International Journal of Advanced and Innovative Research (2278-7844) / # 1/

Volume 6 Issue 11

A Survey Study on Secure Dynamic Spectrum Sensing Techniques in Cognitive Radio Sensor Networks

C.Theebendra[1], Dr.T.Ramaprabha[2]

Research Scholar, PG & Research Department of Computer Science and Applications[1]

Vivekanandha College of Arts and Sciences for women (Autonomous), Namakkal, Tamilnadu, India

Professor, PG & Research Department of Computer Science and Applications[2]

Vivekanandha College of Arts and Sciences for women (Autonomous), Namakkal, Tamilnadu, India

theebendra@gmail.com[1], ramaradha1971@gmail.com[2]

Abstract - The enormous development in Wireless Communications has added to an immense request on the sending of new remote administrations and their applications prompts range shortage in both licensed and unlicensed frequency spectrum. Cognitive Radio Technology is utilized to get to the inaccessible range proficiently by designating the range to the unlicensed clients i.e. Secondary Users (SU) when it is not utilized by the licensed users i.e. Primary Users (PU). Be that as it may, the system is defenseless against new sorts of security dangers because of the circulated idea of helpful range detecting. The present range does not give security system to alleviate against these attacks. This proposed framework researches different attacks and security component for the future upgrading in Cognitive Radio Sensor Networks (CRSN).

Keywords - Cognitive Radio System, Dynamic Spectrum Access(DSA), Cognitive Radio Sensor Networks(CRSN), Security component, Cooperative Spectrum Sensing(CSS).

I. INTRODUCTION

The enormous development in access of dynamic range inadequacy is the disadvantage. To keep away from the spectrum insufficiency in Networks CRNs is used. It's accustomed sight the unused spectrum to sense the bandwidth. The use of available spectrum will be allotted dynamically by changing its parameters using Cognitive Radio Networks. The Primary client will get to the range whenever because of they are the approved clients. But, the Secondary user could entrée into the spectrum animatedly when the spectrum is unutilized by Primary users. The unused spectrum are distinguished by Cognitive Radio Networks and allotted for the secondary users. They are called spectrum holes and also known as White spaces. Various security attacks and threats are concerned during the bandwidth allocation in Cognitive Radio Networks.

II. COGNITIVE RADIO SENSOR NETWORKS (CRSN)

Cognitive Radio Sensor Network (CRSN) is one of the circulated organize, works with the assistance of intellectual radio remote sensor nodes. It detects the flag and powerfully impart their readings over the accessible range groups, in the end to fulfill the application particular prerequisites. The transmission parameters are changed and assigned powerfully with the assistance of sensor hubs. Cognitive Radio is a methodology which is used for viable correspondence of range by using Dynamic Spectrum Access. The optional clients are permitted to get to the range without corrupting the execution of the range of essential clients. It might happen in time, recurrence, and space areas. DSA is utilized to manage the range in CRSNs in proficient way. Along these lines, the individual SU ought to experience a subjective cycle, appeared in **Fig.1**, with the accompanying capacities:

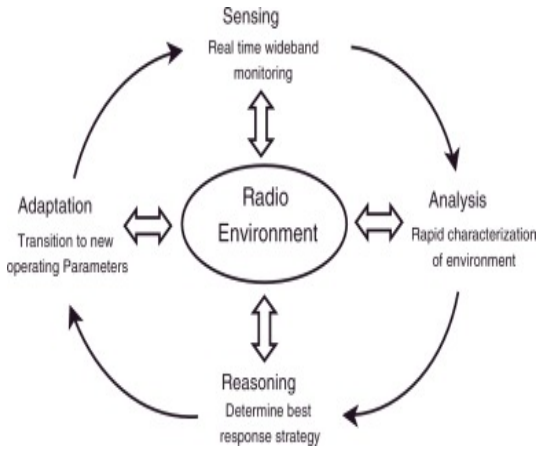

Fig.1: The Cognitive Radio Cycle

- ***Sensing the Spectrum:***

By finding the idle Spectrum, spectrum sharing is done without harmful interference of the primary users.

- ***Analyzing the Spectrum:***

Spectrum scheduling method is followed fairly among co-existing CR users.

- ***Managing the Spectrum****:*

To meet the requirements of the user the optimal accessible spectrum is captured.

- ***Spectrum Mobility:***

It is achieved by maintaining seamless communication on requirements of spectrum better, during the transition.

The main characteristics of DSA is Spectrum Sensing that may be implemented by using numerous strategies based on power detection, matched filter, and wavelet detection. Non Co-operative and Co-operative sensing classification is accomplished by utilizing existing spectrum detecting techniques by method of permitting the trading of the range measurements among more than on CR. The execution of spectrum sensing is misrepresented with the guide of clamor vulnerabilities, multipath blurring and shadowing. The consistency of range detecting is enhanced by methods for Co-operative Spectrum sensing Technology.

Censoring, Clustering and user Selection methods were used to implement CSS as Centralized or Decentralized. In the first one, the sensing report from multiple SUs are collected by central controller to know vacancy of the spectrum bandwidth. To access the predefined channel the data is sent to SU by utilizing decision fusion rules. In second one, SUs trade their detecting reports among themselves without requiring a centralized infrastructure

III.ATTACKS IN COGNITIVE RADIO NETWORKS

There are numerous attacks in Cognitive Radio Networks, by which few are categorized through the three major layers. They are Physical Layer, Data Link Layer and Network Layer.

A. Physical Layer:

i) The Physical Layer is the lower most layer which gives interfaces to the transmission medium. It is utilized to convey two system devices, utilizing Fiber optics in Cognitive Radio Networks. In Cognitive Radio, the procedure is more convoluted when contrasted with different Wireless Networks in due to dynamic distribution of the spectrum.

ii) Primary User Emulation Attack (PUEA):

The CRN needs capability to differentiate the signals of Primary and Secondary user within the PUEA. In order to vacate the spectrum, an attacker might regulate their interfaces such as it emulates the Primary user signals characteristics inflicting alternative Secondary users to incorrectly verify that frequency is in use by the PU. The pretender might attack egotistically, by using the spectrum the alternative legal users can have their communication discontinuous, leading to the denial of service attack.

B. Data Link Layer Attacks:

Spectrum Sensing Data Falsification (Byzantine Attack):

The Byzantine attack is also alluded as Spectrum

Sensing Data Falsification. Here an aggressor mix the false detecting data into the decision stream of the framework. Byzantine may do the attacks egotistically by gaining expanded range accessibility for themselves. Likewise the aggressors may have an objective of disturbing the throughput of the system for different reasons as delineated in **Fig.2.**

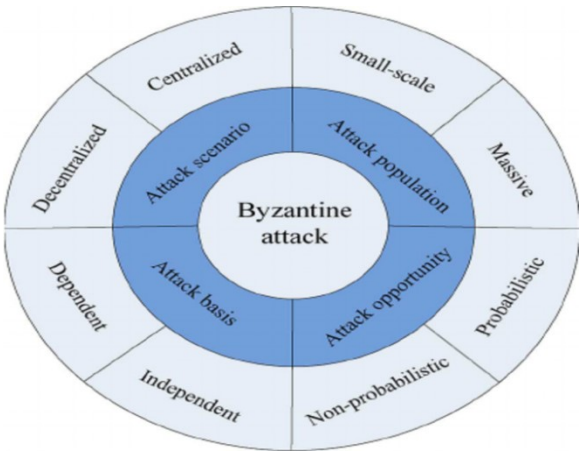

Fig.2: A taxonomy of Byzantine attack parameters

The characteristics of Byzantine attack is flexibility and diversity. It is categorized on the origin of four parameters. They are attack scenario, attack basis, attack opportunity and attack population which means where, how, when and who to attack is the concept.

C. Network layer Attacks:

The Network Layer is liable for sending packets from source to destination for keeping up nature of administration and furthermore performs fragmentation and reassembling of packets. The CRN gives security issues to the exemplary wireless communication because of the shared architecture of the Mesh Adhoc Network.

Wormhole Attack:

Here, an attacker tunnel messages got in one a branch of the system over low inaction interface and the messages are replayed in another branch of the system. These are normally administrated by noxious nodes that comprehend the partition among them by handoff packets along an out-of-bound channel that is not accessible to alternate nodes.

III.MITIGATION OF ATTACKS IN COGNITIVE RADIO NETWORKS

The mitigation of attacks can be carried out using four steps. Initially, it has the adaptability to check verification among the nearby nodes shaping the CRSN. Second, ready to swap data among different SUs in strong and secure manner. Thirdly, it has the flexibility to concede the data among various SUs. At last, we have a pattern to think about the conduct of the different nodes in the system.

IV.CONCLUSION

The Mitigation of attacks was not carried out by current spectrum sensing techniques. Then again, CRSN have exact requesting circumstances because of the natural resource limitations of sensor nodes preparing request and extra correspondences constrained by CR, effective low power sensor nodes and communications over licensed and unlicensed spectrum. These are the different difficulties for the advancement of such security mechanisms. The execution of security defense mechanism could be established through simulations in the future work.

REFERENCES

[1] M.Padmadas, Dr.N.Krishnan and V.Nellai Nayaki, "Analysis of attacks in Cognitive Radio Networks" in International Journal of Computer Science and Engineering (IJARCEE), Vol 4, Issues 8 Aug 2015, DOI: 10.17148/IJARCCE.2015.4835.

[2] Laila Nassef and Reemah Alhebshi, "Secure Spectrum Sensing in Cognitive Radio Sensor Networks: A Survey" in International Journal of Computational Engineering and Research (IJCER), ISSN(e):2250-30005, Volume 06 Issue 03, March 2016.

[3] Linyuan Zhang, Guoru Ding, and Yulong Zou, "Byzantine Attack and Defense in Cognitive Radio Networks" in IEEE Communications survey and tutorials, 1553-877X© 2015IEEE. DOI:10.1109/COMST.2015.2422735.

[4] R. K. Dubey and G. Verma, "Improved Spectrum Sensing for Cognitive Radio Based on Adaptive Threshold," in Second International Conference on Advances in Computing and Communication Engineering (ICACCE), Dehradun, 1-2 May, 2015, DOI: 10.1109/ICACCE.2015.70.

[5] X. Zhang, X. Liu, H. Samani and B. Jalaian, "Cooperative Spectrum Sensing in Cognitive Wireless Sensor Networks," International Journal of Distributed Sensor Networks,13 April 2015, Article ID 170695, http://dx.doi.org/10.1155/2015/170695.