FAST CHANNEL ALLOCATION FOR MULTIMEDIA COMMUNICATION IN CRAHNS UNDER BYZANTINE ATTACK

Submitted by
Aadity Aabha Patel
17MT001980
Under the Guidance of
Dr. Ansuman Bhattacharya

Department of Computer Science and Engineering
Indian Institute of Technology (Indian School of Mines), Dhanbad

May 8, 2019

CONTENTS

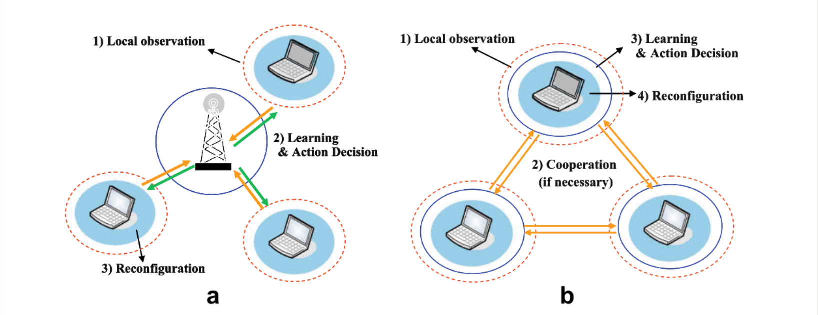
I. INTRODUCTION
II. COOPERATIVE SPECTRUM SENSING (CSS)
III. MULTIMEDIA COMMUNICATION
IV. PRELIMINARY IDEA
V. AGREEMENT PROTOCOLS
VI. FAULT TOLERANCE
VII. PROBLEM STATEMENT AND CONTRIBUTION
VIII. PROPOSED METHOD
IX. RESULT ANALYSIS

I. INTRODUCTION

COGNITIVE RADIO (CR)

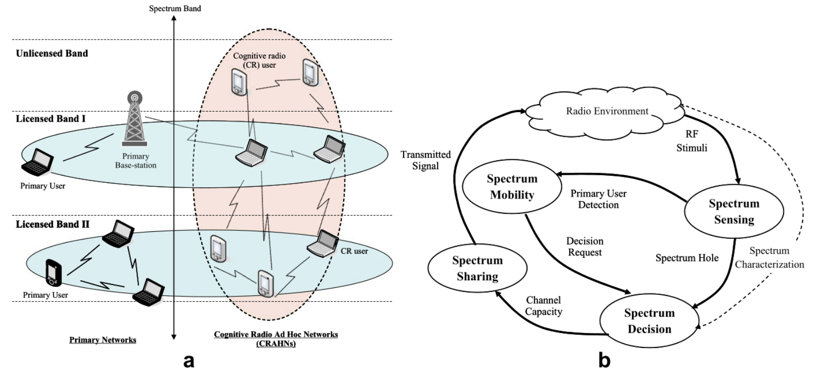
- **Cognitive Radio (CR)** is a technology which facilitates the utilization of radio spectrum efficiently by changing its radio parameters based on the interaction with its environment.
- The basic idea of CR networks is to overcome the spectrum scarcity problem by utilizing the temporarily unused spectrum or Spectrum Holes in a licensed band.The unlicensed devices operate in the analyzed spectrum holes in the licensed bands and vacate the band whenever a licensed device arrives.
- According to the network architecture,cognitive radio(CR) networks can be classified as
    - **the infrastructure-based CR network**
    - **the CRAHNs**

Comparison between infrastructure-based CR networks and CRAHNs.



I. INTRODUCTION

The CRAHN architecture and the cognitive radio cycle are shown in (a) and (b), respectively.



II. COOPERATIVE SPECTRUM SENSING (CSS)

The CRAHN necessitates the following functionalities for spectrum sensing:

- PU detection: The CR user observes and analyzes its local radio environment. Based on these location observations of itself and its neighbors, CR users determine the presence of PU transmissions, and accordingly identify the current spectrum availability.
- Cooperation: The observed information in each CR user is exchanged with its neighbors so as to improve sensing accuracy.
- Sensing control: This function enables each CR user to perform its sensing operations adaptively to the dynamic radio environment. In addition, it coordinates the sensing operations of the CR users and its neighbors in a distributed manner, which prevents false alarms in cooperative sensing.

III. MULTIMEDIA COMMUNICATION

- A rising trend of multimedia communication as text, audio, still image as well as video in various applications including CRN has been observed
- Distinct bandwidths are required for various types of signals to maintain the quality-of-service (QoS) during multimedia communication over a CRN. For multimedia communication, therefore, the bandwidth necessity of the channel varies.
- Let B$_{min}$ be the minimum bandwidth of all these channels. For example, B$_{min}$ may be set equal to 64kbps corresponding to a voice signal. We assume that the whole spectrum is divided in units of this bandwidth B$_{min}$ and the required number of channels each of width B$_{min}$ are allocated to different multimedia signals.

III. MULTIMEDIA COMMUNICATION

- Thus, for transmission of data, still image, video and online streaming data, we may need 128 kbps, 256 kbps, 384 kbps and 512 kbps bandwidth, respectively.
- Hence, we allocate 1, 2, 4, 6 and 8 channels (each of width B min) to voice, data, still image, video and online streaming data, respectively.

IV. PRELIMINARY IDEA

- The CR ad hoc network model is assumed to be having reliable communication medium.However, the nodes in the network are assumed to be prone to failures. If a malicious node is present in the network, it can create issues in the CR node communication.
- A processor can fail in three modes:
  - **Crash fault**
  - **Omission fault**
  - **Malicious fault(Byzantine faults)**
- The capability of a faulty node to distort what the sender receives from other nodes greatly depends upon the type of underlying message. There are two types of messages:
  - **Authenticated and**
  - **Non-Authenticated.**

V. AGREEMENT PROTOCOLS

1. DEFINITION

The entire process of reaching an agreement in distributed systems (where sites (or processors) often compete as well as cooperate to achieve a common goal) is called an agreement protocol.

2. A CLASSIFICATION OF AGREEMENT PROBLEMS

There are three well known agreement problems in distributed systems:

- **Byzantine Agreement Problem**
- **Consensus Problem**
- **Interactive Consistency Problem**

V. AGREEMENT PROTOCOLS

3. THE THREE AGREEMENT PROBLEMS

Problem	Byzantine Agreement	Consensus	Interactive Consiue stency
Who initiates the value	One processor	All processors	All processors
Final agreement	Single value	Single value	A vector of values

Table: The three agreement problems

VI. FAULT TOLERANCE

1. DEFINITION

- To avoid disruptions due to failures and to improve availability, systems are designed to be fault-tolerant.
- System can be designed fault tolerant in two ways :
  1. A system may mask failures.
  2. A system may exhibit a well-defined failure behaviour in the event of failure.
- Widely used techniques, in the design of fault-tolerant systems are:
  1. **Commit Protocols:** Implement well defined behaviour in the event of failure.
  2. **Voting Protocols:** Mask failure in a system.

VI. COMMIT PROTOCOLS

- The commit protocols enforces global atomicity.
- The commit protocols ensure that all the sites either commit or abort the transaction unanimously, even in the presence of multiple and repetitive failures.

VI. VOTING PROTOCOLS

- The voting mechanism is a technique used to manage replicated data.
- With the voting mechanism, each replica is assigned some number of votes, and a majority of votes must be collected from a process before it can access replica.
- The voting mechanism is more fault-tolerant than a commit protocol in that it allows access to data under network partitions, site failures, and message losses without compromising the integrity of the data.
- The voting mechanism is classified into two categories:
  1. Static Voting
  2. Dynamic Voting

VI. VOTING PROTOCOLS

STATIC VOTING

- **Basic Idea :** Every replica is assigned a certain number of votes. This information is stored on table storage. A read or write operation is permitted if a certain number of votes, read quorum or write quorum, respectively, are collected by the requesting process.
- **The Voting Algorithm**

DYNAMIC VOTING PROTOCOLS

Dynamic voting protocols adapt the number of votes or the set of sites that can form a quorum, to the changing state of the system due to site and communication failures.

- **The Majority Based Dynamic Voting Protocol**
- **Dynamic Vote Reassignment Protocol**

VII. PROBLEM STATEMENT AND CONTRIBUTION

PROBLEM STATEMENT

The channel allocation problem for multimedia communication in CRAHNs under the Byzantine attack.

- **Channel Allocation Problem:** Different bandwidths are needed for multimedia communication for distinct types of data to be transmitted over a CRN. When there is a malicious node in the network, it can mislead other nodes regarding channel availability by providing with conflicting results. Throughout this process, Miss-Detection and False Alarm occur.

VII. PROBLEM STATEMENT AND CONTRIBUTION

CONTRIBUTION

- Fast channel allocation is done for multimedia communication in CRAHNs under Byzantine Attack using majority voting algorithm.
- Finally, the results of the computation and the efficiency of the algorithm for majority voting are compared to the existing algorithm.

VIII. PROPOSED METHOD

- The channel allocation from source to destination is done using the Majority Voting algorithm.
- Firstly, a route is find out from source to destination and then the Channel Allocation procedure is called and the channels are allocated for source and destination node data transmission.
- In the Channel Allocation algorithm, the data transmission between source and destination node takes place by considering the frequencies used by all the nodes in its one hop and two hop range. If the selected set of channels are free, it is used for data transmission.
- In the network, apart from the source and destination node, the other non faulty nodes senses for the channel availability in its one hop and two hop range and replies with the correct sensing result.

VIII. PROPOSED METHOD

- For data transmission in a network, the problem arises when the nodes become faulty. Faulty or malicious nodes can provide with false sensing results causing confusion in making the correct decision. As the source or the destination cannot sense channels beyond its one hop, faulty nodes can provide the network with false sensing results.
- After the route and channel selection procedure, the data transmission between the nodes are done

IX. RESULT ANALYSIS

- Basically, two types of protocols are considered: Majority Voting and Existing Method. The Majority Voting considers the most common results given by the neighboring nodes. Whereas, in the Existing Method, the node leaves the selected channel if any one of the neighboring nodes replies with a busy message.
- Three types of faulty node assignment method is considered
  - **Method 1**
  - **Method 2**
  - **Method 3**
- For each of these method Majority Voting Algorithm is compared with Existing Method for multimedia data including text, image, audio and video.

X. RESULT

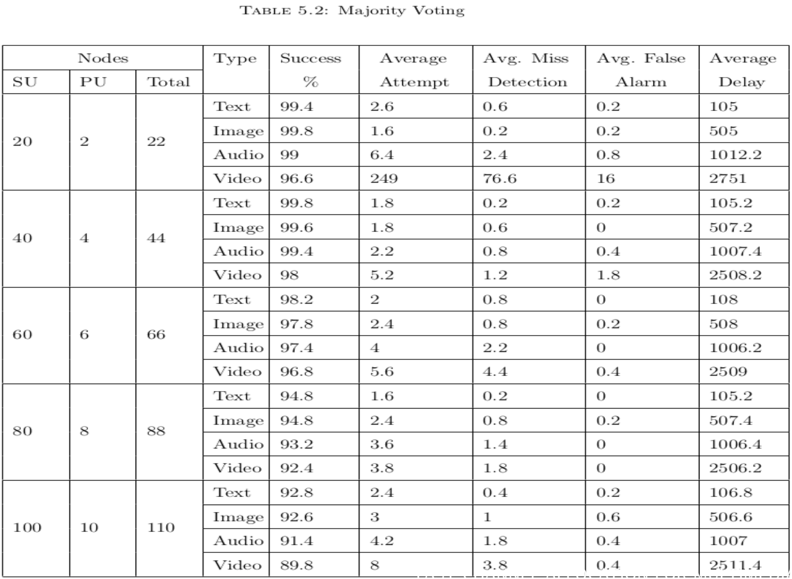


Table 5.2: Majority Voting

Nodes			Type	Success	Average	Avg. Miss	Avg. False	Average
SU	PU	Total		%	Attempt	Detection	Alarm	Delay
20	2	22	Text	99.4	2.6	0.6	0.2	105
			Image	99.8	1.6	0.2	0.2	505
			Audio	99	6.4	2.4	0.8	1012.2
			Video	96.6	249	76.6	16	2751
40	4	44	Text	99.8	1.8	0.2	0.2	105.2
			Image	99.6	1.8	0.6	0	507.2
			Audio	99.4	2.2	0.8	0.4	1007.4
			Video	98	5.2	1.2	1.8	2508.2
60	6	66	Text	98.2	2	0.8	0	108
			Image	97.8	2.4	0.8	0.2	508
			Audio	97.4	4	2.2	0	1006.2
			Video	96.8	5.6	4.4	0.4	2509
80	8	88	Text	94.8	1.6	0.2	0	105.2
			Image	94.8	2.4	0.8	0.2	507.4
			Audio	93.2	3.6	1.4	0	1006.4
			Video	92.4	3.8	1.8	0	2506.2
100	10	110	Text	92.8	2.4	0.4	0.2	106.8
			Image	92.6	3	1	0.6	506.6
			Audio	91.4	4.2	1.8	0.4	1007
			Video	89.8	8	3.8	0.4	2511.4

X. RESULT

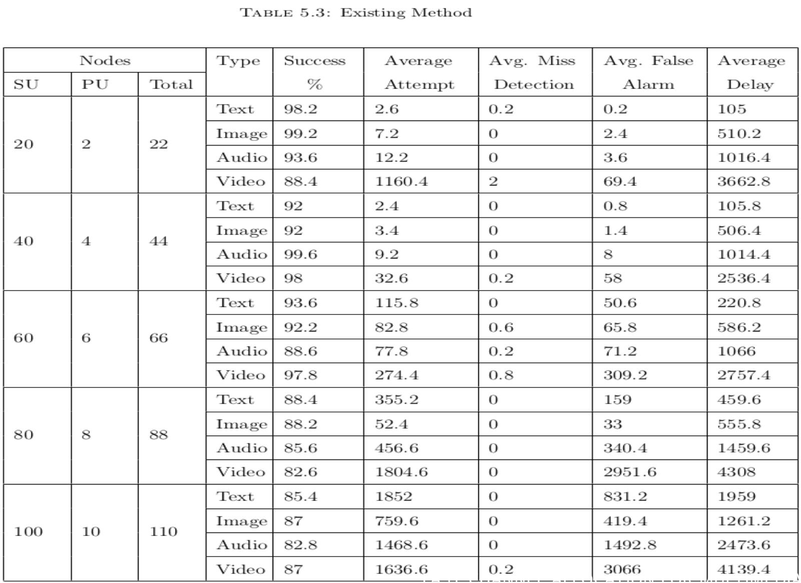


TABLE 5.3: Existing Method

Nodes			Type	Success	Average	Avg. Miss	Avg. False	Average
SU	PU	Total		%	Attempt	Detection	Alarm	Delay
20	2	22	Text	98.2	2.6	0.2	0.2	105
			Image	99.2	7.2	0	2.4	510.2
			Audio	93.6	12.2	0	3.6	1016.4
			Video	88.4	1160.4	2	69.4	3662.8
40	4	44	Text	92	2.4	0	0.8	105.8
			Image	92	3.4	0	1.4	506.4
			Audio	99.6	9.2	0	8	1014.4
			Video	98	32.6	0.2	58	2536.4
60	6	66	Text	93.6	115.8	0	50.6	220.8
			Image	92.2	82.8	0.6	65.8	586.2
			Audio	88.6	77.8	0.2	71.2	1066
			Video	97.8	274.4	0.8	309.2	2757.4
80	8	88	Text	88.4	355.2	0	159	459.6
			Image	88.2	52.4	0	33	555.8
			Audio	85.6	456.6	0	340.4	1459.6
			Video	82.6	1804.6	0	2951.6	4308
100	10	110	Text	85.4	1852	0	831.2	1959
			Image	87	759.6	0	419.4	1261.2
			Audio	82.8	1468.6	0	1492.8	2473.6
			Video	87	1636.6	0.2	3066	4139.4

XI. REFERENCES

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. next generation/dynamic spectrum access/cognitive radio wireless networks: a survey. Computer networks, 50(13):21272159, 2006.

[2] I. F. Akyildiz, W.-Y. Lee, and K. R. Chowdhury. Crahns: Cognitive radio ad hoc networks. Ad Hoc Networks, 7(05):810836, 2009.

[3] A. Bhattacharya, R. Ghosh, K. Sinha, D. Datta, and P. B. Sinha. Multimedia channel allocation in cognitive radio networks using fdm-fdma and ofdm-fdma. IEEE Transactions on Cognitive Communications and Networking.

[4] A. Narayanan. fast channel allocation and optimum route selection in crahns under byzantine attack. 2017.

[5] R. Chen and J. M. Park. ensuring trustworthy spectrum sensing in cognitive radio networks. 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, pages 110119, 2006.

XI. REFERENCES

[6] T. C. Clancy and N. Goergen. security in cognitive radio networks: Threats and mitigation,. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom 2008), pages 18, 2008.

[7] H. Deng, W. Li, and D. P. Agrawal. routing security in wireless ad hoc networks,. IEEE Communications Magazine, 40:7075, 2002.

[8] J. R. Douceur. the sybil attack,. Revised Papers from the First International Workshop on Peer-to-Peer Systems, IPTPS 01, (London, UK, UK), pages 251260, 2002.

[9] S. Haykin. cognitive radio: brain-empowered wireless communications. IEEE journal on selected areas in communicationss, 23(2):201220, 2005.

[10] C. Karlof and D. Wagner. secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2):293315, 2003.