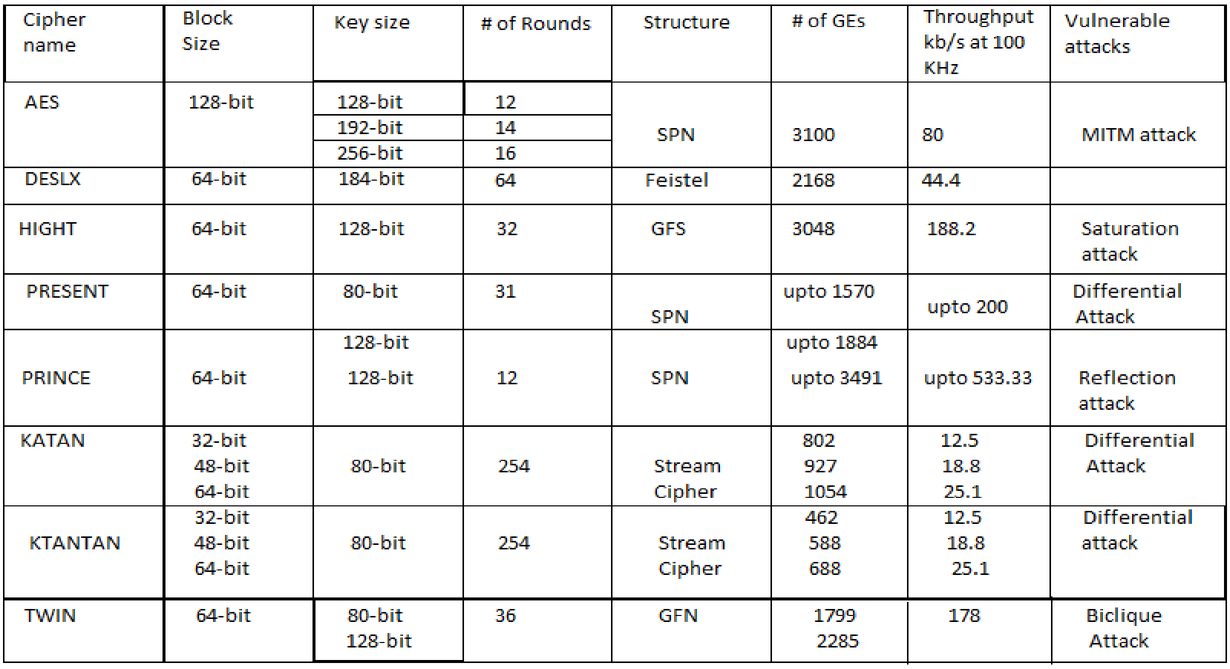
- **PRESENT:**It is an ultra-lightweight cryptographic algorithm that works proceeding 64-bit blocks using 80 bit or 128-bit key sizes. Encryption takes place in 32 rounds using PRESENT. The re-layer establishment layer of the SPN currently uses a 4 bit S-box aimed atinvolvement and yield. This slabcodestandsrecognizedaimed on the tallnear of safety and simplicity it provides. When using 80-bit keys, the 1570 GE (gate equivalent) and 128-bit keys require a current of up to 1884 GE and provides activenear200 Kb / s of control at 100 KHz. Remainspresently in the grasp of a disparityoutbreak

- **KATAN and KTANTAN:**These standrivuletcodeswhich work in 32-bit, 48-bit or 64-bit size-blocks, and both use an 80-bit key. Encryption by KATAN and KTANTAN takes place in 254 rounds. The main difference between the designs is that the kitten requires half of the gate block replicas required for hardware execution with all block sizes. For 32-bit size blocks, Caiton needs 462 EG, while Cotton requires 802 EG. For a 48-bit size block, Kaiton needs 588 EG, and Caton needs 927 EG. Finally, for a 64-bit size block, Kaiton needs 688 EG, and Caton needs 1054 EG. When encrypting 32, bit, 48-bit and 64-bit size blocks, KATAN and KTANTAN provide outputs of 12.5, 18.8 and 25.1 for Kb / s at 100 KHz power. Both ciphers are vulnerable to differential attack.

- **PRINCE:**Insubstantialcodesrecognizeddesigned for using the light-reflectance property: encryption and decryption are the same, but each use a different key to reduce design requirements [32]. This cipher works in a 64-bit size block using the 128-bit key and uses the SPN architecture. Encryption by PRINCE takes place in 12 rounds. Currently requires up to 3491 GE (gate equivalent) and provides up to 533.3 Kb / s with 100 KHz power. PRINCE is under attack by reflection.

- **Elliptic Curve Cryptography ECC:**Lightweight ECC is measured the utmost efficient public key method because it requires low power consumption, a small area, and low clock cycles. It is based on the algebraic system and uses the smallest keys generated using the discrete algorithm. Several customized implementations for mild ECC have been proposed. Most designs do not require less than 10000 GE. Five operations are given in the main field arithmetic: multiplication, addition, subtraction, trade and subtraction. Multiplying is very possible for these tasks, reducing the complexity of the operation because it can be run up to 30 k GE. Optimization by adding for bit shifting and multiplication rather than using a microprocessor.

- **RSA:** A resource-hungry slant that ensuresnot work much for light optimization. RSA trusts on pickingdoublebigkeyfacts to discoveryhiscommunitythensecludedsolutions, which remainclassicallyflanked by 1024 and 4096 jiffs. Irregular cryptographic old-styletacticsremaintranquilnonexpectantaimed atpawnssince the effectiveness of execution of somewhat of the futureenactments is nonoptimum.



Cipher name	Block Size	Key size	# of Rounds	Structure	# of GEs	Throughput kb/s at 100 KHz	Vulnerable attacks
AES	128-bit	128-bit 192-bit 256-bit	12 14 16	SPN	3100	80	MITM attack
DESLX	64-bit	184-bit	64	Feistel	2168	44.4	
HIGHT	64-bit	128-bit	32	GFS	3048	188.2	Saturation attack
PRESENT	64-bit	80-bit	31	SPN	upto 1570	upto 200	Differential Attack
PRINCE	64-bit	128-bit 128-bit	12	SPN	upto 1884 upto 3491	upto 533.33	Reflection attack
KATAN	32-bit 48-bit 64-bit	80-bit	254	Stream Cipher	802 927 1054	12.5 18.8 25.1	Differential Attack
KTANTAN	32-bit 48-bit 64-bit	80-bit	254	Stream Cipher	462 588 688	12.5 18.8 25.1	Differential attack
TWIN	64-bit	80-bit 128-bit	36	GFN	1799 2285	178	Biclique Attack

Table 2.1: Different Encryption Techniques

2.5 PLANNEDSAFETYALGORITHM

In our planned structure, we analyze the faith of the primary user and the malevolent user. A high-risk user with a misalignment can perform healthier as a chief user and can deliver untruthful info to a additional user in relation to physical objects that cause significant disruption and limited use. Our supply warranty system is based on two parameters -

1. Distance
2. Received signal powerlevel

Cognitive radio (CR) operatorpartakes the competence to intelligence the mainoperatorsite. Mainmanipulatorshows the positiondata to altogether CR operators. A CR operatortotals the aloofnessamongst the subordinateoperatorthen the chiefoperatororiginatedhappening the numerouslimits. Associate this intendedaloofnessthroughdissimilartechnique (Receivedsignalpowerlevel). Uncertaintyaloofness is competitionformerlyauthenticate that propagatorisaauthenticoperatoror elsemalevolentoperator.(Figure3),demonstrationsthecorroborationprogression of the mainoperator and malevolentoperator.

A. Distance Calculate Based on the Location Coordinate

Detachmentamong the operator'stinstandplannedscheduled the foundation of the PlaceSynchronize. Contemplate the (x, y, z) is x, y and z synchronize of the cerebraloperator and (x_1, y_1, z_1) is x, y besidesz coordinate of the chiefmanipulator. Detachmentamongst the cerebralmanipulatorthen the chiefoperatortin be premeditated Distpr by means ofsubsequentcalculation-

$$\mathbf{Distpr=\{(x- x_1)^2+(y-y_1)^2+(z-z_1)^2 \}} \qquad \textbf{(i)}$$

B. Distance Calculate Based on the Received Signal Power Level

Computeestablishedsignauthority level by the receivingcrossarranged the foundation of gettingsignbesides the communicated signal on the receivinglateral. The acknowledgedsignauthority Pr is unhurriedthrough the subsequentcalculation-

$$\boldsymbol{P_r= \frac{PtGtGrh_t^2h_r^2}{d^4L}} \qquad \textbf{(ii)}$$

Where $\mathbf{P_t}$ = Transmit power level

$\mathbf{h_t}$ = Height ofatransmitter

$\mathbf{h_r}$= Height of receiver

$\mathbf{tt_t}$ = Transmitter antenna gain

$\mathbf{tt_r}$= Receiver antenna gain

L =System loss factor

Contemplate h_t, h_r, tt_t, tt_r and L remaincontinuousthenlike to 1. Consequently, the establishedsupremacy level resolvebe contingentscheduled the conveyauthorityclose and aloofness:

$$\boldsymbol{Pr}=\frac{\boldsymbol{Pt}}{\boldsymbol{d^4}}$$

Deliberate the communicatesupremacy level, P_t is accord. Grounded on conventionalinfluence level, the aloofnessamongst the operatorsremainsassumedthrough:

Dist= ______ **(iii)**

$$\mathbf{0.25}^{\mathbf{1}(\boldsymbol{Pr})^\wedge}$$

Hence, distance between the user can be estimated based on the received power level, given the transmit power level is known.

Tocalculatethetrustworthinessoftheuser,Ifthedistancecalculatedbyusingthecoordinates matches the distance calculated with received power level, Then the user can be considered trustworthy or vice versa. We define the relative trustworthiness of a user, Y,as:

Y = min (Distpr/Distms, Distms/Distpr) (iv)

Where, **Distpr** = Planned Distance of PrimeOperator

Distms = Planned Distance of MalevolentEmployerAloofnessconsideredperestablished ower equalmightnow be actualprecise; approximatelyracketgestureincreasesthrough the communicatedsign. Aloofnesscomputesthroughtogether of the techniqueoughtto originateadjacent and equivalent. We suppose the faithprinciplestowards be near or identical to 100 % aimed atdependableoperators. Likewise, we imagine the faithrate to remainlittleaimed atdishonestworkers.

CHAPTER-3

PERFORMANCE ANALYSIS OF BASE ARTICLE

3.1 System Model/System Model

We have considered a vehicular system where cognitive and certified users exist together within the same region similar to one shown in the figure 1. Cognitive system is an infrastructure where every cell has a certain number of associated SVUs and a fusion center or base station. Each SVU access the vacant PU channel and each SVU send its information to FC and FC sends a combined decision back to that cell. Each SVU follows Poisson Distribution. All the vehicles move independent of each other. Hence, all sensing channels between SVU's and PU's are independent of each other.

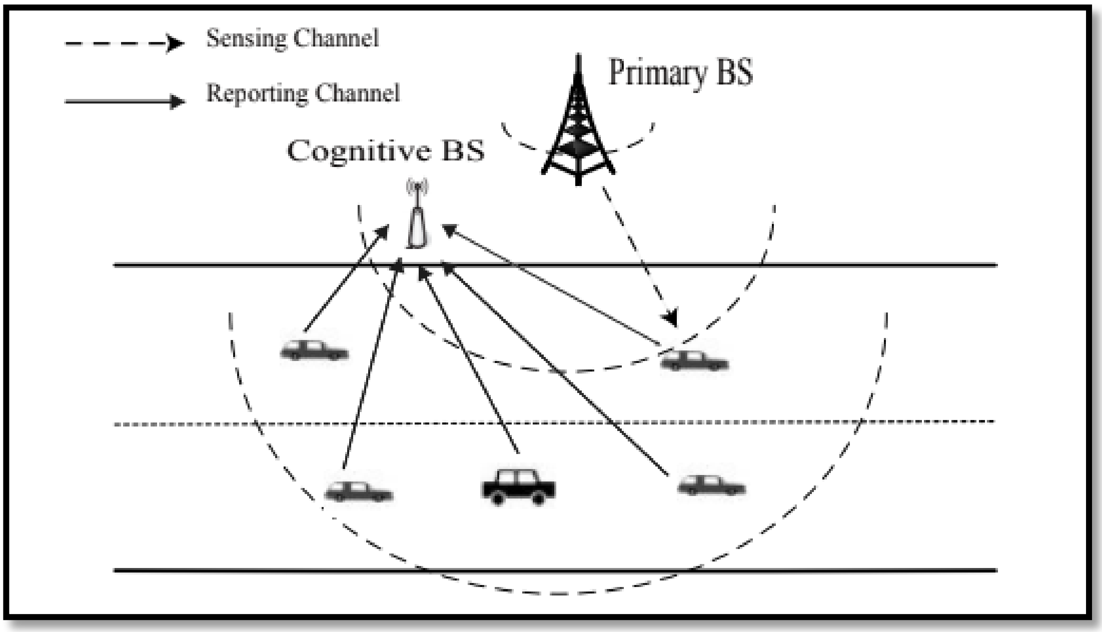


Figure 3.1: System Model

3.2 Sensing Model

Binary Hypothesis Detection is used in Spectrum Sensing, with H (0) and H1(1) as two Hypotheseswhich are associated with absence and presence of PU respectively.

Let N be the number of SVUs and L be number of Sampling observations. Two hypotheses associated can be expressed as:

$$\mathbf{x_i(k)} = \mathbf{(i)} \quad \begin{cases} \mathbf{n_i(k)} & \mathbf{H_0} \\ \mathbf{h_i(k)s(k)+n_i(k)} & \mathbf{H_1} \end{cases}$$

In above equation, $x_i(k)$ is the establishedsign by i th SVU, s(k) can be expressed as the signal received from PU, h_i (k) is the channel coefficient between SVU and PU and n_i (k) remains the multifacetedpreservativesnowy gaussian sound (AWGN) which has uncaring equal to nothing and modification σ n 2 . All s(k), h_i (k) and n_i (k) are independent of one another [6].

Every SVU will make a binary decision $u_i = q\ (x_i) \in +1, -1$ with P f_i (Probability of false alarm) and P m_i (Probability of miss detection) and then, these decisions are sent to Fusion Center (FC) via Rayleigh Fading Channel. Observation from i th SVU at Fusion Center can be expressed as:

$$\mathbf{Z_i = g_i u_i + w_{ir} \quad (ii)}$$

In above equation, w_i is zero mean gaussian random variable with δ_i^2 as variance and g_i as fading gain of channel from SVU to Fusion Center [7].

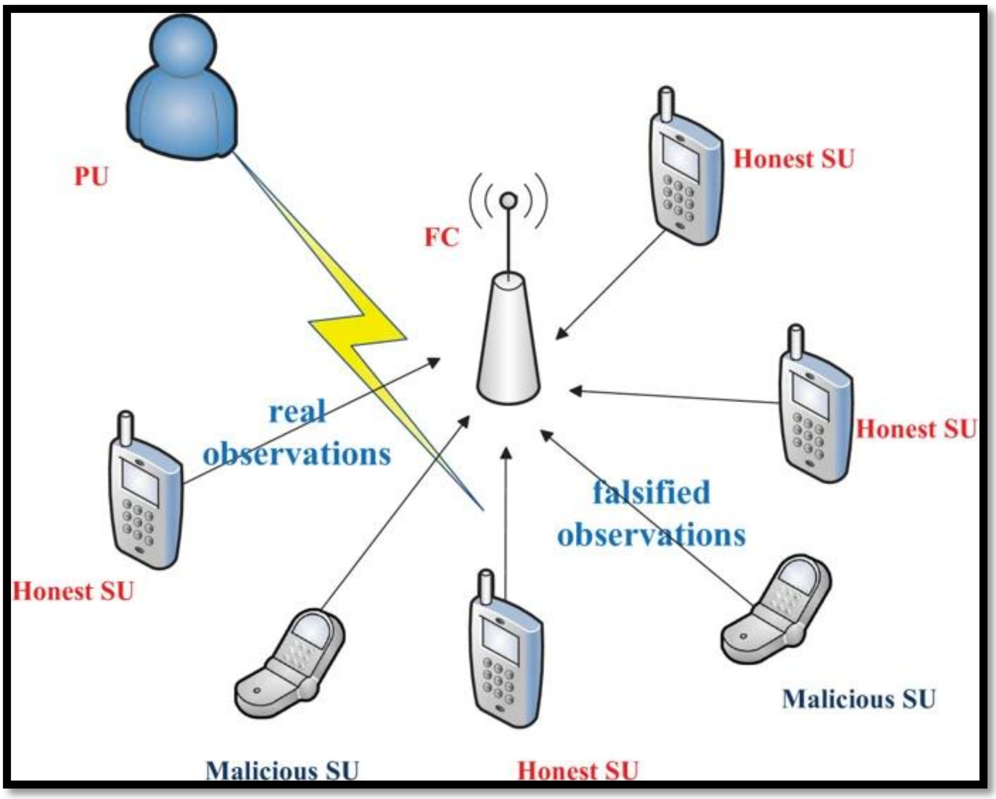


Fig 3.2: Frequency Allocation

3.3 Local Sensing with Energy Detection

Energy Detection is commonly used spectrum sensing technique for local sensing. Also, energydetection is the most suitable option for vehicular systems because of its low latency tolerance and environment with high mobility.

Energy Statistic associated with i th SVU is denoted by e_i:

$$\mathbf{e_i = \sum_{k=0}^{L-1} |x_i(k)|^2} \qquad \textbf{(iii)}$$

In above equation, L represents Quantity of examplesinside a distinguishingintermission. e_i represents the quantity ofsquares of L gaussian random Variables. follows central chi square

$$\mathbf{\frac{e_i}{\sigma^2_n}} \qquad \textbf{(iv)}$$

Distribution with L degrees of freedom and parameter η(i).VerdictRegulation at apiece SVU can be expresses by way of:

$$\mathbf{u_i} = \begin{cases} \mathbf{+1,} & \mathbf{if\ e_i \geq \lambda} \\ \mathbf{-1,} & \mathbf{if\ e_i < \lambda} \end{cases} \qquad \textbf{(v)}$$

In above equation, +1 denotes that PU Signal is detected, and -1 denotes that PU sign is nonnoticed. Once L remainsadequatelybig, the vigor statistic tin be labelledthrough a Gaussian circulationlowermutuallypremises H_0 and H_1 [22]. Lease threshold be λ.

3.4 Probability of False Alarm

Probability of False Alarm(P_f) can be represented in terms of ratio of incomplete and complete gamma function.

$$\mathbf{P_{f} = P_{r}\,(e_{i} \geq \lambda|H_{0}) = \frac{\Gamma(u, \frac{\lambda}{2})}{\Gamma(u)}} \qquad \textbf{(vi)}$$

Where $\Gamma(u, \frac{\lambda}{2}) = \int_{x}^{\infty} t^{(u-1)}\, e^{-t} dt$ **and** $\Gamma(u) = \int_{0}^{\infty} t^{(u-1)}\, e^{-t} dt$

Thus, P_f can remainassumed as:

$$\mathbf{P_{f} = \frac{\int_{x}^{\infty} t^{(u-1)}\, e^{-t} dt}{\int_{0}^{\infty} t^{(u-1)}\, e^{-t} dt}} \qquad \textbf{(vii)}$$

Where u is time – bandwidth product.

Thus, Probability of False Alarmcan remainassumed as:

$$\mathbf{P_{f} = P_{r}\,(e_{i} \geq \lambda|H_{0}) = Q\,\left(\frac{\lambda - L\sigma^{2}}{\sqrt{\sigma^{2}}}\right)} \qquad \textbf{(viii)}$$

3.5 Probability of Detection

Probability of Detectioncan remainassumedby way ofuth order Marcum-Q function with parameters γ and λ where γ represents SNR and λ represents threshold value.

$$\mathbf{P_{d} = Q_{u}\,(\sqrt{2\gamma}, \gamma)} \qquad \textbf{(ix)}$$

uth order Marcum-Q function can be expressed as:

$$\mathbf{Q_{m}\,(a, b) = \frac{1}{2\pi j} \oint_{r} \frac{e^{g(z)}}{z^{m}(1-z)} dz} \qquad \textbf{(x)}$$

Where $\mathbf{g(z)} = \frac{a^2}{2}\left[\frac{1}{z} - 1\right] + \frac{b^2(z-1)}{2}$

Here, $\mathbf{a} = \sqrt{2\gamma}$ **and b**= $\sqrt{\gamma}$

Thus:

$$\mathbf{g(z)} = \frac{\sqrt{2y^2}}{2}\left[\frac{1}{z} - 1\right] + \frac{\sqrt{\lambda}^2\,(z-1)}{2}$$

$$\mathbf{g(z)} = \gamma\left[\frac{1}{z} - 1\right] + \frac{\lambda}{2}\mathbf{(z\text{-}1)} \qquad \mathbf{(xi)}$$

Thus, Probability of detection can be expressed as:

$$\mathbf{P_d} = \frac{1}{2\pi j}\oint_{\Omega} \frac{e^{\left(\frac{1}{z}-1\right)\gamma+\frac{\lambda}{2}(z-1)}}{z^u(1-z)}\,dz \qquad \mathbf{(xii)}$$

$$\mathbf{P_d} = \frac{e^{\frac{-\lambda}{2}}}{2\pi j}\oint_{\Omega} \frac{e^{\left(\frac{1}{z}-1\right)\gamma+\frac{\lambda}{2}(z-1)}}{z^u(1-z)}\,dz \qquad \mathbf{(xiii)}$$

Where w is circular contour of radius r Ɛ [0,1]

Thus, P_d can be given as:

$$\mathbf{P_d = Q\ (\frac{L+n_i)_n^2-\lambda}{\sqrt{(L+2\eta)^2}})} \qquad \textbf{(xiv)}$$

3.6 Probability of Miss-Detection

Probability of Miss-Detection(P_m) can be given as: 1 – $P_{(d)}$:

3.7 Cooperative Sensing

In Cooperative Sensing, numerous SVUs at dissimilarplacesremainexploitedbesidesformerly their self-governing sensing communications are mutualhooked on one combinedchoice which expresses us around the presence of PU.

To combine these independent sensing messages, we use hard fusion.

As mentioned earlier, Observation from i th SVU at UnionEpicenter canremainarticulatedby way of:

$$\mathbf{z_{(i)} = g_{(I)} u_{(i)} + w_{(i)},} \qquad \textbf{(xv)}$$

Lease $v_i$mean the decipheredkind of z(i) aimed at i(th) SVU next toUnion Center and the interpretingregulation can articulatedby means of:

$$\mathbf{v_i = \begin{cases} 1, & \text{if } z_i \geq \lambda \\ 0, & \text{if } z_i < \lambda \end{cases}} \qquad \textbf{(xvi)}$$

Let E[x] represent the equation:

$$E\,[v_i \,|\, H_j] = P\,(v_{i\,=}\,1|\,H_j).\,1 + P\,(v_{i\,=}\,0|\,H_j).\,0 \quad \text{(xvii)}$$

$$E\,[v_i \,|\, H_j] = P\,(z_i \geq 0|H_j)$$

Let D[x] represent the variance:

$$D\,[v_i \,|\, H_j] = E\,[v_i^2|\,H_j] - E\,[v_i \,|\, H_j]^2 \quad \text{(xviii)}$$

$$D\,[v_i \,|\, H_j] = P\,(z_i \geq 0|H_j) - P\,((z_i \geq 0|H_j))^2$$

$v_{(i)}$ is unswervinglyreliant on on P ($z_{(i)} \geq 0|$ $H_{(j)}$) which remainsalike to probability of Miss-DetectionandProbability of False Alarmin Local Sensing. Beneath the proposition $H_{(0)}$ and $H_{(1)}$, u(i) trails the circulationthroughlimitations $P_{(fi)}$ and $P_{(di)}$:

$$P\,(u_i|H_0) = \begin{cases} P_{fi}, & \text{if } u_i = +1 \\ 1 \;\; - P_{fi}, & \text{if } u_i = -1 \end{cases} \quad \text{(xix)}$$

$$P\,(u_i|H_1) = \begin{cases} P_{di}, & \text{if } u_i = +1 \\ 1 - P_{di}, & \text{if } u_i = -1 \end{cases} \quad \text{(xx)}$$

Let P_{fi} be Probability of False Alarmand can be voicedby way of:

$$P_{(Fi)} = f\,(z_i \geq 0 \,|\, H_0) = \sum_{u_i \in \{-1,+1\}} f(z_i \geq 0|u_i)P(u_i|H_0) \qquad \textbf{(xxi)}$$

$$P_{(Fi)} = f\,(z_i \geq 0 \,|\, u_i = +1)\, P_{fi} + f(z_i \geq 0|u_i = -1)(1 - P_{fi})$$

Let P_{Di} be Probability of False Alarmand can be statedby means of:

$$P_{Di} = f\,(z_i \geq 0 \,|\, H_1) = \sum_{u_i \in \{-1,+1\}} f(z_i \geq 0|u_i)P(u_i|H_1) \qquad \textbf{(xxii)}$$

$$P_{Di}= f\,(z_i \geq 0 \,|\, u_i = +1)\, P_{di} + f(z_i \geq 0|u_i = -1)(1 - P_{di})$$

Local Probability of False Alarmand Local Probability of Detectionand Probability of Miss-Detectionis articulatedby way of:

$$\mathbf{P_{Fi}} = \frac{1}{2} + \left(P_{fi} - \frac{1}{2}\right).\sqrt{\frac{\gamma_i}{2+\gamma_i}} \qquad \textbf{(xxiii)}$$

$$\mathbf{P_{Di}} = \frac{1}{2} + \left(P_{di} - \frac{1}{2}\right).\sqrt{\frac{\gamma_i}{2+\gamma_i}} \qquad \textbf{(xxiv)}$$

$$\mathbf{P_{Fi}} = \frac{1}{2} + \left(P_{fi} - \frac{1}{2}\right).\sqrt{\frac{\gamma_i}{2+\gamma_i}} \qquad \textbf{(xxv)}$$

$$\mathbf{P_{Mi} = 1- P_{Di} =} \ \frac{1}{2} + \left(\boldsymbol{P_{mi}} - \frac{1}{2}\right) \cdot \sqrt{\frac{\gamma_i}{2+\gamma_i}} \qquad \textbf{(xxvi)}$$

3.8 Global Probability of false alarm and Miss Detection

We are assuming that each and every reporting channel do not interfere with one another. The fusion center decodes z $_i$ and gets v$_i$. Counting Rule is used to calculate the global statistic:

$$\mathbf{A} = \sum_{i=1}^{N} \boldsymbol{v_i} \qquad \textbf{(xxvii)}$$

At Fusion Center, the decision rule can be expressed as:

$$\mathbf{v_0} = \begin{cases} \mathbf{1} & \textbf{if} \quad \mathbf{A \geq T} \\ \mathbf{0} & \textbf{if} \quad \mathbf{A<T} \end{cases} \qquad \textbf{(xxviii)}$$

Let Q$_m$ and Q$_f$ be the global probability of miss-detection, global probability of false alarm and global probability of error be expressed as:

$$\mathbf{Q_f = Q} \left(\frac{T - \square}{\sqrt{\sigma^2}}\right) = \mathbf{Q}\left(\frac{T - \sum_{i=1}^{N} P_{Fi}}{\sqrt{\sum_{i=1}^{N} P_{Fi}(1-P_{Fi})}}\right) \qquad \textbf{(xxix)}$$

$$\mathbf{Q_m = Q} \left(\frac{\square - T}{\sqrt{\sigma^2}}\right) = \mathbf{Q}\left(\frac{\sum_{i=1}^{N} P_{Di} - T}{\sqrt{\sum_{i=1}^{N} P_{Fi}(1-P_{Di})}}\right) \qquad \textbf{(xxx)}$$

$$Q_e = Q_f + Q_m = Q\left(\frac{T - \sum_{i=1}^{N} P_{Fi}}{\sqrt{\sum_{i=1}^{N} P_{Fi}(1 - P_{Fi})}}\right) + Q\left(\frac{\sum_{i=1}^{N} P_{Di} - T}{\sqrt{\sum_{i=1}^{N} P_{Fi}(1 - P_{Di})}}\right) \qquad \text{(xxxi)}$$

CHAPTER-4

PERFORMANCE ANALYSIS OF NEW CONTRIBUTIONS

4.1 Analysis for time varying channel

Mobility is the biggest concern for vehicular wireless channel. Earlier for calculating the channel vector, we used the random Rayleigh fading channel and obtained the results and comparisons for probabilityof miss-detection. But in real life scenarios, due to temporal correlation, the sensing channel changes which results in changes in the detection at the SU. So, time varying channel should be introduced for sensing the spectrum information. For implementing this, we have used the Auto-Regressive model (AR Model) to describe our time varying channel [5]. (AR model is used for representing any time varying process in nature). AR Model uses the past data of channel (at previous time instances) tocalculate the channel vector for the current instance. And that instance of channel vector has been used for modelling to obtain the received signal and Probability of Miss-detection has been calculated for that canal.

The frequencytrajectory fork-th time promptstaysassumedby:

$$\mathbf{h_j(k) = p_j^{k-1} h_j\ (1) +} \sqrt{\boldsymbol{1 - p_j^2}}\ \boldsymbol{\sum_{t=1}^{k-1} p_j^{k-l-1} e_j(l)} \qquad \textbf{(i)}$$

Parameters:

$\mathbf{p_j = J_0}(\frac{\boldsymbol{2\pi f_c v_j}}{\boldsymbol{R_s c}})$is the correlation parameter, where J $_0$ (.) is the zeroth-order Bessel function of first kind.

$\mathbf{v_j}$ is the relative speed of j-th SVU.

$\mathbf{R_s}$is the transmission symbol rate.

$\mathbf{h_j}$ **(k)** is the channel component of j-th SVU at k-th instance.

$\mathbf{e_j\ (l) \sim C\ N\ (0, \sigma_e^2\ j)}$ represents time varying component of the channel [5].

We have compared the Pm vs SNR graph for time varying and time invariant channel. For any time, varying channel, Pm value for a fixed SNR should be more than that for time invariant channel [Refer section 4.3 for comparison result].

4.2 System model

In instruction to recover the application of spectrum possessions Co-operative RangeDetecting (CSS) Tactic is considered influentialinstrument. Nonethelessunique of the chiefdisadvantage of CSS remains that it mightshoulder that entirely the subordinate vehicles(SVU) are authentic which means that they doesn’t direct any kind of untruthfulinformation [4].Consequentlynow the chance is shapedaimed at the assailant to direct the untrueinformation to the synthesismidpoint(FC).Nonetheless to stop the fabrication of information, faithdevice is industrialized. Nonethelessapproximately of theassailant’scontainerconspirebyapieceadditionalthenprocedure a collusive faction which can evade the discovery of trust expedient. As informationtin be moreoveruntrue or truthful, we partakeplannedaarrangementsince the standpoint of XOR aloofnessinvestigation which can notice and evade the outbreak. Fusion center gathers the information of individual sensing of SVU, data reporting and data fusion. Firstly, each of the SVU sense the PU signal via sensing channel. After that each SVU send their data to the fusion center via reporting channel.

FC will have a database of all data sent from every SVU.Based on this, a simple ratio of credibility (correctly reported / Total Values) will be maintained of each SVU at the FC. As in Co-operative spectrum sensing a single SVU cannot change a FC’s decision individually. In order to change the FC decision, many SVU’s (attacker) would have to send same type of data, where as honest SVUs will not send same type of data. There will be some diversity in it. To exploit this diversity, we use calculationof XOR distance between each and every SVU. XOR distance is used because there are only 2 classes of data that is 0 and 1 and XOR is the best tool to measure difference between these classes. Both honest and malicious SVU may have higher trust value, but what separates them is XOR distance. Malicious SVU will have smaller XOR distance than Honest SVUs. After this operation, attacker SVU’s can be identified and their data won’t be considered in fusion process. Hence, decision won’t be affected.

4.3 Algorithm

- Algorithm to detect Attackers

```
for each i = 0 to n:
for each j = 0 t o n:
        xor matrix (j) = columni (xor) column2;
end
for t = 0 to k
sum(:) = sum(:) + k∗xor_matrix (t) // simultaneo usrow−updates
end
        x (i) = sum (:)         // simultaneous row−updates
end
```

As the xor distance will be very high in magnitude, we normalize it by max elementof the row. Therefore, the xor distance will be in range [0,1].

Both honest SVU and Attackers will have high credibility, therefore, we will distinguish those SVU which have higher ratio.

- Algorithm To remove attackers from current Fusion Process

```
for each i in n:
        ifratio> 0.6 and x (i)< 0.4
Label = Attacker;
discard data from fusion decision process.
end
```

CHAPTER-5

NUMERICAL RESULTS

5.1 Simulation Framework

The various controlling parameters are as follows:

1) For time varying simulation:

number of samples: 60

number of monte Carlo simulations = 10^5

Probability of false alarm Pf= 0.01

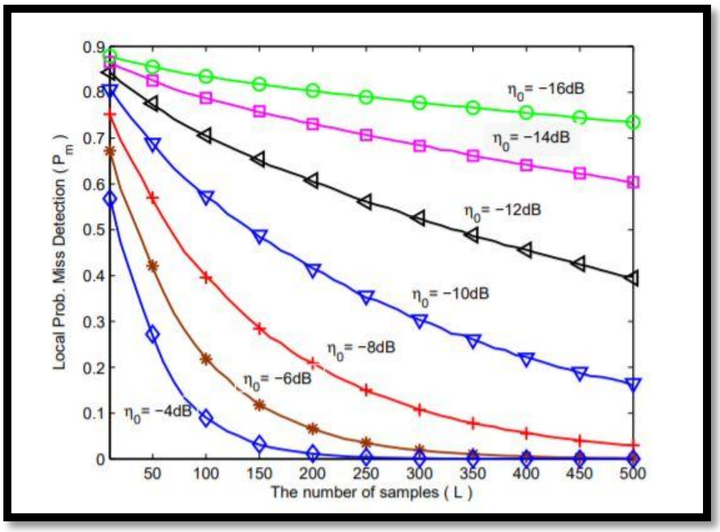
2) For SSDF attack simulation

number of SVU h = 40

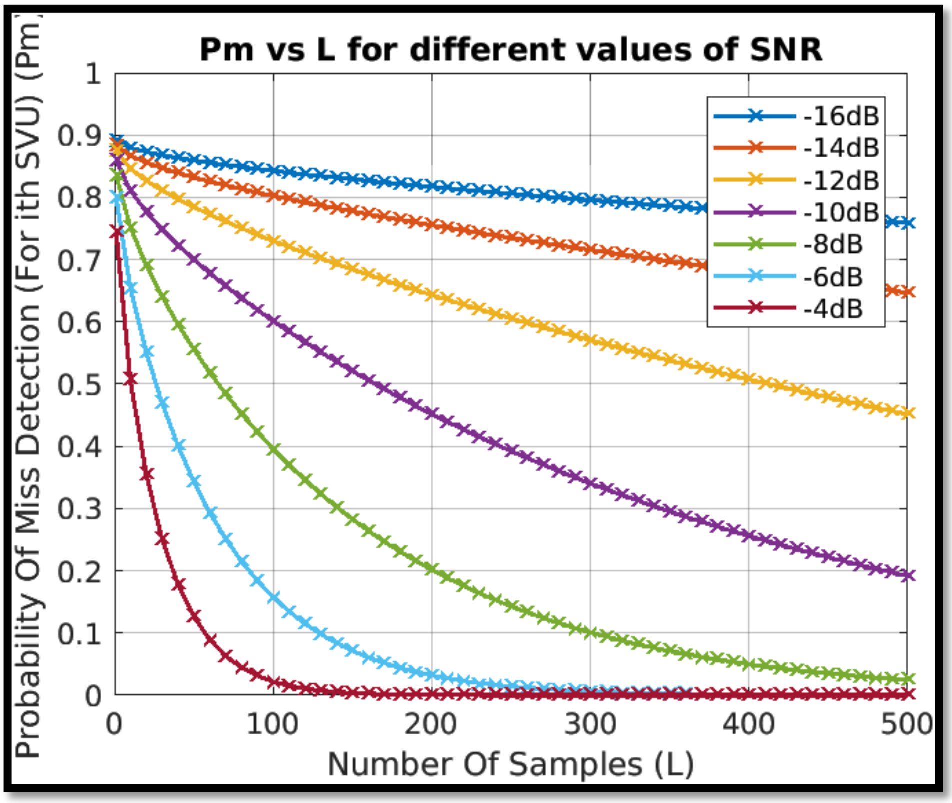
No. of truth values = any random value between 2000 and 4000

No. of false values = total - truth values.

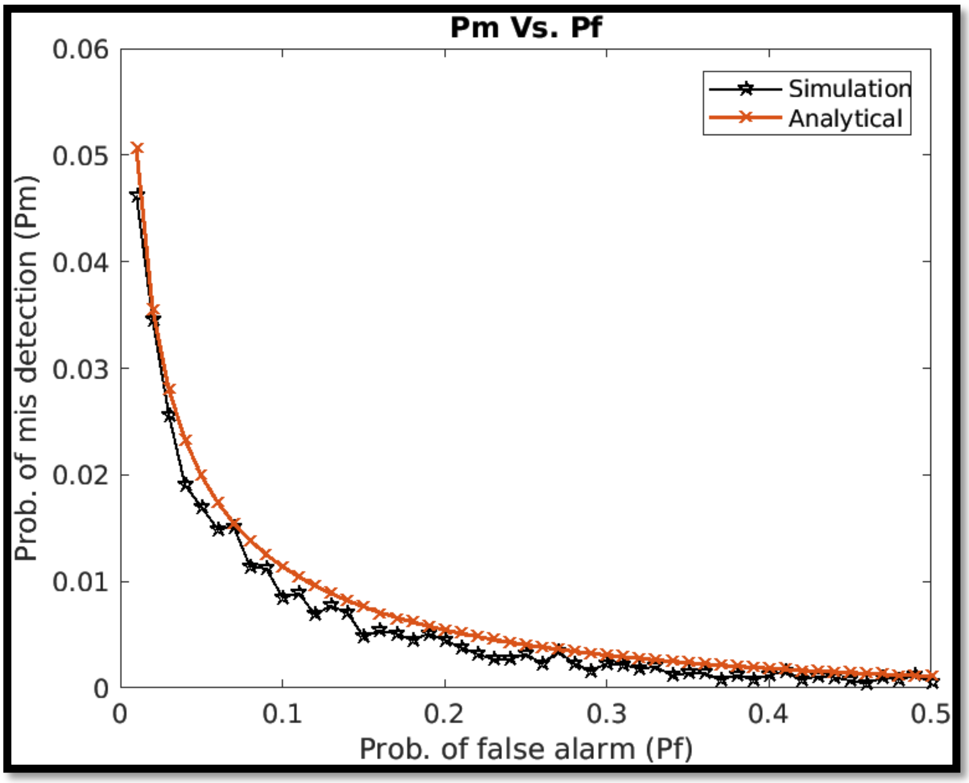
5.2 Reproduced Figures



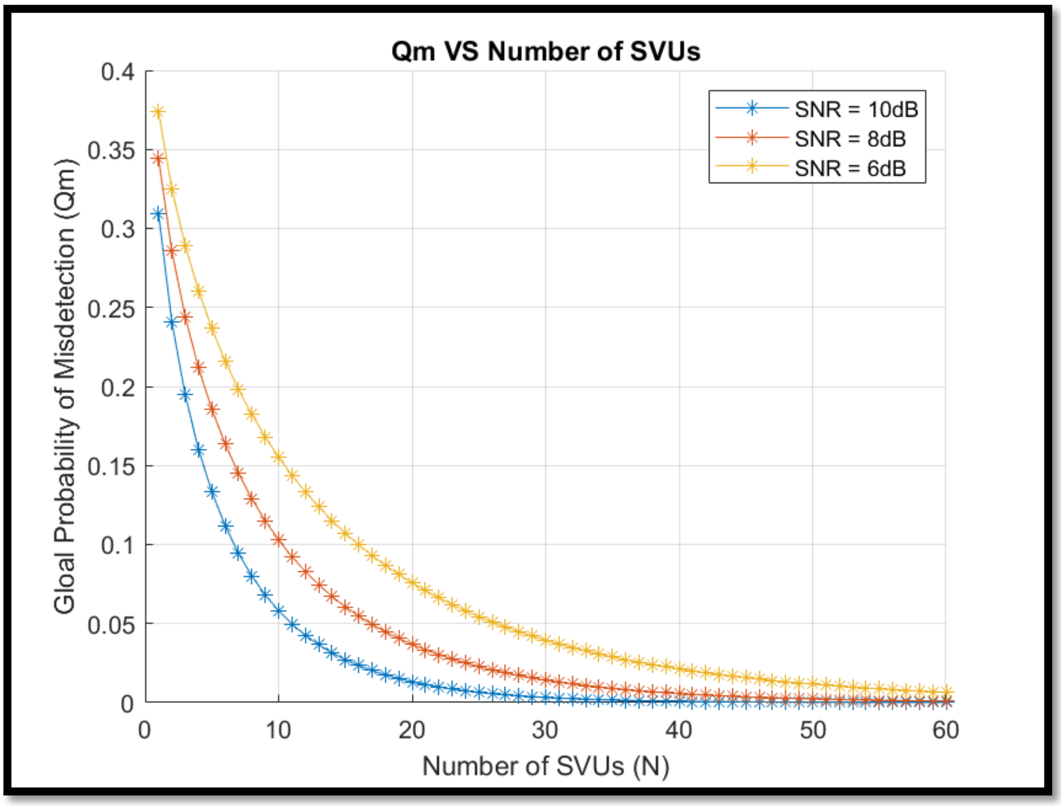
Graph5. 1: Local Probability Miss Detection v/s No. Of Samples taken



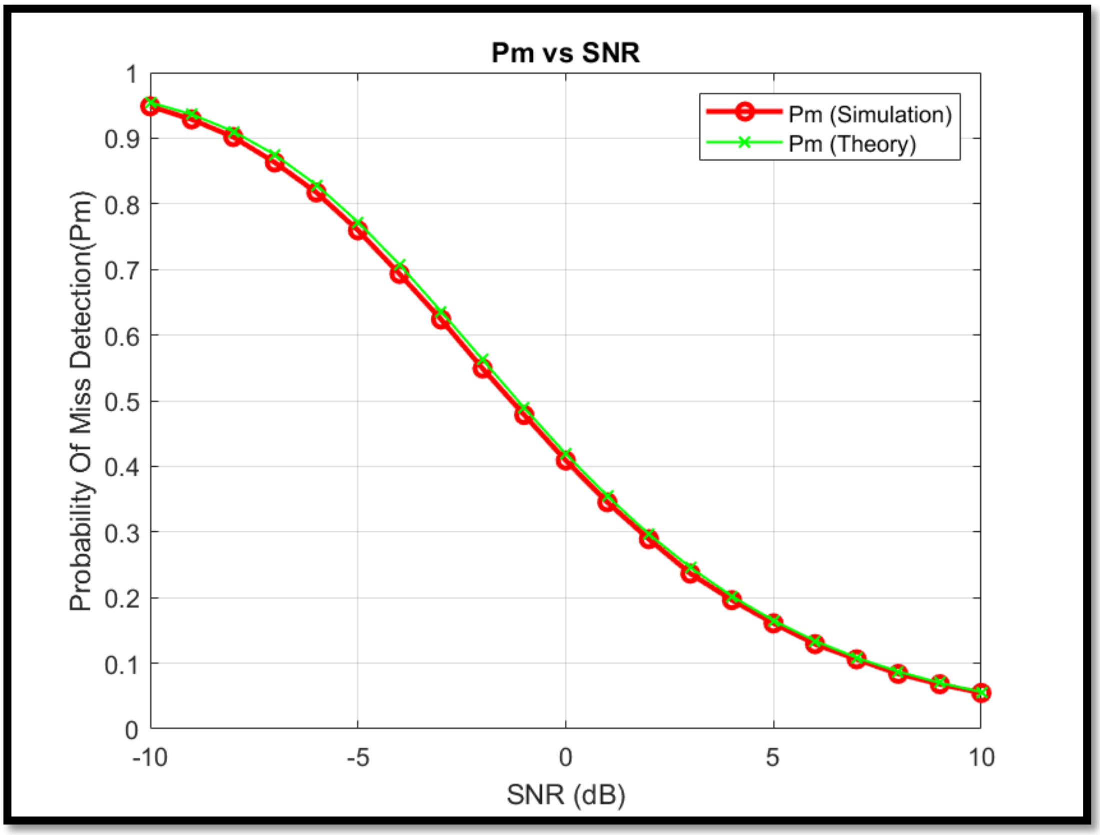
Graph 5.2: P_m v/s L (for various SNR values)



Graph 5. 3: P_m v/s P_f



Graph5.4: Q_m v/s Number of SVUs



Graph 5.5: P_m v/s SNR

- **P_m vs L:** For different SNR's, the local probability of Misdetection (Pm) has been calculated on basis of number of samples (L) in a particular sensing interval. This denotes the value of Pm for ith SVU (i.e. local probability). As the number of samples (L) increases, the value of Pm decreases gradually. Also, with increase in SNR values, Pm decreases.

• **P_m vs P_f Curve**: Graph of Probability of Misdetection vs Probability of false alarm has been shown in the given figure and comparison has been made between analytical and simulation results. For different values of Pf, and fixed value of SNR = -8db, Pm has been plotted. With the increase in Pf value, Pm gradually decreases.

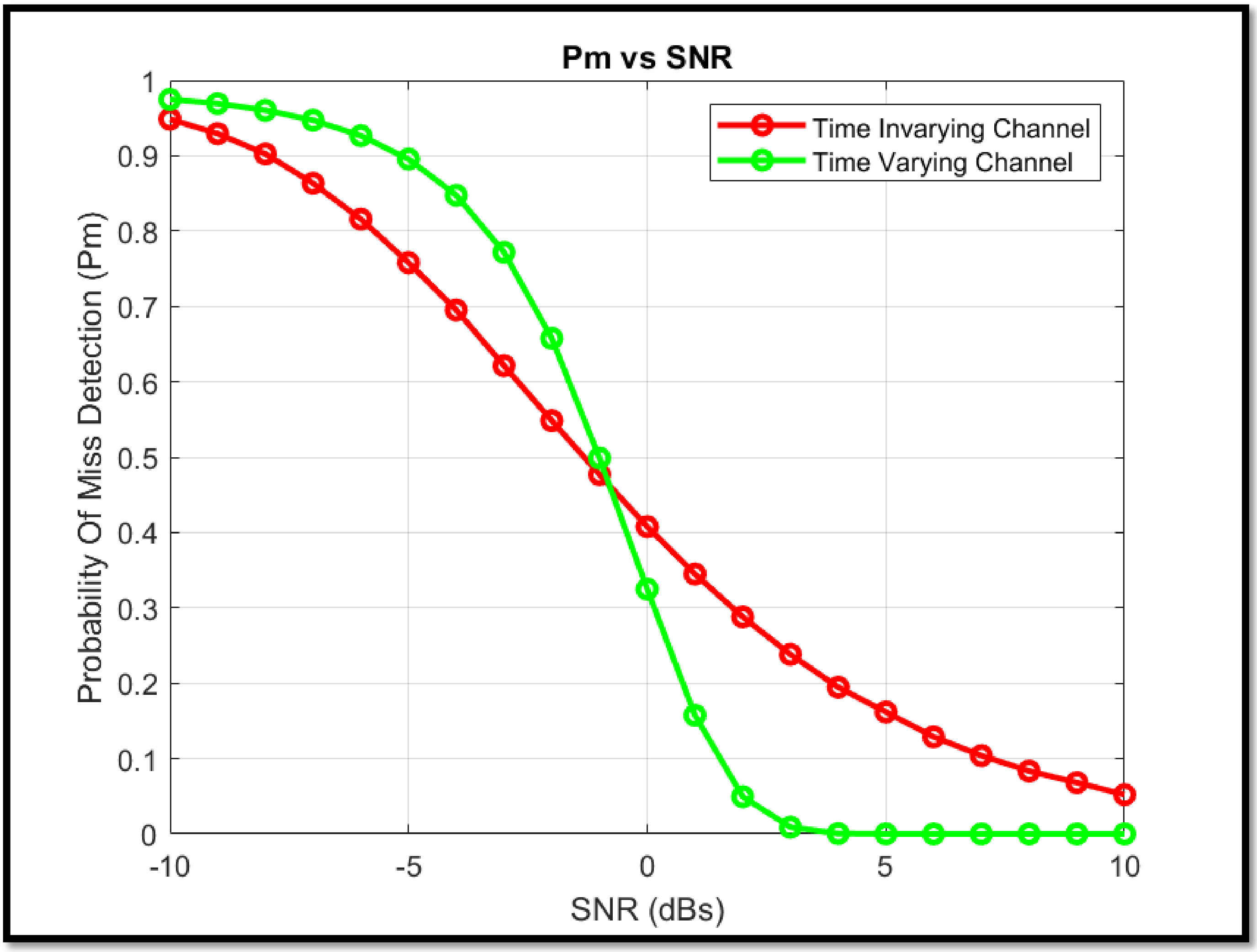
• **Q_m vs N:** This graph shows comparison of Global probability of misdetection (Qm) vs Number of SVU's for different values of SNRdb. It can be clearly seen that with the increase of number of secondary users, the value of Qm decreases as the vehicles involving in the decision process at the fusion center are more. Also, for high value of SNR, the value of Qm is low as compared to value of Qm for low SNR (in dBs).

• **P_m Analytical Simulation**: The comparison of Simulational and Analytical Results for Pm (Prob. Of Misdetection) vs. SNR (Signal to Noise Ratio) has been done. For Simulational Results, the received energy has been compared with a given threshold (in terms of gamma inverse function), which gives corresponding value of Pm.

5.3 New Results

• Comparison of Time Invariant and Time Varying Channel.

[This comparison is not correct for value of SNR > 0]



Graph 5.6: P_m v/s SNR (NEW)

For SNR ≤ 0, the trend is correct, as the Pm value for time varying channel is less than Pm value of time invariant channel for same value of SNR.

CONCLUSION

In this project report, we have first investigated the general concepts of security threats to the cognitive radio systems and their proposed solutions. We have also shown the analytical of Cognitive radio System. We also Seen various attacks on different Open System Interconnection Layers of Cognitive Radio system. This report shows the number of malicious users has a great role to affect the CR system of sending false alarm and creating miss detection. We have also seen Different algorithms available for the security of CRN.

Our forthcomingeffortdrivestay to lock CR arrangement by executing an effectualprocess to protect the cognitive radio systems. Encoded key drivestayproduced by Main user then to inhabit the network by moralsubordinateoperator, they obligate to have to match the key initial.

- In the sensing channel, byupsurge in number of subordinate vehicles (SVUs), number of samples and SNR Value, the Probability of Miss-Detectiondeclines. Also, while associating the channels, the rate of Pm in circumstance of time variable channel is supplementary as linked to that of periodin variable channel. This change is observed due to mobility of vehicles, which in turn decreases the performance of the channel.

- Security is a big concern in co-operative spectrum sensing as secondary vehicle users can easily falsify data. Some ways for incorporating security are clustering, XOR distance analysis, trust or reputation-based mechanisms can be used for labelling or differentiating the attackers. We have tried to implement XOR distance-based security method for above case.

REFERENCES

[1] R. Dubey, L. Chauhan, S. Sharma – “Secure and Trusted algorithm trusted algorithm,” in – 2011 ABV – Indian Institute of Information Technology and Management, Gwalior, India.

[2] Fahia Nasnin, Mst. Najia Islam – “Security Analysis in Cognitive Radio System,” in - 2017. BRAC University, Dhaka, Bangladesh.

[3] Chowdhury Sayeed Hyder, Brendan Grebur, And Li Xiao- “Defense against Spectrum Sensing Data Falsification Attacks in Cognitive Radio Systems,” in - 2013. Department of Computer Science and Engineering, Michigan State University East Lansing, MI 48823, USA.

[4] K. Geetha – “Handling TCP-Session Hijacking with Transport Layer Defense Method (TLD) In mobile ADHOC systems,” in – June 2016, Vol. 11 No. 11, Department of Computer Science, Periyar Arts College, Cuddalore, India.

[5] Long Tang, Juebo Wu – “Research and Analysis on Cognitive Radio System Security” in - 2012 State Key Laboratory of Software Engineering, Wuhan University, Wuhan, China.

[6] Yih-Chun Hu, Adrian Perrig and David B. Johnson – “Wormhole Attacks in Wireless Systems”.

[7] Muhammad Ayzed Mirza, Mudassar Ahmad, Muhammad Asif Habib, Nasir Mahmood, C.M. Nadeem Faisal, Usman Ahmad – “CDCSS: cluster-based distributed cooperative spectrum sensing model against primary user emulation (PUE) cyber-attacks” in – 17 April 2018, Department of Computer science, National Textile University, Faisalabad, Pakistan.

[8] Jose Marinho, Jorge Granjal, And Edmundo Monteiro - “A survey on security attacks and countermeasures with primary user detection in cognitive radio systems” in 2015, EURASIP Journal at Information Technology.

[9] Sonia Hashish, Loai Tawalbeh And Anwar Aldairi Hala Tawalbeh “Security in Wireless Sensor Systems Using Lightweight Cryptography” in - 2015, Faculty of computer and information Technology, Jordan University of Science and Technology, Irrbid, 22110, Jordan.

[10] Ahmad M. Rateb. - “Introduction to Cognitive Radio Systems by Department Of telematics and Optical Engineering” in - 2008, Faculty of Electrical Engineering, UTM.

[11] L. H. Xiaomin Qian, “Hard Fusion Based Spectrum Sensing Over Mobile Fading Channels in Cognitive. Vehicular Systems,” Sensors, vol. 18, no. 6, 2018.

[12] J. Mitola, “SNR walls for signal detection,” IEEE J. Sel. Topics Signal Process., vol. 2, no. 6, pp. 13–18, 1999.

[13] H. W. Ali A, “Advances on Spectrum Sensing for Cognitive Radio Systems: Theory and Applications.” IEEE Commun. Surv. Tutor. 2017., vol. 19, no. 6, 2017.

[14] M. Z. Jingyu Feng, “Securing Cooperative Spectrum Sensing Against Collusive SSDF Attack using XOR Distance Analysis in Cognitive Radio Systems,” Sensors, vol. 19.

[15] L. Gahane, “An Improved Energy Detector for Mobile Cognitive Users Over Generalized Fading Channels,” IEEE Transactions on Communications., vol. 66, pp. 534 – 545, 2018.

[16] Ho-Van, “Bit error rate of underlay decode-and-forward cognitive systems with best relay selection.” IEEE/KICS J. Commun. Netw., pp. 162–171, 2015.

[17] J. Tsitsiklis, “Decentralized detection.” Adv. Stat. Signal Process., pp. 297–344, 1993.