Security Issues in Cognitive Radio Networks

Abstract: *Cognitive radio technology is the field of wireless communication networks that enhances the spectrum management and effective utilization while offering many social and individual benefits. The objective of the cognitive radio network technology is to utilize the unutilized spectrum by primary users and fulfill the secondary users' demands irrespective of time and location (any time and any place). Due to their flexibility, the cognitive radio networks are vulnerable for numerous threats and security problems that will affect the performance of the network. Little attention was given to security aspects in cognitive radio networks that include spectrum sensing (sensing primary user), attacks that threaten the network at various layers and adversary effects on performance due to the security threats. In this survey, we discuss the cognitive radio networks, problems involved in sensing and management, attacks on cognitive radio networks, attacks on various network layers and threats on cognitive radio networks,.*

I INTRODUCTION

The first idea of cognitive radio in wireless transmission was given by Joseph Mitola in 1998. with an aim to provide appropriate intelligence to portable devices so that they cater to communication needs. The portable device is required to detect open channels in the wireless spectrum band and auto-adjust its parameters according to user needs.

The main purpose of the sensory radio is to detect white spaces (unused spectrum or spectrum) in the first measure of the optimal use of that unused acquired area without harming the main user. Sent signal detection can be done using one or more of the techniques including a simulated filter, power acquisition, cyclostationary element detection, co-acquisition (sensing spectrum with the cooperative effort for multiple sensory radiation), and an internally based visual detection method.

Cognitive Radio Network Security includes anonymous discovery and false user acquisition. False detection that primary signal detection is recorded when the signal is missing (false detection) In addition, false detection includes malicious users pretending to be the primary user (PU) by sending a strong signal to others users of understanding. Misdetection involves the presence of a primary user undetected by the cognitive user via a matched filter.

In wireless networks, hacking and malicious attacks In addition, security is inevitably threatened, and includes security resources due to its nature of openness. Better security measures ensure the soundness of the wide range. Adoption problems apply when they operate in a hostile environment. In case of a hostile environment, it is possible to replicate the existing status symbols and make them (simulate the original features) as the first user. In such cases, integrating the official senders of the first and second users to the spectrum sensitivity will improve the reliability of the acquisition process

II RELATED WORK

Most of the test papers on understanding radio networks (CRN) discuss security issues in certain aspects of the network. Research conducted on CRN reflects the state of the art research in certain or a few common areas. Fragkiadakis et al [1] discussed security threats and CRN detection strategies. This paper covers the challenges posed by perceptual radios as well as cognitive radio networks as well as the current state of finding parallel attacks.

Newman and Clancy [2] discussed security threats in the classifiers classifiers. They discussed the signal separation model, threats analysis, and feature release threats.They say the signal separation algorithm opens up a new area of security research related to access to a powerful spectrum and signal segregation. They used a signal separation algorithm to distinguish primary user (PU) and secondary user signals. Chen et al [3] devised a defense system to identify vulnerable users by measuring location information and viewing signal strength. Spectrum sensitivity is also reported by Chen et alin [4, 5]. In [4], the authors discussed the main user simulation problem and showed disturbing effects on comprehension radio networks.

The implications for the implementation of radio sensory in sensory radiation were discussed by Cabric et al in 2004 [6]. The authors pointed out that the detection of a cyclostationary element has a significant advantage between parallel filtering and power acquisition due to its ability to distinguish measured signals, disturbances, and low noise levels. The process of acquiring Energy to acquire a key signal became a major problem for security threats and security performance focused on recent years in the analysis of basic signal simulation. Chen et al [3] has used a variety of techniques that include LocDef's basic signal simulation to eliminate false and inaccurate detection. Newman and Clancy [7] discussed the security threats in signal classifiers. They discussed the signal classifier model, threat analysis, and threats on feature extractions. They discussed it as a new area of research and said that it would lead to some very interesting possibilities in this realm.

III COGNITIVE RADIO NETWORK ENVIRONMENT AND SECURITY

One of the main requirements for understanding networks is their ability to scan the spectral band and identify the vacant channels available for opportunistic transmission. Since the pri-mary user network is physically different from the second user's network, secondary users do not receive direct feedback from key users regarding their transfers.Usual users must rely on individuals or their abil-ity partners to get primary user submissions. As early users can spread across a large area, hearing the entire spectral group accurately is a challenging task [1] [7]. Secondary users should rely on weak transmission signals that are weak to measure their presence. Most research on spectrum sensor techniques falls into three categories: transmitter detection, co-detection and interference-based detection. The main aim of all these methodologies is to avoid interference to primary transmissions. The interference temperature, amount of interference caused by all the secondary users at a point in space, should be below a specified threshold in the proximity of the primary users. This seems like a simple task, it is quite hard to achieve since the location of primary users is unknown to the secondary users. Also, when multiple networks overlap, the users should not confuse the transmission from other secondary users with their primary transmissions.

The number of users along with the frequency range set each network apart from it's other counterparts. When a list of spectrum bands is available to the secondary users, they choose the most appropriate bands for themselves. Spectrum mobility is the agility of cognitive networks to dynamically switch between spectrum access. The availability of vacant spectrum bands frequently changes over time hence the designing of cognitive protocols requires a key knowledge of spectrum mobility. Spectrum handoff, the delay incurred during handoff, is the main factor used in deciding the spectrum mobility. Another important factor to be considered is the time difference between the secondary network detecting a primary transmission and the secondary users vacating the spectral band and they also cause some strong interference to the primary users.

IV TYPES ON COGNITIVE NETWORKS

In a centralized architecture, the network is divided into cells and each cell is managed through another secondary base station. The medium access and the secondary users are controlled by this secondary base station. There is an option of connecting the secondary base stations through a wired backbone network.

In Decentralized architecture, the secondary users communicate with each other on a need-to basis. Users within range exchange the information directly and those outside of their range share the information through multiple hops. Decentralized networks are further segmented into spectrum sharing networks, which has two wireless networks coexisting in an unlicensed band. In such a network, a common spectrum management system is implemented to help exchange the control information on transmitter and receiver parameters. Since these are decentralized they don't require primary user verification, spectrum mobility and management functions.

V ATTACKS ON COGNITIVE NETWORKS

We define cognitive network attacks as any activity that results in (a) unacceptable conflicts with key licensed main users or (b) missed opportunities for secondary users. Attacks are considered strong if they involve a small number of opponents performing small tasks but result in high damage / loss of initial support or support to the network.

V A Physical Layer based Attacks

Physical layer is present at the bottom of the protocol stack.In fact it is one of the simplest layers that determines bit rate, bandwidth and channel capacity of a network. Some of the attacks on cognitive networks that target the physical layer:

Sensitivity Amplifying Attack

Attacks are considered strong if they involve a small number to prevent interference to the main network, other key user acquisition methods have high sensitivity to the primary transmission (see Section 4). This leads to false discovery and missed opportunities for secondary users. A lucky business can increase sensitivity which is why the number of opportunities missed by re-introducing basic transfers to opponents doing small tasks but causing significant damage / loss to first and second-time users on the network.

Primary Receiver Jamming Attack

Lack of information about the location of the primary recipients can be used for the purpose of causing serious disruption to the primary recipient of the victim. The attack was triggered when a threat actor close to the victim's primary recipient participated in a collaborative protocol and requested referrals from other users to be targeted at the malicious user.

V B Link Layer based Attacks

Link layer lies above the physical layer on the network protocol stack. This is responsible for data compression,fragmentation and modulation. It provides the functionality to transfer data between network entities with a system that can possibly detect and correct errors in the physical layer.

Asynchronous Sensing Attack

Instead of synchronizing the hearing function with other secondary users in the network, the malicious second user may transfer syncally while other secondary users perform sensory functions. If the primary channel or other secondary users view it as a transfer from the main user, then this may lead to lost opportunities.

Biased Utility Attack

A second malicious user can selfishly reduce user usage limits to increase its bandwidth. If secondary users and / or base stations are unable to contain such behavior, this could lead to the depletion of the transmission system for other secondary users. If a malicious user adjusts its utility function for transmission at higher power, it will result in other users getting less bandwidth. Some secondary users may lose transmission ability too.

V C Network Layer based Attacks

The network layer in the OSI model is responsible for routing of packets from source to destination.Every node in the network is responsible for keeping track of traffic (usually in the form of a table) about neighboring locations. When a connection is to be established, every node decides which of its neighbors should be the next link in the path to your destination. Some of the router protocols used in wireless for example are dynamic source routing (DSR) and ad-hoc on demand vector (AODV) routing [32]. A malicious node in route can disrupt a route by spreading incorrect route information to its neighbors or by redirecting packets incorrectly. Several channel attacks have been found on ad-hoc wireless networks, most attacks can be divided into two categories: retrieval of disruptive attacks and resource use attacks which will be primarily discussed below.

Network Endo-Parasite Attack

Network Endo-Parasite Attack assumes the presence of at least one fixed or malicious node in a network. Trojanised nodes are trying to increase interference on overloaded chan-nels. Most of the time, the affected links are in the pathway through the malicious nodes near the cable gate; Attack therefore takes the name of an insect attack.Under normal channel operation, a node provides at least uploaded channels under the interface and transmits the latest information to its domain neighbors. The compromised node introduces NEPA by providing its connectors with the most important channels. However, they do not inform their neighbors of the change. As information is passed on to neighbors, the network remains unaware of the change. It causes hidden use of heavily loaded channels

Channel Ecto-Parasite Attack

It is a modified version of the NEPA attack in which a captured node will launch this attack by switching interfaces to the channel using the highest priority link. This is an easy to perform attack but has severe effects.

V D Transport Layer based Attacks

It is the fourth layer in the OSI model and responsible for end to end network communication. It also ensures that data packets are received in the same sequence as they are sent. UDP (User Datagram Protocol) and TCP (Transmission Control Protocol) are two protocols that are used in this layer. UDP is connectionless, which means we don't have receipt of packet delivery. TCP is connection oriented protocol and guarantees ordered packet delivery.

Key Depletion Attack

Unusually high travel times and frequent relapses suggest that hole layer transfer sessions in cognitive networks last only a short time. This results in an increase in the number of sessions initiated for any given application. Most automotive security systems such as SSL and TLS establish cryptographic keys at the beginning of each transition layer. A higher number of times in understanding networks and where the number of key institutions will increase the chances of using the same key twice. Key duplication can be used to break the basic cipher system

V E Application Layer based Attacks

Application layer stands at the top of the OSI model and provides users basic services such as File Transfer Protocol, email, SMB etc. Qos (Quality of Service) is one of the main parameters in this layer and is of prime importance to multimedia applications. Network delay in lower layers due to unnecessary routing is the main cause of Qos degradation in application layer attack.

VI Defenses against the attacks

Some of the Cognitive Radio Network Challenges are Spectrum sensation, Spectrum management and display distribution.Initial signal analysis is suggested in the current survey.For example, a malicious threat actor interprets the primary user signal and uses the selfish use category. These attacks can be detected by the transmitter verification process and location verification procedures. Alternatively, cognitive usersimulatesthe primary user for personal gain.That is, discerning user limits These activities can be controlled using a variety of practices and access limits. This problem can be fixed using the honey pot database to mislead the malicious user.

Acquisition of the main user signal is difficult when using signal spread or changing parameters by a dangerous user.These problems can be solved using cloud application. The spectrum can be easily achieved through multiple users in a collaborative way. and transactional integrity. This method provides security and the problem of storing hidden terminal remains. Jamming Problem, hidden storage problem, key exchanges between bumps and malicious user actions can be eliminated using the cloud system.Security on cloud remains an open problem.Harmful activity may appear outside or between users of understanding. Detection of malpractice among cognitive users can be done using internal detection procedures and capturing bee information.

In addition, the shortcut technology used is fitted with communication technology that will attack the upper layer attacks. Incorporating the cryptographic techniques or digital signature basedprint signal identification can help differentiate malicious users. Additional functionality is required in this guide.The spectrum flow includes a standard control channel, operating frequency range, and location information. Requires the current location of the first operating system and user functionality so that the second user can emit the captured rays as soon as the PU enters. Dependent visibility depends on the basic user login and the basic user migration.The cloud application will solve many attacks and hidden storage problems in high-resolution cognitive networks such as sudden first user entry.

VII CONCLUSION

The literature shows that the spectrum management schemes lack formal security models. Finally we conclude that the threat proof mechanism is difficult and impossible. Cognitive radio networks and wireless networks lay a huge emphasis on threat detection and protection mechanisms. Therefore it is recommended that threat detection mechanisms must be developed and incorporated as a part of spontaneous need. The study shows that security at each layer of every network is crucial as any one of them might lead to sabotaging the entire network, leading to a loss of the users, both primary and secondary.

VIII REFERENCES

1. 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.
2. T. R. Newman and T. C. Clancy, “Security threats to cognitive radio signal classifiers”, Proceedings of the Virginia tech wireless personal communications symposium, 2009, pp. 1-9.
3. 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
4. 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.
5. R. Chen, J. Park, Y. T. Hou and J. Reed, “ Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks”, IEEE Communications Magazine, 2008,vol. 46, issue. 4, pp. 50-55.
6. 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.
7. T. R. Newman and T. C. Clancy, “Security threats to cognitive radio signal classifiers”, Proceedings of the Virginia tech wireless personal communications symposium, 2009, pp. 1-9.