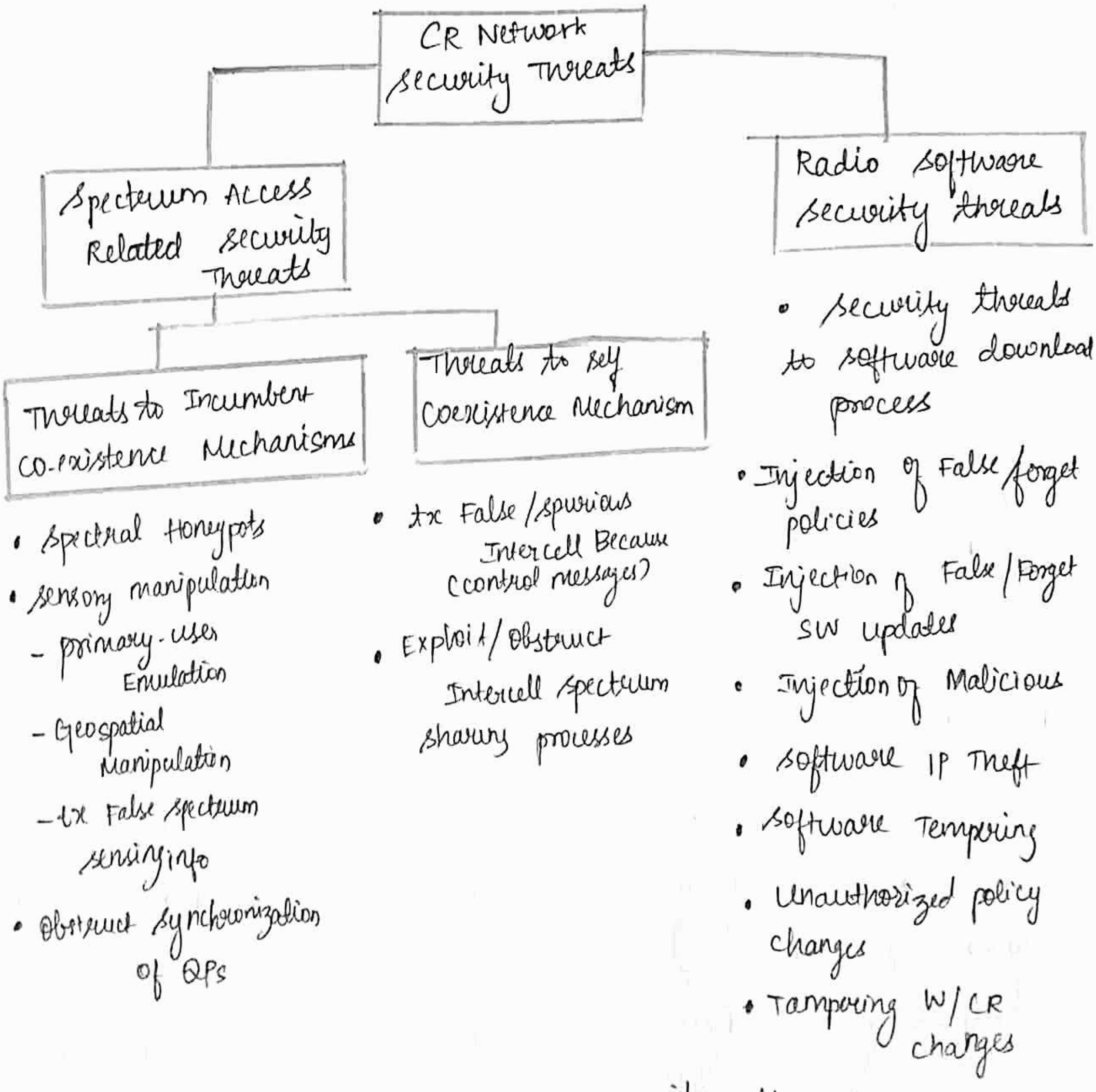
UNIT-V ADVANCED TOPICS IN COGNITIVE RADIO

COGNITIVE RADIO NETWORK SECURITY - INTRODUCTION

Cognitive radio is a revolutionary technology that promises to alleviate the spectrum shortage problem and bring about remarkable improvements in the efficiency of spectrum utilization.


CR Network security Threats
Spectrum Access Related security Threats
Radio software security threats
Threats to Incumbent co-existence Mechanisms
Threats to sely Coexistence Mechanism
• Spectral Honeypots
• sensory manipulation
- primary-uses Emulation
- Geospatial Manipulation
- tx False spectrum sensing info
• Obstruct synchronization of QPs
• tx False/spurious Intercell Because (control messages)
• Exploit/obstruct Intercell spectrum sharing processes
• security threats to software download process
• Injection of False/forget policies
• Injection of False/Forget SW updates
• Injection of Malicious
• software IP Theft
• software Temporing
• Unauthorized policy changes
• Tampering W/CR changes

A taxonomy of security threats

OVERVIEW OF SECURITY THREATS TO INCUMBENT COEXISTENCE

Spectrum sharing, or Coexistence, is an important attribute of CR networks. CR networks support two types of coexistence; incumbent coexistence and self coexistence

A CR needs to carry out spectrum sensing to identify fallow spectrum bands; that is spectrum "white space".

Hence we focus our discussion on two particular security threats to incumbent co-existence: primary user emulation and transmission of false sensing results.

In the OSS paradigm, secondary users equipped with CRs opportunistically utilize fallow licensed bands after identifying them via spectrum sensing.

1. primary user Emulation Attack

In a primary user emulation (PUE) attack, a rogue secondary user attempts to gain priority over other secondary users by transmitting signals that emulate the characteristic of the incumbent's signals

The potential impact of a PUE attack depends on the legitimate secondary users ability to distinguish the attacker's signals and actual incumbent signals while conducting spectrum sensing.

Another security issue threatens the reliability of the distributed spectrum sensing (DSS) process in CR networks.

In DSS individual nodes send their local sensing data to a fusion center, which processes the data to determine a sensing decision

2. Byzantine failures in DSS

In the context of DSS, Byzantine failures may be caused by either malfunctioning sensing nodes or malicious nodes launching spectrum sensing data falsification (SSDF) attacks

In either case, incorrect spectrum sensing data are reported to the fusion center, which can affect the accuracy of the sensing decision

Moreover, the investigation of DSS Byzantine failures involves not only the study of data fusion techniques, but also interplay between the data fusion techniques and the spectrum sensing techniques.

OVERVIEW OF SECURITY THREATS TO SELF-COEXISTENCE

Self co-existence mechanisms for a CR network are defined as part of the network's air interface and have features specific to the air interface

Therefore, here we focus on self-coexistence mechanisms of IEEE 802.22 to facilitate our discussion

The UHF/VHF TV bands between 54 and 862 MHz

It is quite possible for a number of 802.22 cells to have overlapping coverage area

ODSC protocol

The ODSC process enables a cell to acquire better channels or more channels to support the quality of service of the admitted workloads

A Base station collects neighbouring cells spectrum utilization information by receiving inter cell control messages.

Although inter-cell beacons play a crucial role in self, co-existence, they are not protected by 802.22's security sub layer

RADIO SOFTWARE SECURITY THREATS

The flexibility and adaptiblity brought by modern software, low cost microprocessors and smart antennas have made software-defined and cognitive radios a reality

The emergence of software-defined radio and software based CR have brought about new security threats not considered previously

The attacks in CR may include execution of malicious code, removal of software based authentication or access control functions, intellectual property theft via reverse engineering etc.

PRIMARY USER EMULATION ATTACK

In PUEA, the attacker generates fully similar type of signal as the PU to makean error in frequency band and to confuse the SU.

This kind of attack is referred as PUEA.

In the multi-hop channel environment, if PUEA is launched and there is no idle channel for SU, then the call is dropped or delayed.

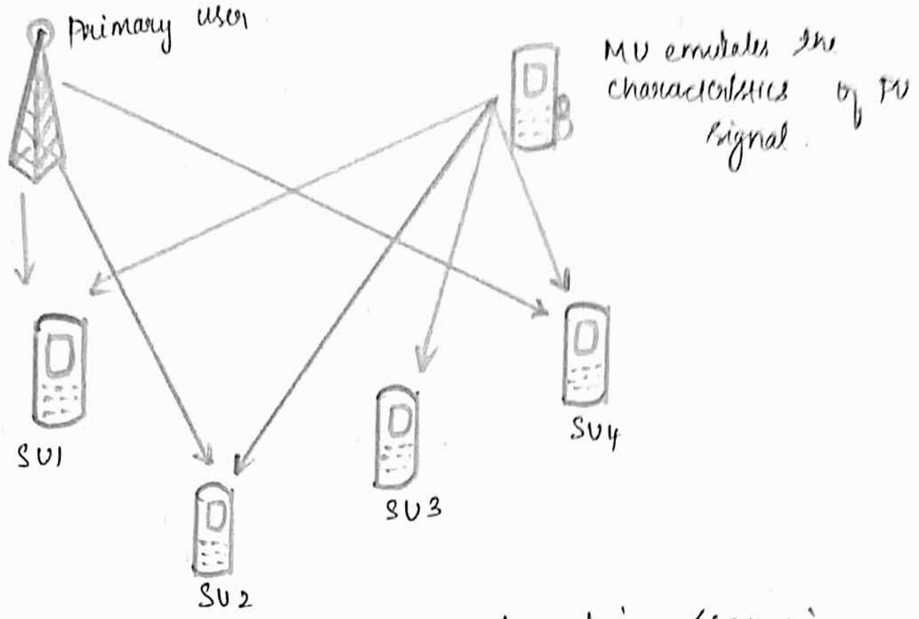


Illustration of PUEA launching scenario

A dropped call results is unreliable communication and the delayed call degrades the quality of service

One of the major technical challenges in spectrum sensing is the problem of precisely distinguishing, primary user signals from secondary users signals.

To distinguish the two signals, existing spectrum sensing schemes based on energy detectors implicity assume a "native" transmitter verification scheme

A selfish or malicious secondary user can easily exploit the spectrum sensing process

There are alternative techniques for spectrum sensing, such as matched filter and cyclo-stationary feature detection

Devices capable of such detection techniques are able to recognize the intrinsic characteristics of primary-user signals.

However such detection techniques are still not robust enough to counter PUE attacks

CLASSIFICATION OF PUE ATTACKS

Depending on the motivation behind the attack, a PUE attack can be classified as either a selfish PUE attack or a malicious PUE attack:

1. Selfish PUE attacks

An attacker's objective is to maximize its own spectrum usage.

When selfish PUE attackers detect a fallow spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of primary-user signals

2. Malicious PUE attacks

The objective of this attack is to obstruct the DSA process of legitimate secondary users.

Unlike a selfish attacker, a malicious attacker doesnot necessarily use fallow spectrum bands for its own communication purposes.

ROBUST DISTRIBUTED SPECTRUM SENSING

The Byzantine failure problem can be caused by spectrum sensing devices that are malfunctioning or carrying out spectrum sensing data falsification attacks.

A malfunctioning sensing terminal is unable to conduct reliable spectrum sensing and may send incorrect sensing reports to the data collector.

a) Distributed spectrum sensing

The hidden node problem in the context of CR networks can be described as an instance in which a secondary user in a CR network is within the protection region3 of an operating incumbent but fails to detect the existence of the the incumbent.

In DSS, each secondary acts as a sensing terminal that conducts local spectrum sensing. The local results are reported to a data collector that executes data fusion and determine the final spectrum sensing result.

b) Byzantine failure in Data fusion

A Byzantine failure could be caused by either malfunctioning sensing terminals or an SSDF attack. Both cases result in one or more sensing terminals sending false local spectrum sensing reports to a data collector, causing the data collector to make a wrong spectrum sensing decision

AUCTION BASED SPECTRUM MARKETS IN COGNITIVE RADIO NETWORKS

Access to the radio spectrum is a key requirement for continuous wireless growth and deployment of new mobile services.

spectrum trading is a market-based approach for spectrum redistribution that enables a spectrum liscense holder to sell or lease all or a portion of its spectrum to a third party

DYNAMIC SPECTRUM MICRO AUCTIONS

These types of aution mechanisms could be highly attractive to network operators : they provide a flexible and cost effective means for dynamic expansion of their spectrum resources without the need for costly capital investments in new spectrum.

THE ROLE OF COGNITIVE RADIOS

Cognitive functionality is essential in the realization of such types of micro auctions

The access technologies such as OFDMA will play an important role in enabling our micro aution mechanisms.

The market place differs significantly from conventional FCC-style spectrum aultions in three aspects

A. Multiparty trading with spectrum reuse

Multiple providers can selectively offer their idle spectrum pieces, and each spectrum piece can be sold to multiple "small" buyers.

B. On-demand spectrum trading

The flexibility not only attracts a large number of participants, but also enables the system to effectively multiplex spectrum supply and demand, further improving spectrum utilization.

C. Economic robustness with spectrum reuse

Without good economic design, spectrum auctions easily can be manipulated by bidders, suffering huge efficiency loss.

Therefore, only by preventing market manipulation can an auction attract bidders and new entrants and efficiently distribute spectrum to make the best use of this important resource.

ON-DEMAND SPECTRUM AUCTIONS

A on demand spectrum auction must distribute spectrum on-the-fly to a large number of bidders.

An efficient allocation algorithm is also needed to distribute spectrum in real time subject to the complex interference constraints among bidders.

a) Bidding Format: placewise Linear price-Demand Bids

Assume there are K channels in total, F_t is the set of channels assigned to bidder i. and hence the normalized spectrum assigned to i is $f_i = |F_i| K$.

A simple example is a linear demand curve.

$$P_i(f_i) = -a_i f_i + b_i, a_i \geq 0, b_i > 0,$$

where the negative slope represents price sensitivity of buyers as the per unit price decreases, demands in general increase.

b) pricing Models

without considering economic robustness, the auction princing follows directly from each bidder's bid.

$$R_i(P_i) = \frac{b_i P_i - P_i^2}{a_i}$$

For linear demand curves, the revenue is a quadratic function of price, with a unique maximum at $p_i = b_i/2$

Dividing the pricing models into two types

1. Uniform pricing
2. Discriminatory pricing

c) Linearizing the interference constraints

The constraints becomes: Every neighbour of i to the left of i and i itself should be assigned with different channels.

$$f_i + \sum_{j \in N_L(i)} f_i \leq 1, \quad i = 1, 2, \ldots, N$$

where $N_L(i)$ is the set of neighbours of i lying to its left.

ECONOMICALLY ROBUST SPECTRUM AUCTIONS

We know now define a truthful auction and a truthful and efficient spectrum auction

Definition 1: A truthful auction is one in which no bidder i can obtain higher utility u_i by setting $b_i = v_i$.

Definition 2: An efficient and truthful spectrum auction is one that is truthful and maximizes the efficiency of spectrum usage subject to the interference constraints.

DOUBLE SPECTRUM AUCTIONS FOR MULTIPARTY TRADING

In addition to truthfulness and spectrum reuse, a double spectrum auction must also achieve two additional properties.

- individual rationality and
- budget balance

Definition 3: A double auction is individual rational if no winning buyer pays more than its bid (i.e $P^b_n \leq B^b_n$) and no winning seller gets paid less than its bid (i.e $P^s_m \geq B^s_m$).

This property guarantees non-negative utilities for bidders

Definition 4: A double auction is expost budget balanced if the auctioneer's profit is $\phi \geq 0$.

$$\phi = \sum_{n=1}^{N} P^b_n \sum_{m=1}^{M} P^s_m \geq 0$$

This property ensures that the auctioneer has to incentive to set up the auction.

TRUST

Four required properties:

Spectrum reuse

Truthfulness

Individual rationality and

Budget Balance

VERITAS - address only single-sided buyer-only auctions

Comparison of various Double Auction Designs

Existing Double Auction Design	Spectrum Reuse	Truthfulness	Ex-post Budget balance	Individual Rationality
VCG	×	✓	×	✓
McAfee	×	✓	✓	✓
VERITAS extension	✓	×	✓	✓
RUST	✓	✓	✓	✓

Comparisons of Double Auction Designs

A. Grouping Buyers

TRUST groups multiple non-conflicting buyers into groups so that buyers in each group do not conflict and can reuse the same channel

B. Determining Winners

For any group G_l with $n_l = |G_l|$

The group bid π_l is

$$\pi_l = \min \{ B_n^b \} n \in G_l \} . n_l$$

The buyer group bids in non-increasing order: $B^t = B_1^s \le B_2^s \le \ldots \le B_m^s$ and B^n:

$$\pi_1 \ge \pi_2 \ge \ldots \ge \pi_L$$

Define k as the last profitable trade

$$K = \text{argmax}_{L \leq \min} \{L, M\} \pi L B^S_1$$

C. Pricing

This group price is evenly shared among the buyers in the group l:

$$P^b_n = \pi k / n l \text{ , for all } n \in G_1$$

with such pricing mechanism, the auctioneer's profit becomes $\phi = (k-1) \cdot (\pi k - B^S_k)$ and it is easy to show that $\phi \geq 0$.

PUBLIC SAFETY AND COGNITIVE RADIO

In public safety applications, robustness and rock-solid technology are paramount. The communication system of reuse workers should always work, even under extreme conditions.

Requirements

The next generation communication system for public safety will have very extensive requirements.

COMMUNICATION STRUCTURE

A public safety wireless network consists of a backbone network, base stations, and handsets

* The backbone network is used for inter base station Communication

Each type of node has different physical layer requirements.

For instance, emergency workers carry battery-powered handsets that are energy limited.

RELIABILITY

There are two kinds of reliability

- * robustness
- * security

i) Robustness

It is the ability of a system to avoid total failure despite unforeseen condiltions or partial damage.

ii) security

It is the ability of a system to withstand malicious attacks.

BROADBAND

In an emergency situation a picture could say more than a thousand words. video is even powerful, so there is huge demand for multimedia. The next generation public safety communication equipment will provide advanced features.

PAGING

Paging is even more important that Voice communication, used for instance, to alarm firefighters etc.

DISADVANTAGES OF COMMERCIAL WIRELESS COMMUNICATION NETWORKS

The network gets overloaded, As a result the communication network may callapse

when a disaster occurs, a part of the infrastructure may be damaged.

commercial networks have no backup for the power supply.

BENEFITS OF USING COGNITIVE RADIO RELATED TO EMERGENCY CONDITION

The general meaning of a cognitive radio is a smart device that does all kinds of useful things for its owner, based on sensory input and machine learning

A. Improved communication structure

- * Communication with other networks
- * Backwards compatibility.
- * Introduction of new services

B. Improved Reliability

- * Minimize interference to other networks
- *. Adaptability feature

C. Enabling Broad band

public safety networks are heavily used

Implementing the whole network would be very costly.

Relatively large Bandwidths required

PUBLIC SAFETY COMMUNICATION - STANDARDS

Several communication standards are

- * P25 (APCO project 25)
- * TETRAPOL
- * TETRA

TETRA

TETRA was formly known as trans-European trunked radio and standardized by ETSI in 1995.

Designed for government agencies, emergency services, rail transportation staff, and the military.

TETRA System supports several types of data communication:

1. status messages
2. short data services
3. packet data
4. circuit switched data communication

C2000

TETRA is only a standard and manufacturers make only generic base stations and handsets that implement the standard.

It consists of three components.

T2000

A TETRA-based network for voice and low rate data communication, use the frequency band 380-385 MHz for uplink and 390-395 MHz for downlink communication

P2000

paging is a very important communicaton application in public safety, where short predetermined text are transmitted and displayed on pager devices.

M2000

M2000 is a software system used in the public safety answering point (PSAP)

APPLICATION OF COGNITIVE RADIO

public safety and emergency response is another area in which cognitive radio has gained a lot of attention.

For years public safety agencies have desperately needed additional spectrum allocation to ease frequency congestion and enhance interoperability.

These particular problems can be mitigated through the use of cognitive radio technology

For emergency and public-service providers, a major part of this concept is spectrum sharing which can help in maintaining call priority and response time.

Cognitive radios can prove to be more effective by utilizing some of the existing spectrum that is not widely used.

PROPAGATION CONDITIONS

The propagation conditions determine how far a radio wave propagates.

A simple path loss model that is often used for land mobile radio is the plane Earth models, which predicts a path loss exponent $\gamma = 40\text{dB}$,

$$P_{rx} = P_{tx} G_{tx} G_{rx} \left[\frac{c}{4\pi f d}\right]^2 \cdot 4\sin^2\theta \left[\frac{2\pi b_{tx} b_{rx}}{cd}\right]$$

SYSTEM SPECTRAL EFFICIENCY

The system spectral efficiency can be defined as

$$\eta \approx \frac{R/B}{K}, \quad [b/s/Hz/site]$$

The shannon formula

$$C = B.\log 2\,(1+SNR)\,[b/s].$$

In a spatial reuse system, as in our example, the SNR is interferena limited and

$$SNR \propto \frac{1}{6}\,(3K)^{\gamma/2} \quad \text{applies.}$$

WHITE SPACE ASSESSMENT

To get permission from spectrum regulators to apply cognitive radio in a certain band, one has to convince them the spectrum in this band is structurally under utilized.

a) why is the 400 MHz to 1 GHz Band Optimal for mobile communication?

Below the 240, MHz the antenna is too large for mobile communication

One well-known trick to make an antenna shorter is to roll it up, but this makes it too selective for only one narrow frequency band.

Frequency from 240 to about 400 MHz are used by military communication.

The frequency range from 1 to 1.4 GHz

Frequencies below 1 GHz have less indoor penetration loss

The indoor penetration loss and body loss for DAB band III and the L band are reported.

Anti-jamming

An important requirement of public safety networks is resistance to jamming. Jamming is the intentional use of a strong radio signal, for instance by terrorists, in an attempt to disrupt communication.

There are two well-known spreading techniques.

- Direct-sequence spread spectrum
- Frequency hopping

INTERNET OF THINGS (IOT)

The internet of things, or IOT refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data.

"The IOT integrates the interconnectedness of human culture - our things - with the interconnectedness of our digital information system - 'the internet'. That's the IOT".

Overview of Four stages of IOT

stage 1: Networked things (wireless sensors and actuators) stage 2 : (sensor data aggregation systems and analog to digital data conversion)

stage 3 (Edge Analytics) :

stage 4 (Analysis , management , and storage of data at cloud Analyctics)

C. Applications of IOT

IOT applications are expected to equip billions of everyday objects with connectivity and intelligence.

It is already being deployed extensively, in various domains , namely :

* Wearable's
* smart Home Applications
* Health care
* smart cities
* Agriculture
* Industrial Automation

D. IOT - Instrial Automation

IOT here can prove to be game changing with solutions for all the following domains in its arsenal.

* Factory Digitalization
* Product flow Monitoring
* Inventory Management

- safety and security
- Quality control
- packaging optimization
- Logistics and supply chain optimization

COGNITIVE RADIO FOR INTERNET OF THINGS

Recent research and technology trends are shifting toward IOT and CRNs. Equipping IOT objects with CR capability has lead to a new research dimension of CR based IOT.

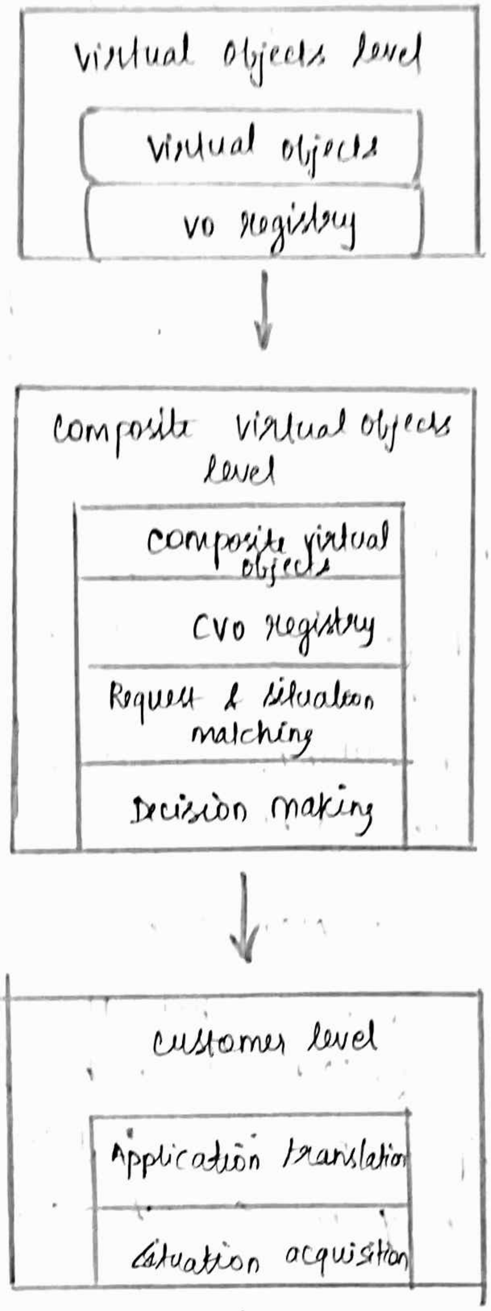
MOTIVATIONS FOR USING CR IN IOT

The main motivation comes from bandwidth allocation for IOT objects. The number of IOT objects is expected to grow in large numbers, and it will be very difficult to allocate spectrum band to these objects.

CRNs can facilitate in all of these situations. Traditional communication techniques do not support spectrum sharing among multiple users.

CRN ENHANCES WITH SHARING CAPABILITIES:

cellular communication incurs costs, while Bluetooth and zigbee have limited range. IEEE 802.22 for a wireless regional access network.



CR based IOT framework with three levels: the virtual objects level, composite virtual objects (CVOs) level, and consumer level.

Raw data is fused, cleaned, classified into clusters according to its features, stored and analyzed for its conversion into useful form.

CR-based IOT frameworks can alleviate interference situations by looking for interference-free channels through dynamic spectrum access capability

Equipped with cognitive capability, IOT objects can achieve seamless connectivity.

CR BRINGS SEVERAL BENEFITS TO IOT

* It enables efficient spectrum utilization
* It improves accessibility to various networks and services.
* It can autonomously adapt its operation to simplify the Tasks.

COGNITIVE IOT FRAMEWORKS

It is desired that IOT objects should have cognitive facility to make smart decisions about the spectrum and perform intelligent operation by analyzing network conditions.

Many researchers are working on CR to enhance M2M communications.

Large-scale IOT applications generate huge volumes of data

A data-centric CR-based IOT framework can be implemented for data management and intelligent decision making

The contextual data processing can produce large overhead

context acquisition is followed by data discovery and data mining to detect different events.

Virtual objects (VOs) are developed to represent sensors, create sensor data and embed context information

The network architecture has sensors, controllers, a central hub, a server and a user layer

A composite virtual object represents a collection of VOs that have cognition with semantic interoperability. The consumer level provides an interface for users to interact with the system for application usage.

A Distributed Internet like Architecture for Things (DIAT) based on three level architecture can support secure addition of a number of heterogeneous devices

The layered architecture deals with privacy and scalability as well.

cognitive capabilities realize smart decisions with autonomous service provision

cognitive functions are incorporated at all three levels, resulting in a stack called IOT Daemon.

The framework has to be flexible and less complex in computation

The platform for a base station in the form of a wireless edge appliance. (WEA)

A wireless access appliance serves as customer premises equipment. (CPE)

STANDARDIZATION EFFORTS IN CRN-BASED IOT

To bring CR-based to realization, a great ideal of effort is required. As CR-based IOT frameworks are in their infancy, categorizing research directions is difficult

There are certain bodies working independently on both CRNs and IOT such as IEEE, the International Telecommunication Union and 3GPP,

As work is going on to open new bands for CRNs, it will be a better choice to place IOT in this framework

Another solution may be the coexistence of CR based IOT in current regulatory assignments

Research in IOT standards in terms of communication techniques is related to RFID and NFC

CRN standards have considered the

Co-existance in short range to medium range

similarly, protocols are at a progressive level for CRNs, but negligible work has been done on IOT protocols

SECURITY AND PRIVACY RELATED TO CR-IOT

The heterogeneity in CR based IOT frame works has security problems as we cannot apply the same security levels to all situations

The adaptive capability of CR can become a security problem as an intruder may pretend to be a CR.

Access to information should be easy for validation and monitoring conditions

The introduction of a smart object also introduces privacy issues.

A major source of privacy issues is the misuse of application.

Privacy is required at the data collection point as CR-based IOT will be a global frame work with a variety of technologies and with diverse data.

Data is collected using RFID, WSNs, cellular phones, and others

Thus data anonymization with strict control, management among objects, and identification is required.