International Journal of Engineering & Technology, 7 (2.8) (2018) 372-378

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A Survey on advances in security threats and its counter measures in cognitive radio networks

D. Ganesh[1*], T. Pavan Kumar[2]

[1]Research Scholar, Koneru Lakshmaiah Education Foundation, Guntur, AP, India
[2]Professor of CSE, Koneru Lakshmaiah Education Foundation, Guntur, AP, India

Abstract

Cognitive radio is a promising wireless communication technology that improves spectrum utilization and offers many benefits for internet users. Cognitive radio networks utilizes the available limited resources in a more efficient and flexible way. The main objective of the Cognitive network is to efficiently utilize the unutilized spectrum and meet the demand of the secondary users. some of the important features of cognitive of Cognitive radio networks are dynamic spectrum access, self organizing and flexibility. As Cognitive radio networks are flexible in nature, it will be effected by various security attacks which in turn affects the performance of the network. Furthermore Cognitive radio networks transmit the spectrum in several licensed bands and it also performs dynamic spectrum allocation. Cognitive radio and Cognitive radio networks are wireless in nature these face conventional attacks. In this survey we address various attacks in different layers , new threats and challenges that Cognitive networks face, current available solutions to address layer attacks. In addition applications, open problems and future Research challenges are also specified.

Keywords: *Cognitive radio, Cognitive radio networks, Layer attacks, Security requirements, IEEE 802.22*

1. Introduction

Cognitive radio is an emerging area which will overcome the problem of underutilization of the spectrum. Normally these spectrum vales range between 2.4 GHZ to 5 GHZ. Normally spectrum studies are conducted federal communication commission (FCC).Many licensed bands such as TV bands are underutilized but the unlicensed bands are over utilized. As emerging standards like IEEE 802.22 exploit these underutilized spectrums. Basically IEEE 802.22 is a standard for Regional area network using white spaces. This standard uses Cognitive radio techniques[1] to allow sharing of geographically unused spectrum allocated to television broadband service.

In wireless communication spectrum is critical resource and is assigned for data transmission for a duration of time. Spectrum assignment is basically of two types ,i.e static and dynamic allocations. During static allocation[2] the main problem encountered is under utilization of spectrum. This problem is reduced by the advent of Cognitive radio networks. Radio equipment in the Cognitive radio networks can sense the available spectrum around it and reallocate the spectrum. Cognitive radio networks consists of two types of users: Primary users(PU's) and Secondary users(SU's). Primary users(PU's)[3] are licensed users where as secondary users(PU's) are unlicensed. Primary users are having more priority over secondary users. switching and balancing the spectrum between primary and secondary users will be taken care by Cognitive radio networks. This networks are more smart and flexible which will dynamically optimize spectrum usage[4]. Spectrum utilization raises several open issues. one among them is Providing communication and managing the spectrum between primary and secondary users in Cognitive radio networks. To overcome the underutilized portions of the spectrum, a good idea was proposed by mitola[6] using Cognitive radio's.

These Cognitive radio's are interconnected to form Cognitive radio networks. all the Cognitive radio's senses the spectrum and finds the free portions which are called as whitespaces available in the spectrum. These white spaces are called as spectrum holes. Reassignment of Unused spectrum will be taken care by cognitive radio networks

As we specified Cognitive radio networks are open, dynamic, and flexible in nature. Hence, these are vulnerable to malicious attacks [7]. Providing security to these networks is not an easy task, this specifies various challenges and it may become more complicated now days because day to day number of threats are increasing and securing them is an challenging task .In this work we are addressing both traditional and new threats specific to Cognitive radio networks. some of the traditional threats for Cognitive radio networks are Eavesdropping, Spoofing, Personal user emulation ,wormhole, sinkhole[8], Sybil attacks and many more. These consequences may effect the functionality of the Cognitive radio networks. Hence we require efficient preventive measures to reduce these traditional attacks.IEEE 802.22 is the first standard which utilizes fallow TV bands and does the spectrum management. This strandard follows all the security mechanisms such as authentication, confidentiality, integrity, privacy and non repudiation. however several solutions for these attacks has been proposed in this paper.

The key contributions of this paper are:

1. clear descriptions of Cognitive radio networks in context of spectrum usage.
2. Provides clear description about various security threats and attacks
3. Overview of open problems and future challenges in Cognitive radio networks

There have been significant developments in the area of cognitive radio networks. This survey gives attacks and recent counter

measures in the area of cognitive networks. In Section II, we give an overview of Cognitive radio architecture & cognitive cycle and its elements. Section III reviews security requirements in cognitive radio networks. Section IV provide various attacks at different layers and its existing solutions. Section V & VI Provides an overview of Conventional and specific security threats. In section VI we conclude the paper and provide future research diections

2. Cognitive Radio Architecture

Cognitive radio is defined as "It is a radio that can change its transmitter parameters dynamically depending upon the environment it operates". The main aim of cognitive radio is to seek the white spaces and utilize them for increasing various QOS parameters such as throughput, reliability and fairness. The standardization of Cognitive radio networks came with the advent of IEEE 802.22,the first standard with only one base station and performs spectrum management. To exploit TV white spaces Europeon computer manufacturing association(ECMA) defines a new standard called ECMA-392.This standard opposed IEEE 802.22 because 802.22 targets on houses and buildings. Furthermore ECMA has proposed several standards regarding reconfigurable radio systems(RRS)

Some of the main characteristics of Cognitive radio networks are:

1. *Proper sensing of the operating environment*: Here CR Works in a multi dimensional cooperative and non cooperative emitters, works accordingly senses the changes in the emitters & traffic and works accordingly.
2. *Effective Management of Resources*: Radio spectrum is a valuable and distributed resource. hence spectrum will not be available at a single location. Balancing of spectrum at multiple locations will be taken care by Cognitive radio's.
3. *Managing Operational state Languages:* These languages are used for sharing the information in the network. As cognitive radio networks are dynamic in nature its states are informed in the network as per changes. The language that CRs use for this purpose is called operational state languages

These are some of the important characteristics of cognitive radio networks. Cognitive radio functions are spectrum sensing, Spectrum Management, Mobility and Sharing.

Cogntive Cycle:

As we already specified cognitive radio is a device which senses its environment dynamically and assigns the spectrum. The operation that cognitive radio performs to sense the environment is referred as Cognitive cycle[9]. The allocation of spectrum from primary to secondary users is also done immediately. The main Key phases in cognitive cycle are Spectrum sensing, Spectrum analysis and spectrum Decision.

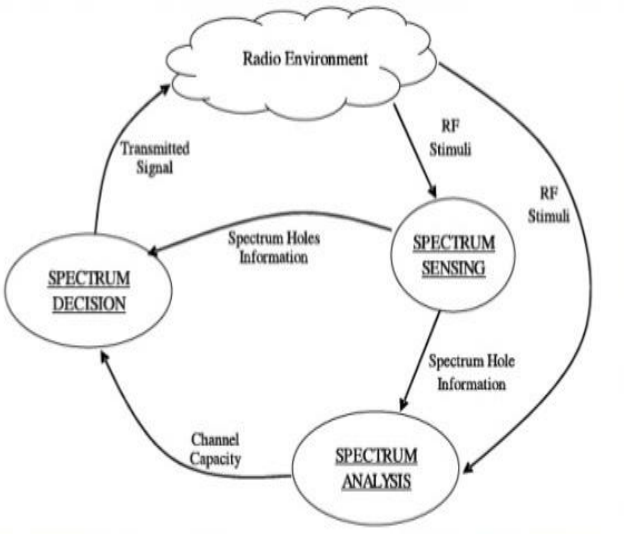

Fig. 1: Cognitive Radio Architecture

The working of each and every phase is as follows.

I. Spectrum Sensing: This is one of the most important phases of Cognitive cycle. Here two types of sensing will be done i.e, fast and fine sensing. This sensing operation will be done by the Base station, where its primary responsibility is detecting the incumbent signals. Same operation will be done by IEEE 802.22 by using energy detection method. The main advantages of sensing is simplicity and less computational time, so that it became an important operation in the cognitive architecture. Some of the popular spectrum sensing techniques used by the cognitive networks are Cooperative sensing, Wave form based sensing, match filtering, cyclostationery based sensing and many more.

II. Spectrum Analysis: Here analysis of available holes information will be done and it is purely statistical based process. It analyses several channels and network characteristics like Delay, Error rate etc. The collected and analyzed information will be given as an input to the next phase i.e spectrum decision process.

*III. Spectrum Decision :*In this phase the most appropriate spectrum hole is selected for transmission. Once selected it will be reused by another secondary user.

The above functionality of all the phases will gives an abstract view of each and every phase.

3. CRN Security Requirements

As cognitive networks are wireless in nature they have all the security requirements which are in the wireless networks. Some of the requirements are as follows[10]:

a. *Confidentiality:* all the users in the cognitive networks are interested in keeping their data confidential. They have to ensure that their messages are only received by the Authorized users in the network. One of the major application of CRN is military, here data should be kept confidential.

b. *Availability:* The spectrum required to the primary users must be available to all the users in the CRN's. All the base stations consists of various security measures to make the data available to all the Primary and Secondary users.

c. *Authentication:* Authenticating all the users in CRN's i.e Primary , Secondary users and all the other devices is essential for secure data transmission. Major threats in the CRN's will be overcome by using various cryptographic techniques like Public and Private key cryptographies. These are majorly required in all the algorithms of cryptography.

d. *Integrity:* It is not sure that all the messages sent by the base station, CRN, Primary and secondary users have not been modified in the due course. This security requirement that data has not been modified from Primary to secondary users and vice versa. To maintain integrity ,we use Cryptographic Hash functions and MAC's.

e. *Nonrepudiation:* In communication parties sender will not deny sending a message and receiver do not want to deny receiving a message, we can call it as sender receiver non repudiation in CRN. Necessary cryptology has to be developed to ensure this non repudiation at sender and receiver similarly CRN do not deny a message received from a Base station.

4. Layer Attacks

i. Physical Layer Attacks:

Physical Layer is the bottom layer which is used for communication between two networking devices. This layer is vulnerable to many threats. Some of them are discussed below.[7-20]

a. Primary User Emulation Attack: (PUEA)

PUEA is the major among all the attacks. This attack gained more attention from all the researchers. In CRN's, secondary users use

the available spectrum only when it remains unused. And secondary users have to vacate the spectrum whenever primary user wants it. For this reason secondary users will continuously check for primary user. In this attack, the attackers do not allow the secondary users from using available spectrum. The attackers act as primary user by transmitting signals those characteristics which are similar to primary user's signals. Whenever the secondary user found those signals it will automatically vacate the spectrum and this will occupy by the attacker (who is pretended as primary user). And this secondary user moves to the next available spectrum by detecting another PU's. If attacker again detect that next available spectrum band, he/she could also make unavailable for secondary users resulting Denial of Service (DoS). There are two types of PUEA: i) Malicious PUEA, ii) Selfish PUEA.

Malicious PUEA: In this type of PUEA, Attackers do not allow the SU's to use the available spectrum. Their main goal is to reduce the spectrum utilization. Here attackers will not use band for their own purpose.

Selfish PUEA: In this type of PUEA, attacker acts as SU who is selfish and if he detects that spectrum is unused then he could make it unavailable for the secondary users.

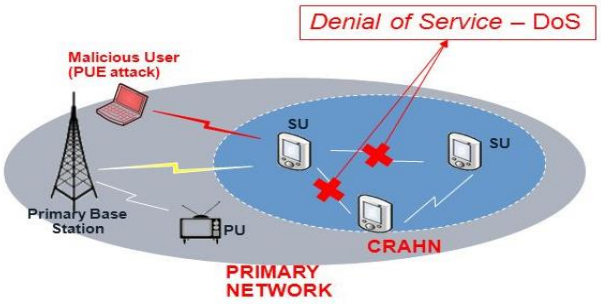

Fig 2: Primary User Emulation attack

One example of PUEA is explained in the below diagram. The network has 10 available channels. In which channels (1,4) and (2,3,5) are occupied by primary users, while the remaining (6,7,8,9,10) remains idle so that they can be used by secondary users. But the attacker occupies the channels (7,8,9). Therefore, only two channels (6,10) are available for secondary users.

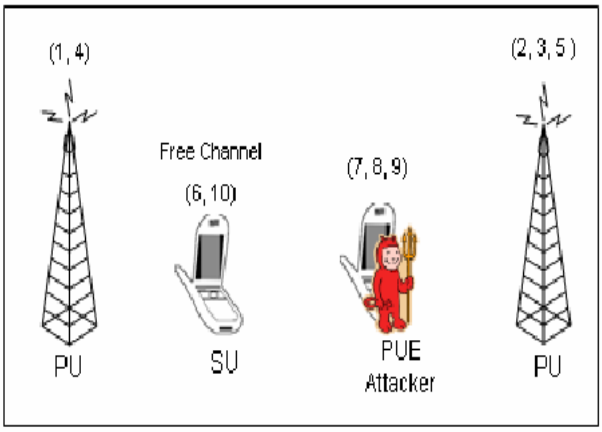

Fig 3: Example of PUE attack

To mitigate PUE attack, a technique called Principal component analysis for spectrum sensing is used. In this technique all the SU's send details about all PU's they have observed to the Fusion Centre(FC). And this center also keep information about SU's Transmission Signal power. By collecting all this information Fusion Center correctly identify the PU and discard the suspected node. Another method which is called as Belief Propagation is used to mitigate this attack. In this technique, all the secondary users has to follow some sequence of steps until the suspected node is identified and discarded from sending process.

B. Objective Function Attack:

Normally cognitive radio has the capacity to modify its radio parameters based on the current situation. By this adversary will attack this objective function by wrongly predicting its parameters to meet its own objective function. Objective function main aim is high data rate and low power. For example we consider the following objective function:

$$f = w1P + w2R$$

where w1,w2 are the weights of power and data rate. The attacker will modify any one of these parameter in the function to make CR to use wrong channel. By do this he can make to move the CR to low security channel which is less secure.

To mitigate this attack, we must set the predefined threshold for these parameters. By doing this, we can stop the communication if the values of parameters cross the threshold and this will be reported to the Fusion Center(FC).

C. Jamming Attack

In this attack, the attacker aim is to send packet out of network so that they can block the legitimate user from participating in communication. This will cause denial of service.

To mitigate this attack, the primary user information about the location must be kept by the secondary users. Secondary users get this information by connecting to base station.

ii. Data Link Layer Attacks:

Mostly attacks in the data link layer are due to the attack of MAC address. Some of the attacks are discussed below.

A. Specturm Sensing Data Falsification Attack:

In this attack, attackers acts as legitimate members of the network and shares false sensing information to the decision stream. So that they will get more available spectrum for their own purpose which reduces throughput. To mitigate this attack a new method is introduced. By using this method the center fusion will keep track that how many no.of times all the nodes make correct decisions about presence of PU's.

B. Control channel saturation attack

Generally in CRN's, there will be only one control channel to carry the traffic between the users. This control channel will enter the saturation state when it is not able to carry more control traffic. By knowing this the attacker intentionally make the control channel to saturate. So that attacker can reduce the no.of legitimate nodes to use spectrum. And attacker can use all the available frequency bands.

To mitigate this attack the network is categorized into clusters. And each cluster will have its own control channel. If the control channel of one cluster is attacked, the control channels of other clusters will remain unaffected.

iii. Network Layer Attacks:

This layer is one of the important layer because it routes the data packets from one network to other. There are many threats in this layer. Some of them are discussed here.

A. Hello Attack

In this attack, the attacker sends the message to all the other nodes in the network to inform that it is the best route to reach the destination within the network. The attacker will send the messages with high power to the other nodes and they receive

with good signal strength. So that attacker can convince the nodes as their neighbors. By this all other nodes may think attacker as their neighbor and send packets through the attackers and lost them.
To mitigate this attack we should make the bidirectional links between the nodes and messages sent through these nodes must be verified by Fusion Center (FC).

B. Sinkhole Attack

In this attack, the attacker tells other nodes as it is the best route to reach the particular destination and motivates them to forward packets through them. By using this attacker may launch a new type of attack called selective forwarding in which it is able to modify or discard a packet in the network.
To mitigate this attack, authentication mechanism is used. In which every node joining the network must be authenticated and verified. And the suspected node is discarded before joining the network.

C. Sybil Attack

In this attack, to represent a identity the attacker uses many fake identities. So that he can able to cheat the legitimate node. This attack mainly affects the co-operative spectrum sensing technique where attacker sends wrong sensing information to make wrong decisions.
To mitigate this attack we use node's identity validation technique. In this we use two types of validation- Direct and Indirect. In Direct validation identity of the node is verified directly. In indirect validation the identity of node is verified by the other nodes.

iv. Transport Layer Attacks

In Cognitive Radio networks, transport layer has many no of attacks.

A. Key Depletion Attack

Cognitive Radio network has more no. of retransmissions and high round trip times therefore it has less transport layer sessions and most of these sessions are occurred between communication parties. Generally there may be many transport layer protocols such as Secure Socket Layer (SSL), Transport Layer Security (TLS). These protocols will generate many cryptographic keys at the start of each session. And more session keys are generated for many sessions. Therefore the attackers listen to the communication and steal the session key. By using these keys they can send and receive the session data.
To mitigate this attack, we have to perform session key sharing in more secure way by using new ciphering algorithms.

v. CROSS LAYER ATTACKS

Cross layer Attacks are the attacks that targets one layer and have consequences over other layers.

A. Lion Attack

This is a kind of cross layer attack, where the attacker performs the attack at the physical layer to degrade the performance of Transmission Control Protocol (TCP) at transport layer. In this attack, the attacker jams the channel or performs PUE attack. PUE attack forces the secondary user to frequently perform the frequency handoff. This frequency handoff interruption will reduce the throughout.
The impact of this attack can be reduced if we provided proper information about handoff's to transport layer. To mitigate this attack we introduce a technique called Freeze TCP by which we can easily predict the upcoming disconnection of window.

Table 1: Layer Attacks and their existing Solutions

S.No	Name of layer	Security requirement	Attack	Contribution	Solution
1.	Physical Layer	Authentication	Primary User Emulation Attack	F. Lin, Z. Hu, S. Hou, J. Yu, C. Zhang, N. Guo, M.Wicks, R. C Qiu, and K. Currie	Principal component analysis for spectrum sensing
			Objective function	D. Hlavacek, and J. Morris Chang	Uses objective function
			Jamming attack		Tracking primary uses location
2.	Data Link Layer	- Non Repudiation - Integrity - Availability	Spectrum sensing Data Falsification	A. Rawat, P. Anand, H. Chen, and P. Varshney	Mitigation method
			Control Channel Saturation		Categorization of network into clusters
3	Network Layer	- Authentication - Confidentiality - Integrity	Hello attack		Session keys method
			Sinkhole attack	L. Akter and B. Natarajan	Authentication
			Sybil attack		Node's identity validation technique
4	Transport Layer	- Confidentiality - Integrity	Key Depletion Attack	J. Hernandez-Serrano, O. León and M. Soriano	- Ciphering algorithms to manage session keys
5	Cross Layer	- Availability - Authentication - Confidentiality	Lion attack	T. Goff, J. Moronski, D. Phatak, and V. Gupta	- Freeze TCP

5. Conventional Security Threats

In CRN communication, Security is one of the most important aspect. As CRN's are the kind of wireless networks, so they suffer more to the attacks. These attacks include the privacy of wireless

node which includes eavesdropping, impersonation and traffic analysis. Here we discuss some among them.

A. Eavesdropping and Impersonation

In Eavesdropping attack, the attacker listens to communication to know information about the communicating parties, PUs and SU's. This information is used to launch replay attack or impersonation attack. To mitigate this attack, we use the encrypted and time stamped messages. In Impersonation attack, the attackers steal the identity of the legitimate node and use this identity to establish communication with other nodes. To mitigate this attack, anonymous ID's to all PU's is introduced. These ID's can be changed along with the encryption keys.

B. Selective Forwarding Attack

In this attack, certain messages are not forwarded to the original CR node by the malicious node. This malicious node will destroy those messages and acts as a block hole. To mitigate this attack, the CR node or BS uses a time limit strategy. If the limit for particular message is exceeded and the message is not received then BS will be informed to resend the message to PU or SU through another secure route.

C. Sinkhole and Sybil Attack

In this attack, the incorrect information about the high quality route to sink is advertised by the attackers To mitigate this attack, the certificates are introduced which are issued by the BS or by Cognitive Radio Network Authority. In Sybil attack, the malicious node is pretended to be present at multiple places, so that the BS will believe it as the moving legitimate node. To mitigate this type of attack we use anonymous ID's and certificates are used.

D. Worm Hole Attack

In this attack, the malicious node will believe the other CR nodes as their neighbors which in fact for away from them. So that their identities and real addresses can be destroyed. To mitigate this attack, the BS will provide anonymous ID's and their distances for each node and this information must be encrypted.

E. Hello flood attack

In this attack, to establish the communication, the attacker will broadcast the HELLO message to all nodes in the network. The attacker will spoof to the acknowledgement which is used by some link layer protocols and attackers use this information to convince other nodes that weak links between the nodes as strong links. So these weak links will be used for routing the packets between nodes and these packets will be corrupted or lost. To mitigate this attack, we use certificates and authentication. Some higher layers use the secure protocols

.

6. Specific Security Threats

In addition to traditional threats[15], CRN's has the new kind of threats due to the specific threats due to their specific functions. Some of them are discussed below.

A. Hardware Attacks

In this attack, hardware of the some of the nodes is altered or damaged. The result of this attack may cause the shutting down of the node completely or transmitting signals in a completely wrong frequency band. To mitigate this attack we must provide hardware encryption. So that hardware of node cannot be accessed by attacker.

B. Cr Software Attacks

The impact of the software attacks in CRN's is greater when compared to other network because of their characteristics. This software attacks can completely make CRN's shutdown. To suppress the malicious software installation we have to use the tamper resistance and virus detection techniques[22]. There is a great need to download the softwares from the trusted servers. With these attacks we have to protect authentication, authorization and integrity of software installations from being eavesdropping.

C. Primary User Emulation Attack

In this attack, attacker is disguised as PU and all characteristics and signals are advertised to all nodes. There are many types of PUE attacks[5]. Here we discuss some among them. The denial PUE attack will occur whenever the attacker will provide the wrong information to the SU as the PU is occupying it. This forces SU to stop using frequency band and it is vacated. The another PUE attack is Induced PUE attack, in this attack the attacker advertises the high frequency signals[12] so that SU fails to identify the presence of PU. In co-ordinated PUE attack, many malicious nodes will co-ordinate with each other to launch attacks on different channels so that as many as CRN's become disrupted. To mitigate PUE attack, we ise a scheme called Localization Based Defense and another method to mitigate this attack is authentication.

D. Jamming Distruption Attack

In Cognitive Radio, one can perform Jamming during data transmission. Here the attacker will not consider the PU and compete with PU to access channel which will cause the DoS for PU. To mitigate this attack CR's should check ID's, certificates and authenticate the transmitting node.

E. Spectrum Sensing Data Attack

This type of attack will be occurred due to incorrect spectral analysis which results in making wrong decision of assigning bands to primary users and secondary users.

F. Secondary Spectrum Data Falsification (Ssdf)

This type of attack will occur whenever nodes are not able to identify the available PU's. SSDF attacks can be launched in three ways:

- Denial SSDF: Whenever attacker will advertise about channel unavailability.
- Induce SSDF: whenever attacker falsely advertise about channel occupation.
- Sybil-based SSDF: In this type, the attackers will provide information about the sensing functionalities to other nodes. So that the legitimate nodes believe the malicious nodes will provide correct information about existing PU.

This attack can be mitigated by using the authentication schemes between Fusion Center and sensing SU's.

Table 2: General and Specific Attacks and their Preventions

S.No	Name of Attack	Mechanism for attack prevention
1.	Eavesdropping	- Encrypted and Time stamped messages
2.	Impersonation	- Anonymous ID's
3.	Selective Forwarding	- Time limit strategy
4.	Sinkhole	- Certificates are Introduced
5.	Sybil	- Anonymous ID's - Certificates
6.	Wormhole	- Anonymous ID's - Distances for each node is encrypted
7.	Hello flood	- Certificates - Authentication - Secure Protocols
8.	Hardware	- Hardware Encryption
9.	CR Software	- Tamper Resistance - Virus Detection technique
10.	Primary User Emulation	- Localization Based Defense - Authentication
11.	Jamming Distruption	- Check ID's - Digital Certificates - Authenticate transmitting node
12.	Secondary Spectrum Data falsification	- Authentication scheme between FC and Sensing SU's

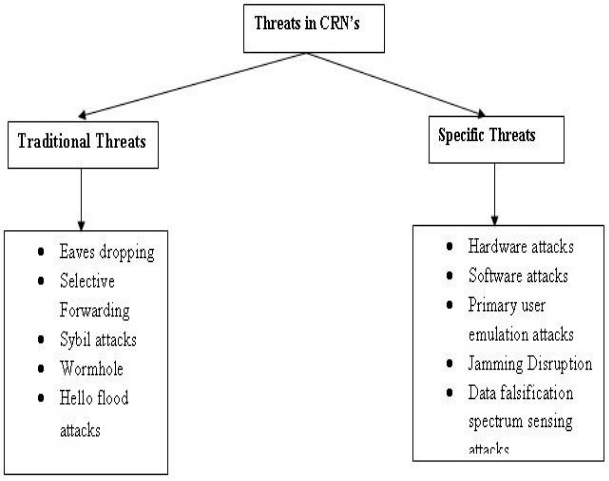

Fig. 4: Threats in CRN's

7. Conclusion

Cognitive radio networks are a rapidly growing area with 1its main characteristics of adaptability, availability, learning, cooperative spectrum sensing and spectrum handoff. This survey mainly concentrates on classification and security attacks in different layers of cognitive networks. As cognitive radio networks are open like wireless networks, we require proper authentication to verify various users and to identify malicious outsiders. In this paper we have identified potential security threatsand attacks in cognitive radio networks. We also provided various counter measures and mitigation techniques to these potential security threats. Security is a long-term research challenge in CRN's. some important research issues are PUE attacks, worm hole attacks, cross layer attacks, dynamic spectrum sensing techniques and many more. all these challenges require further research.

8. Applications and Future Research Directions

CRN's have major applications in all the fields. Some of them are cellular, multimedia, emergency, military, healthcare, smart grid and vehicular networks. The below figure shows its major applications

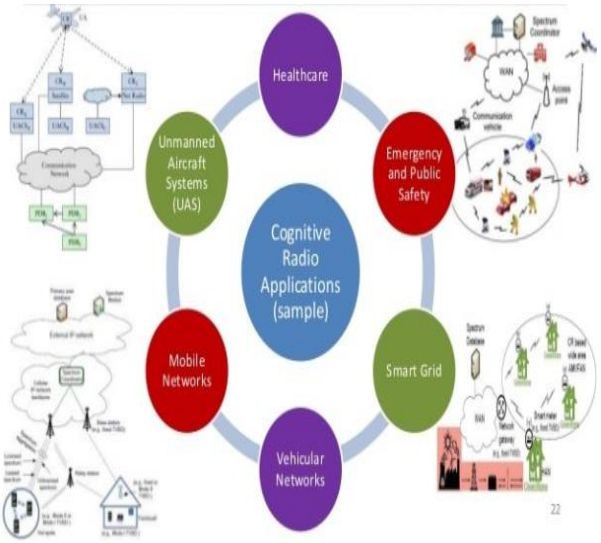

Fig. 5: Applications of CRN's

The researchers have gained more attention towards Routing, security, spectrum sensing and management techniques. In this survey, we present some more research directions which need further attention and investigations to make cognitive networks more useful to the society.

a. Comparison of existing security solutions
b. More focus on cross layer attacks
c. Design efficient spectrum sensing Mechanisms
d. Develop cryptographic algorithms for cognitive networks.
e. Apply Artificial intelligence in cognitive radio networks.

References

[1] J. Mitola and G. Q. Maguire, "Cognitive Radio: Making software radios more personal", IEEE personal Communications, 1989, vol. 6, no. 4, pp. 13-18.

[2] J. Mitola, "Cognitive Radio – An Integrated Agent Architecture for Software Defined Radio", Ph.D. Dissertation, Royal Institute of Technology, Kista, Sweden, May 8, 2000, ISSN: 14035286, 313 pages..

[3] Wassim, S. Haidar and G. Mohsen, "Survey of Security Issues in Cognitive Radio Networks", Journal of Internet Technology, 2011, vol. 12 No. 2, pp. 181-198.

[4] FCC, "Notice for Proposed Rulemaking (NPRM 03-322): Facilitating Opportunities for flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies," ET Docket, No. 03-108, 2003.

[5] D. Sicker and R. Dhillon "Security of Cognitive Radio Networks (Synthesis Lectures on Communications)", Morgan & Claypool Publishers (January 30, 2013), ISBN- 13: 978-1608451005.

[6] Federal Communication Commission, "Unlicensed operation in the TV broadcast bands and additional spectrum for unlicensed devices below 900 MHz in the 3GHz band," ET Docket, No. 04-186, May 2004.

[7] A.G. Fragkiadakis, E. Z. Tragos and I. G. Askoxylakis, "A Survey on Security Threats and Detection Techniques in Cognitive Radio Networks", IEEE Communications Surveys & Tutorials, 2013, vol. 15 , issue: 1 , pp. 428 -445.

[8] S. Parvin, F. K. Hussain, O. K. Hussain, S. Han, B. Tian, and E. Chang, "Cognitive radio network security: A survey", Journal of Network and Computer Applications, 2012, vol. 35, pp. 1691–1708.

[9] O. León, J. Hernández-Serrano, and M. Soriano, "Securing cognitive radio networks", Int. Jr. of Communication Systems, 2010, vol. 23, Issue 5, pp. 633-652.

[10] T. C. Clancy and N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation", CrownCom 2008, 3rdInternational Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2008, pp. 1 – 8.

[11] T. R. Newman and T. C. Clancy, "Security threats to cognitive radio signal classifiers", Proceedings of the Virginia tech wireless personal communications symposium, 2013, pp. 1-9.

[12] K. C. Chen, Y. J. Peng, N. Prasad, N., Liang, Y. C. and S. Sun "Cognitive radio network architecture: part I. general structure", 2nd international conference on ubiquitous information management and communication, 2008, CRs. pp.114–119.

[13] R. Chen and J. Park, "Ensuring Trustworthy Spectrum Sensing in Cognitive Radio Networks", 1st IEEE workshop on Networking Technologies for Software Defined Radio Networks,(SDR '06), 2006, pp. 110 – 119.

[14] R. Chen, J. Park, Y. T. Hou and J. Reed, " Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks", IEEE Communications Magazine, 2012,vol. 46, issue. 4, pp. 50-55.

[15] R. Chen, J. Park and J. H. Reed, "Defense against Primary user Emulation Attacks in Cognitive Radio Networks", IEEE Journal on selected areas in communications, vol. 26, no.1, 2008, pp. 25-37.

[16] A. Safdar and M. O'Neill, "Common Control Channel Security Framework for Cognitive Radio Networks", 69th IEEE Vehicular Technology Conference, 2009, pp. 1-5.

[17] J. L. Burbank, "Security in Cognitive Radio Networks: The Required Evoluation in Approaches to Wireless Network Security", CrownCom 2008, pp. 1-7.

[18] D. Cabric, S. M. Mishra and R. W. Brodersen, "Implementation Issues in Spectrum Sensing for Cognitive Radios", 38th Asilomar Conference on Signals, Systems and Computers, 2004, pp. 772-

776.
[19] “IEEE 802 Tutorial: Cognitive Radio”, Scott Seidel, Raytheon, presented at IEEE 802 Plenary, 18 July 2005.
[20] T. R. Shields, "SDR Update," Global Standards Collaboration, Sophia Antipolis, France, Powerpoint Presentation GSC10_grsc3 (05)20, 2005.
[21] R. W. Thomas, L. A. DaSilva and A. B. MacKenzie, "Cognitive networks," IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, November, 2005, pp. 352-360.
[22] FDR Forum, Cognitive Radio Definitions and Nomenclature, Approved Document SDRF-06-P-0009- V1.0.0, 10 September 2016.
[23] N. Mathur and K. P. Subbalakshmi, “Security issues in cognitive radio networks”, Cognitive networks: towards self-aware networks. John Wiley and Sons, Ltd; 2007.
[24] N. Mathur and K. P. Subbalakshmi, “Digital signatures for centralized DSA networks”, 4th IEEE conf. on consumer comm. and networking, 2007, pp. 1037–1041.
[25] Y. B. Reddy, “Solving Hidden Terminal Problem in Cognitive Networks Using Cloud Application”, SENSORCOMM 2012, pp. 235-240.
[26] Y. B. Reddy and S. Ellis, “Modeling Cognitive Radio Networks for Efficient Data Transfer Using Cloud Link”, ITNG 2013, April 2014, Las Vegas, USA.
[27] M. Shahid and J. Kamruzzama, “Agile spectrum evacuation in cognitive radio networks”, IEEE international conference on communications (ICC), 2015, pp. 1–6.
[28] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks & Soft Computing,ISSN:978-1-4799-3486-7/14,pp.270, August2014.
[29] T. Padmapriya and V. Saminadan, “Inter-cell Load Balancing technique for multi-class traffic in MIMO-LTE-A Networks”, International Journal of Electrical, Electronics and Data Communication (IJEEDC), ISSN: 2320- 2084, vol.3, no.8, pp. 22-26, Aug 2015.
[30] S.V.Manikanthan and V.Rama“Optimal Performance Of Key Predistribution Protocol In Wireless Sensor Networks” International Innovative Research Journal of Engineering and Technology ,ISSN NO: 2456-1983,Vol-2,Issue –Special –March 2017.
[31] S.V.Manikanthan and D.Sugandhi “ Interference Alignment Techniques For Mimo Multicell Based On Relay Interference Broadcast Channel ” International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume- 7 ,Issue 1 –MARCH 2014.