ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 4, April 2013

AN EFFICIENT COMMUNICATION AND SECURITY FOR COGNITIVE RADIO NETWORKS

A.Amarnath prabhakaran[1], A.Manikandan[2]

PG Student [Comm.System], Dept. of ECE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India [1]

Assistant professor, Dept. of ECE, M.Kumarasamy College of Engineering, Karur, Tamilnadu, India [2]

ABSTRACT: A cognitive radio(CR) is a transceiver which automatically detects available channels in wireless spectrum and accordingly changes its transmission or reception parameters. In this paper, it proposes an algorithm for the energy-efficient and spectrum- aware communications requirements in CR network. It enables each node to determine and regulate its transmission strategy to provide minimum energy consumption without sacrificing end-to-end delay performance and also maximizes overall spectrum utilization. Spectrum sensing is one of the essential parameter to be considered in CR networks. Therefore, the security aspect of spectrum sensing should be addressed well. Using a Trust-Worthy algorithm, it improves the trustworthiness of the Spectrum sensing in CR-Networks. It implemented using Network Simulator-2.

Keywords: Cognitive Radio, Spectrum Sensing, Efficient Communication, System Security.

I.INTRODUCTION

One of the primary objectives of cognitive radio (CR) ad-hoc networks is to facilitate an efficient utilization of spectrum resources without interfering with the primary user networks.CR-Network allows intermittently connected mobile unlicensed nodes to exploit temporarily available contacts and idle licensed channels for end-to end message delivery. Cognitive Radio (CR) is a key technology to realize Dynamic Spectrum Access (DSA) that enables an unlicensed user (or, secondary user) to adaptively adjust its operating parameters and exploit the spectrum which is unused by licensed users (or, primary users) in an opportunistic manner. However, the realization of CR-Networks also brings crucial research challenges that must be addressed. In particular, due to different node mobility and spectrum availability patterns, CR-Networks is frequently divided into unpredictable partitions. These partitions are essentially intermittently-connected and deficient in complete end-to-end paths. Hence, spectrum-aware flooding (SAF) is more relevant for CR-Networks. In SAF, a message is first copied to a set of path nodes using available channels. Then, one of these path nodes delivers the message to the destination provided that it encounters. Clearly, if the message is tried to be copied to all paths that do not have the message the end-to-end message delay can be minimized. However, such a forwarding strategy is energy-inefficient and may cause a severe interference to primary user system. Hence, it is necessary to decide which path nodes and licensed channels should be used to mitigate the energy consumption and high interference for an efficient communication in CR-Networks.

In this paper, it proposes efficient communication between CR nodes and spectrum utilization. Secondly the security concerns of spectrum sensing to ensure trustworthiness. It uses two selection schemes called node selection scheme (NSS) and channel selection scheme (CSS). The aim of NSS is to allow each node to check its gain in copying a message to a relay while examining its transmission effort. Using NSS, each node decides which paths should be used in order to provide minimum energy consumption without sacrificing end-to-end delay performance. Based on CSS, each node decides and switches to a licensed channel to maximize spectrum utilization while keeping the interference in a minimum level. This eventually enables CR-Networks nodes to determine optimum path nodes and channels for an efficient communication in CR-Networks. The CR technology allows Secondary Users (SUs) to seek and utilize "spectrum holes" in a time and location-varying radio environment without causing harmful interference to Primary Users (PUs). This opportunistic use of the spectrum leads to new challenges to the varying available spectrum. Using a Trust-Worthy algorithm, it improves the trustworthiness of the Spectrum sensing in CR-Networks.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 4, April 2013

II.SYSTEM MODEL AND ASSUMPTIONS

It considers a network with N mobile unlicensed nodes that move in an environment according to some stochastic mobility models. It also assumes that entire spectrum is divided into number of M non-overlapping orthogonal channels having different bandwidth. The access to each licensed channel is regulated by fixed duration time slots. Slot timing is assumed to be broadcast by the primary system. Before transmitting its message, each transmitter node, which is a node with the message, first selects a path node and a frequency channel to copy the message. After the path and channel selection, the transmitter node negotiates and handshakes with its path node and declares the selected channel frequency to the path. The communication needed for this coordination is assumed to be accomplished by a fixed length frequency hopping sequence (FHS) that is composed of K distinct licensed channels. In each time slot, each node consecutively hops on FHS within a given order to transmit and receive a coordination packet. The aim of coordination packet that is generated by a node with message is to inform its path about the frequency channel decided for the message copying.

Furthermore, the coordination packet is assumed to be small enough to be transmitted within slot duration. Instead of a common control channel, FHS provides a diversity to be able to find a vacant channel that can be used to transmit and receive the coordination packet. If a hop of FHS, i.e., a channel, is used by the primary system, the other hops of FHS can be tried to be used to coordinate. This can allow the nodes to use K channels to coordinate with each other rather than a single control channel. Whenever any two nodes are within their communication radius, they are assumed to meet with each other and they are called as contacted. In order to announce its existence, each node periodically broadcasts a beacon message to its contacts using FHS. Whenever a hop of FHS, i.e., a channel, is vacant, each node is assumed to receive the beacon messages from their contacts that are transiently in its communication radius.

III.EFFICIENT COMMUNICATION

In this scheme, each node with message searches for possible path nodes to copy its message. Hence, possible path nodes of a node are considered. Using NSS, each node having message selects its path nodes to provide a sufficient level of end-to-end latency while examining its transmission effort. Here, it derives the CSS measure to permit CR-Networks nodes to decide which licensed channels should be used. The aim of CSS is to maximize spectrum utilization with minimum interference to primary system. Assume that there are M licensed channels with different bandwidth values and y denotes the bandwidth of channel c. Each CR-Networks node is also assumed to periodically sense a set of M licensed channels. Mi denotes the set including Ids of licensed channels that are periodically sensed by node i. suppose that channel c is periodically sensed by node i in each slot and channel c is idle during the time interval x called channel idle duration. Here, it use the product of channel bandwidth y and the channel idle duration x, tc = xy, as a metric to examine the channel idleness. Furthermore, failures in the sensing of primary users are assumed to cause the collisions among the transmissions of primary users and CR-Networks nodes.

IV.SECURITY

Spectrum sensing: Detecting unused spectrum and sharing it, without harmful interference to other users; an important requirement of the cognitive-radio network to sense empty spectrum. Detecting primary users is the most efficient way to detect empty spectrum. Spectrum-sensing techniques may be grouped into three categories:
Transmitter detection: Cognitive radios must have the capability to determine if a signal from a primary transmitter is locally present in a certain spectrum. There are several proposed approaches to transmitter detection:
1. Cooperative detection: Refers to spectrum-sensing methods where information from multiple cognitive-radio users is incorporated for primary-user detection.
2. Interference-based detection.
Since primary user networks have no requirement to change their infrastructure for spectrum sharing, the task falls to CRs as secondary users to detect the presence of primary users through continuous spectrum sensing. Spectrum sensing by CRs can be conducted either individually or cooperatively. Recently, the efficacy of cooperative spectrum sensing has gained a great deal of attention. There are several advantages offered by cooperative spectrum sensing over the non-cooperative methods. However, due to the randomness of the appearance of PUs, it is extremely difficult to achieve fast and smooth spectrum transition leading to limited interference to PUs and performance degradation of SUs. Locally collected and exchanged spectrum sensing information is used to construct a perceived environment that will impact CR behaviour. This opens opportunities to malicious attackers. In cooperative spectrum sensing a group of secondary users perform spectrum sensing by collaboratively exchanging locally collected information. Malicious secondary users may take advantage of cooperative spectrum sensing and launch attacks by sending false local spectrum sensing results to others, resulting in a wrong spectrum sensing decision. Two known security threats in CRs are Selfish Primary User Emulation (SPUE) and Malicious Primary User Emulation (MPUE) attack. These types of attacks emulate signals with the characteristics of incumbent primary users to fool other secondary users.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 4, April 2013

SPUE: In this attack, an attacker's objective is to maximize its own spectrum usage. When selfish attackers detect a vacant spectrum band, they prevent other secondary users from competing for that band by transmitting signals that emulate the signal characteristics of primary user signals. This attack is mostly carried out by two selfish secondary users.

MPUE: In this attack, the objective is to obstruct the DSA process of SUs- i.e., prevent SUs from detecting and using vacant licensed spectrum bands, causing denial of service.

Using the Trust-Worthy algorithm it defines a threshold value to the SUs to overcome the PUE attacks. It enables CR-Networks nodes to efficiently utilize the available spectrum channels. Nodes, which can easily find various licensed channel opportunities without interfering the primary system increases. This reveals that it has a potential to be able to convert the various network conditions into a performance improvement.

V. RESULT AND DISCUSSION

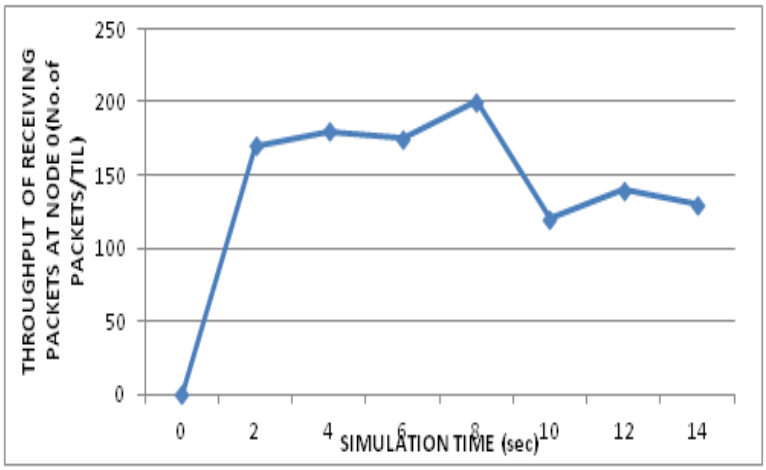

Fig. 1 Simulation time vs Throughput of receiving packets

In the fig 1, it shows the graph of time Vs throughput of receiving packet. Throughput is the average rate of successful message delivery over a communication channel.

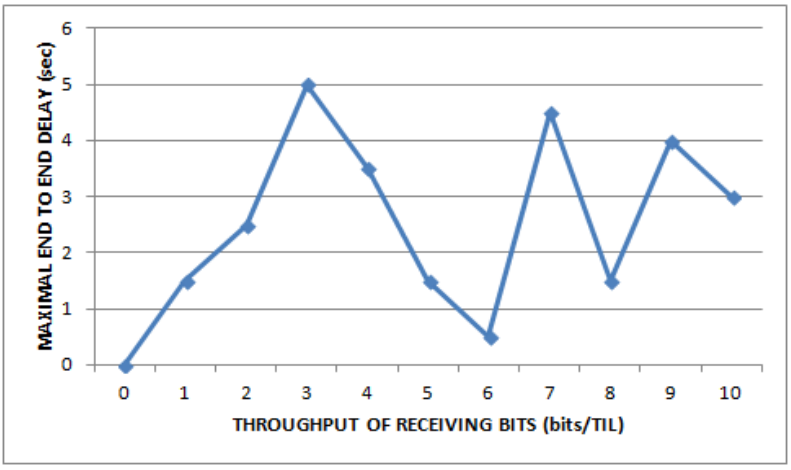

Fig. 2 Throughput of receiving bits vs Maximal end to end delay

In the fig 2, it shows the graph of throughput of received bits Vs Maximal end to end delay. End to end delay is the time taken by a packet to travel from source to reach destination.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering
Vol. 2, Issue 4, April 2013

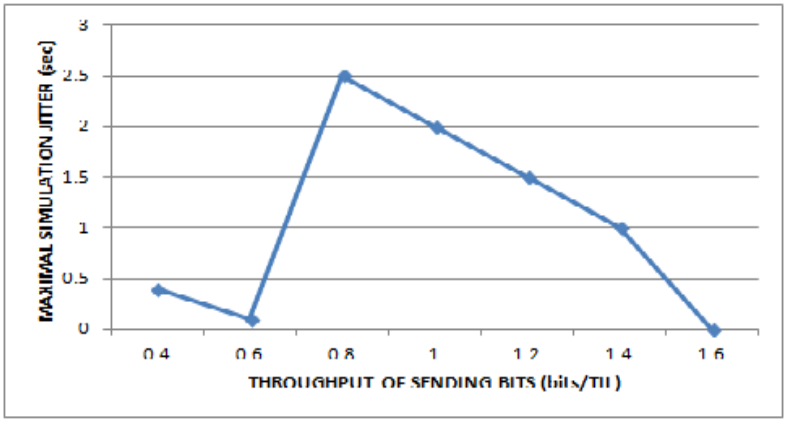

Fig .3 Throughput of sending bits Vs Maximal simulation jitter

In Fig 3, Throughput of sending bits Vs Maximal simulation jitter. Jitter is the undesired deviation from true periodicity of an assumed periodic signal. Jitter period is the interval between two times of maximum effect (or minimum effect) of a signal characteristic that varies regularly with time.

VI.CONCLUSION

Thus it allows each node with message to decide whether to copy the message to a path node by optimizing its transmission effort in order to provide a sufficient level of message delay. Using a channel selection scheme provides spectrum utilization while it minimizes the interference level to primary system. Using trustworthy algorithm, it improves the trustworthiness of the Spectrum sensing in CR-Networks. It enables network nodes to adaptively regulate their communication strategies according to dynamically changing network environment.

REFERENCES

[1] K. R. Chowdhury, M. Di Felice, "Search: a routing protocol for mobile cognitive radio ad hoc networks," Computer Communication Journal, vol. 32, no. 18, pp. 1983-1997, Dec.20
[2] K. M. Passino, "Biomimicry of bacterial foraging for distributed optimization," IEEE Control Systems Magazine, vol. 22, no. 3, pp. 52-67, 2002.
[3] Q. Wang, H. Zheng, "Route and spectrum selection in dynamic spectrum networks," in Proc. IEEE CCNC 2006, pp. 625-629, Feb. 2006.
[4] R. Chen et al., "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," IEEE Commun. Mag., vol. 46, pp. 50–55, Apr. 2008.
[5] H. Khalife, N. Malouch, S. Fdida, "Multihop cognitive radio networks: to route or not to route," IEEE Network, vol. 23, no. 4, pp. 20-25, 2009.
[6] Y.-C. Liang et al., "Sensing-Throughput Trade-off for Cognitive Radio Networks, "IEEE Trans. Wireless Commun., vol. 7, pp. 1326–37 ,April 2008.
[7] P. K. Visscher, "How Self-Organization Evolves," Nature, vol. 421, pp. 799–800 Feb.2003.