Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.305 – 315

RESEARCH ARTICLE

HASH TREE ALGORITHM FOR CENTRALIZED COGNITIVE RADIO NETWORKS

R.Megala*, S.Sathya, M.Sc., M.Phil.******
*M.Phil(Computer Science), Research Scholar,
Vivekanandha College for Women, Unjanai, Tiruchengode, India
******Assistant Professor in Computer Science,
Vivekanandha College for Women, Unjanai, Tiruchengode, India

ABSTRACT: Hash tree is a tree in which every non-leaf node is labeled with the hash of the labels of its children nodes. Hash trees are useful because they allow efficient and secure verification of the contents of larger data structures. Hash trees are a generalization of hash lists and hash chains. Demonstrating that a leaf node is a part of the given hash tree requires processing an amount of data proportional to the logarithm of the number of nodes of the tree this contrasts with hash lists, where the amount is proportional to the number of nodes. The study a multicast communication problem in a multi-hop ad hoc network where each node is equipped with a cognitive radio (CR). The goal is to minimize the required network-wide resource to support a set of multicast sessions, with a given bit rate requirement for each multicast session. In this proposed system they are using hash tree algorithm used. The show that the proposed algorithm can provide a solution that is close to the optimum.

Keywords: Mobile Computing, CRNs, Hash tree algorithm, MANET.NS-2

1. INTRODUCTION

1.1 Mobile Computing

The computers are smaller and bits travel by wireless rather laptop stolen than to have workstation in a thin Ethernet Locked office is physically subverted. In addition to is not a mobile system merely a special case of a distributed system. There any new and deep issues to be investigated. The mobile computing just the latest fad access in mobile environments is complicated by a number of factors. First, scalability is a concern both because of the expected ubiquity of mobile computers and because of the increasing volume of data in shared repositories. Second, they have to cope with certain fundamental constraints of mobility: mobile hosts tend to be resource poor because of size, weight, and power constraints; they are physically vulnerable to loss, theft and other hazards; and they have to cope with considerable variation in the performance and reliability of wireless communication. Third, data is increasingly diverse in format: in addition to the well-understood data formats of Unix-like hierarchical file systems and SQL databases, there is growing interest in video images, maps and other spatial images, and hypertext-like data as in the World-Wide Web resource poverty, physical vulnerability and scalability concerns of mobile hosts suggest a client-server architecture, with servers being the true home of data and clients merely being caching sites. At the same time, the uncertainty in wireless communication requires clients to adapt dynamically, reducing their dependence on servers as the quality of communication degrades. The need to support diverse types of data suggests that the adaptation cannot be universal, but needs to be customized for each type of data considerations lie behind our advocacy of application-aware adaptation as the paradigm of data access in mobile environments. In the model, the role of the operating system is to sense external events and to monitor and allocate resources.

1.2 CRNs Overview

Cognitive radio systems are radios with the ability to exploit their environment to increase spectral efficiency and capacity. As spectral resources become more limited the FCC1 has recommended that significantly greater spectral efficiency could be realized by deploying wireless devices that can coexist with primary users, generating minimal interference while somehow taking advantage of the available resources. Such devices, known as cognitive radios, would have the ability to sense their communication environment and adapt the parameters of their communication scheme to maximize rate, while minimizing the interference to the primary users. Thus the two most popular research areas it comes to cognitive radios are spectrum sensing and interference management and resource Allocation. Spectrum sensing is the ability and available frequencies/ timeslots to transmit in.

The problem is then that the algorithms need to have as little delay as possible so that once channels are available one can transmit immediately. And of course one would want as few false detections and false no-detections as possible. Research in the area of interference management and resource allocation consists of how to allocate power in channels to maximize capacity while minimizing interference to other users. One way is of course to transmit when no one else is using that frequency/timeslot, but given a scenario there are multiple cognitive users in the same environment this may not be possible and certainly not the way to maximize capacity. An intelligent wireless communications system based on SDR technology Reconfigurable Reconfigurable Agile Functionality Aware of its environment RF spectrum occupancy Network traffic Transmission quality. Learns from its environment and adapts to new scenarios based on previous experiences.

2. LITERATURE SURVEY

They formulate a scheduling problem that takes into account different hardware delays experienced by the secondary users (SUs) in a centralized cognitive radio network (CRN) while switching to different frequency bands. The propose a polynomial-time suboptimal algorithm to address our formulated scheduling problem. The evaluate the impact of varying switching delay, number of frequencies, and number of SUs. Our simulation results indicate that proposed algorithm is robust to changes in the hardware spectrum switching delay and its performance is very close to its upper bound. The also compare our proposed method with the corresponding constant switching delay-based algorithm and demonstrate that suggestion of taking into account the different hardware delays while switching to different frequency bands is essential for scheduling in CRNs.

3. METHODOLOGY

Hash tree methodology is used. Hashing is a method to store data in an array so that sorting, searching, inserting and deleting data is fast. For this every record needs unique key. The basic idea is not to search for the correct position of a record with comparisons but to compute the position within the array. The function that returns the position is called the 'hash function' and the array is called a hash table. It provides a small digital “fingerprint” from any kind of data. The function substitutes or transposes the data to create that “fingerprint”, usually called hash value. This value is represented as a short string of random - looking letters and numbers (for example binary data written in hexadecimal notation). By hash functions appears also the term hash collision - the situation when two different inputs produce identical outputs. Of course the better the hash function, the smaller number of collisions that occur. Similarly in cryptography they have a cryptographic hash function it is simply a normal hash function with additional security\properties. This is needed for their use in various information security applications, such as authentication and message integrity. Usually a long string of any length is taken as input and a string of fixed length is given as output. The output is sometimes termed a digital fingerprint. One desirable property of cryptographic hash functions is collision resistance. A hash function is collision resistant it is “infeasible” to find a collision.

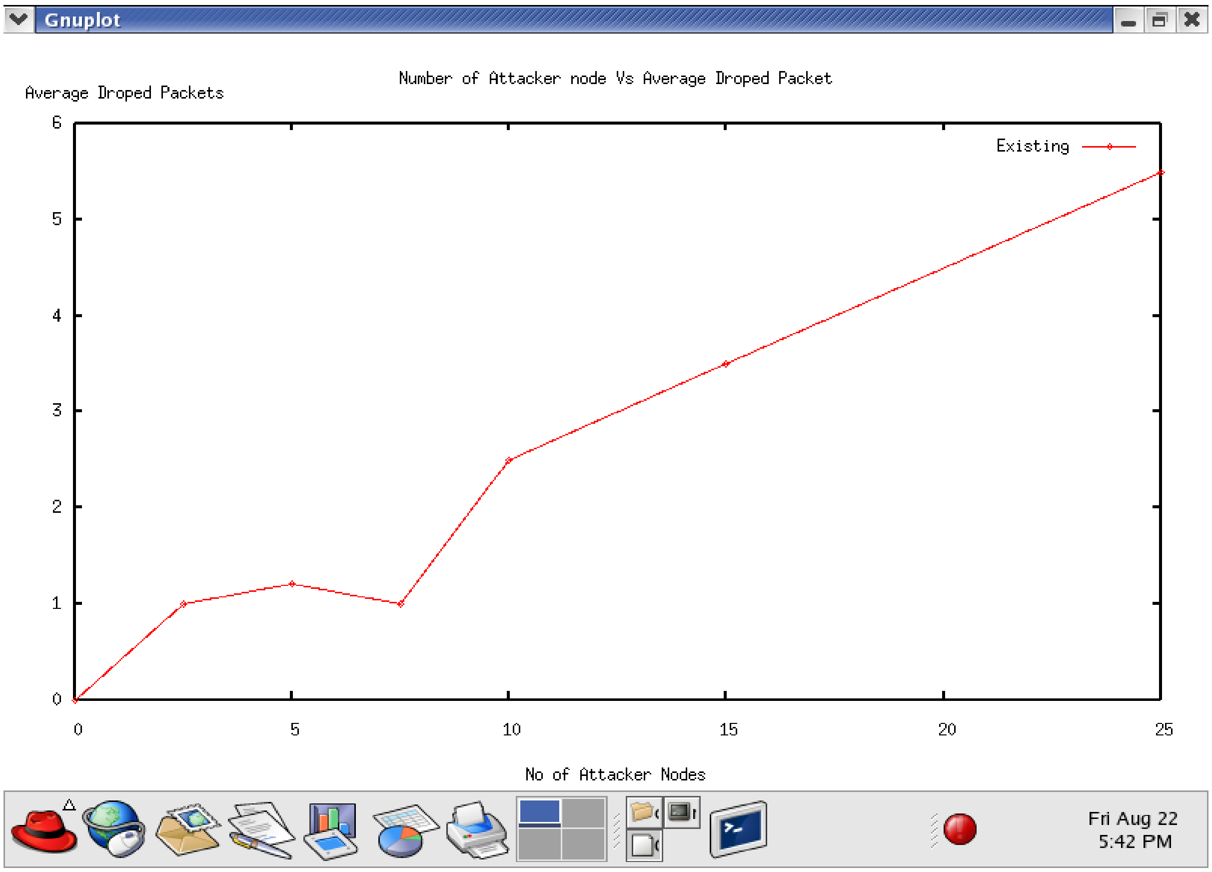
3.1 Hash tree Algorithm

In cryptography and computer science a **hash tree** or **Merkle tree** is a tree in the every non-leaf node is labeled with the hash of the labels of its children nodes. Hash trees are useful because they allow efficient and secure verification of the contents of larger data structures. Hash trees are a generalization of hash lists and hash chains. Demonstrating that a leaf node is a part of the given hash tree requires processing an amount of data proportional to the logarithm of the number of nodes of the tree this contrasts with hash lists, they amount is proportional to the number of nodes. A hash tree is a tree of hashes in the leaves is hashes of data blocks in, for instance, a file or set of files. Nodes further up in the tree are the hashes of their respective children. For example in the picture hash 0 is the result of hashing the result of concatenating hash 0-0 and hash 0-1. That is, hash 0 = hash(hash 0-0 + hash 0-1) where + denotes concatenation. Most hash tree implementations are binary (two child nodes under each node) but they can just as well use many more child nodes under each node. Usually, a cryptographic hash function such as SHA-2 or SHA-3 is used for the hashing. If the hash tree only needs to protect against unintentional damage, much less secure checksums such as CRs can be used.

In the top of a hash tree there is a top hash (or root hash or master hash). The file on a p2p network, in most cases the top hash is acquired from a trusted source, for instance a friend or a web site that is known to have good recommendations of files. The top hash is available, the hash tree can be received from any non-trusted source, like any peer in the p2p network. Then, the received hash tree is checked against the trusted top hash, and the hash tree is damaged or fake, another hash tree from another source will be tried until the program finds one that matches the top hash. The main difference from a hash list is that one branch of the hash tree can be downloaded at a time and the integrity of each branch can be checked immediately, even though the whole tree is not available yet. For example, in the picture, the integrity of data block 2 can be verified immediately if the tree already contains hash 0-0 and hash 1 by hashing the data block and iteratively combining the result with hash 0-0 and then hash 1 and finally comparing the result with the top hash. Similarly, the integrity of data block 3 can be verified if the tree already has hash 1-1 and hash 0. This can be an advantage since it is efficient to split files up in very small data blocks so that only small blocks have to be re-downloaded if they get damaged. If the hashed file is very big, such a hash tree or hash list becomes fairly big. But if it is a tree, one small branch can be downloaded quickly, the integrity of the branch can be checked, and then the downloading of data blocks can start. There are several additional tricks, benefits and details regarding hash trees. See the references and external links below for more in-depth information.

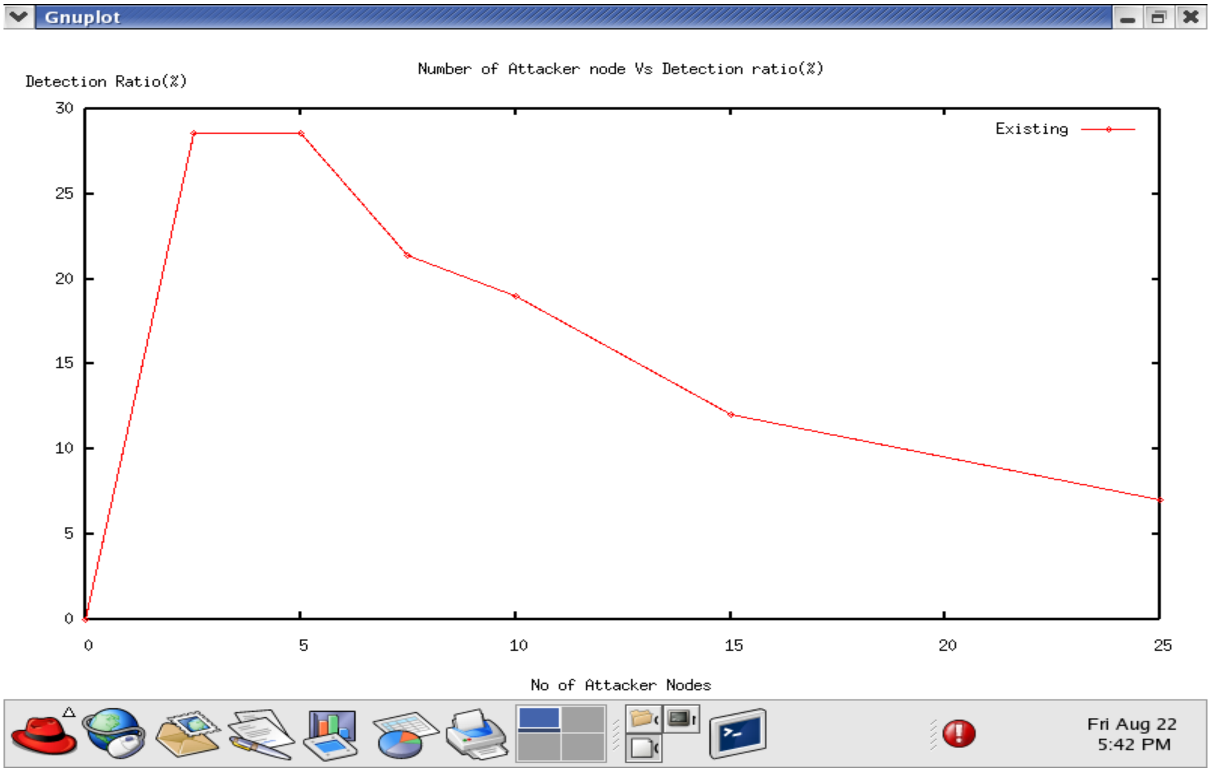
4. EXPERIMENTS AND RESULTS

They analysis the network attacker will be there so if attacker occurs means they will be the packet dropped and they analysis the result this graph.



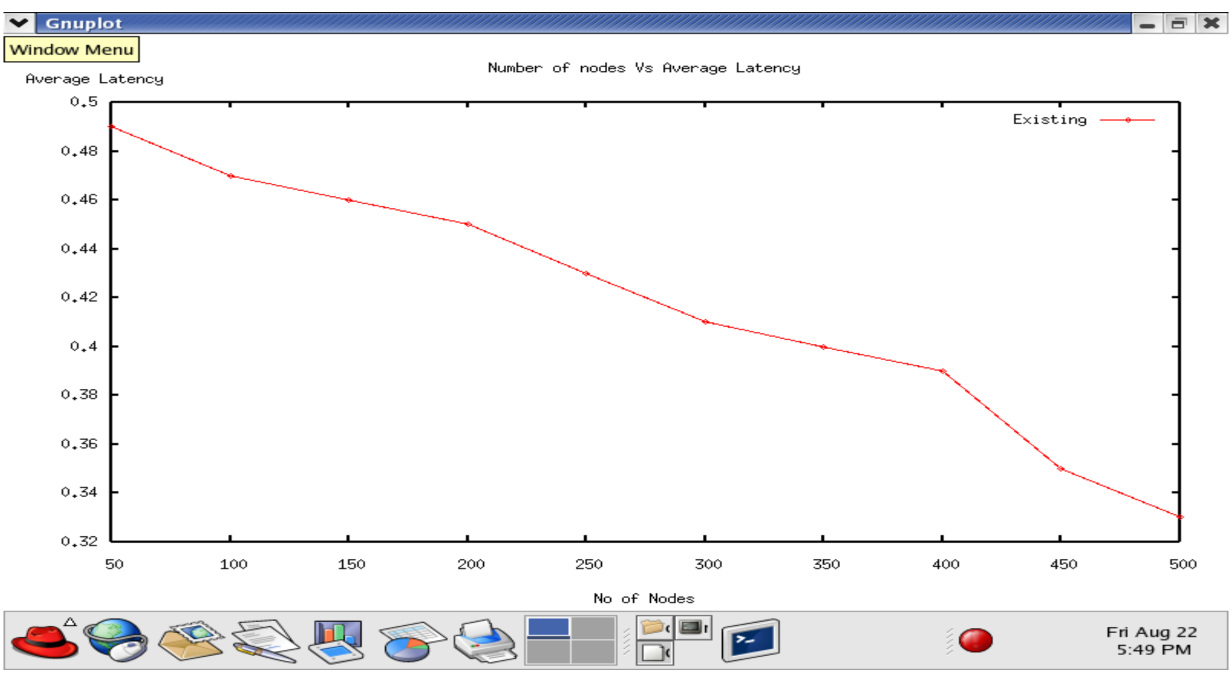
Number of Attacker node Vs Average Droped Packet

The result based on the attack they will be the attacker detection ratio.



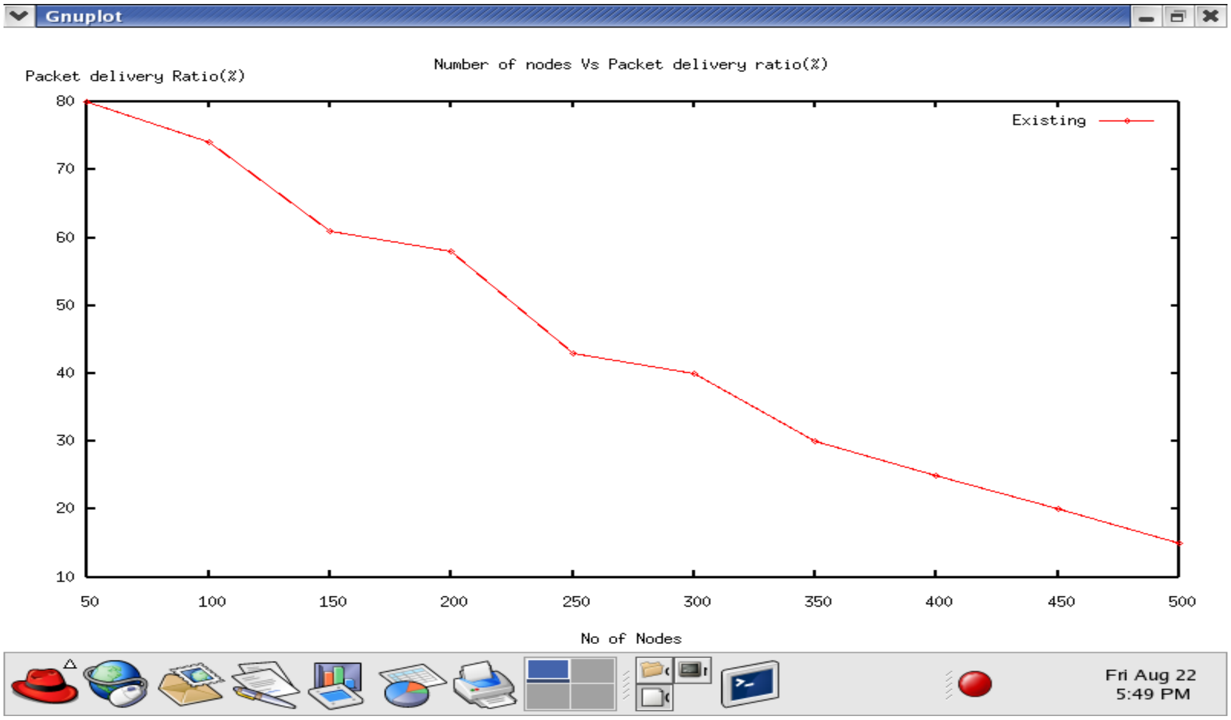
Number of attacker node Vs Detection ratio(z)

The remaining latency for the network this graph will be used for analysis the latency.



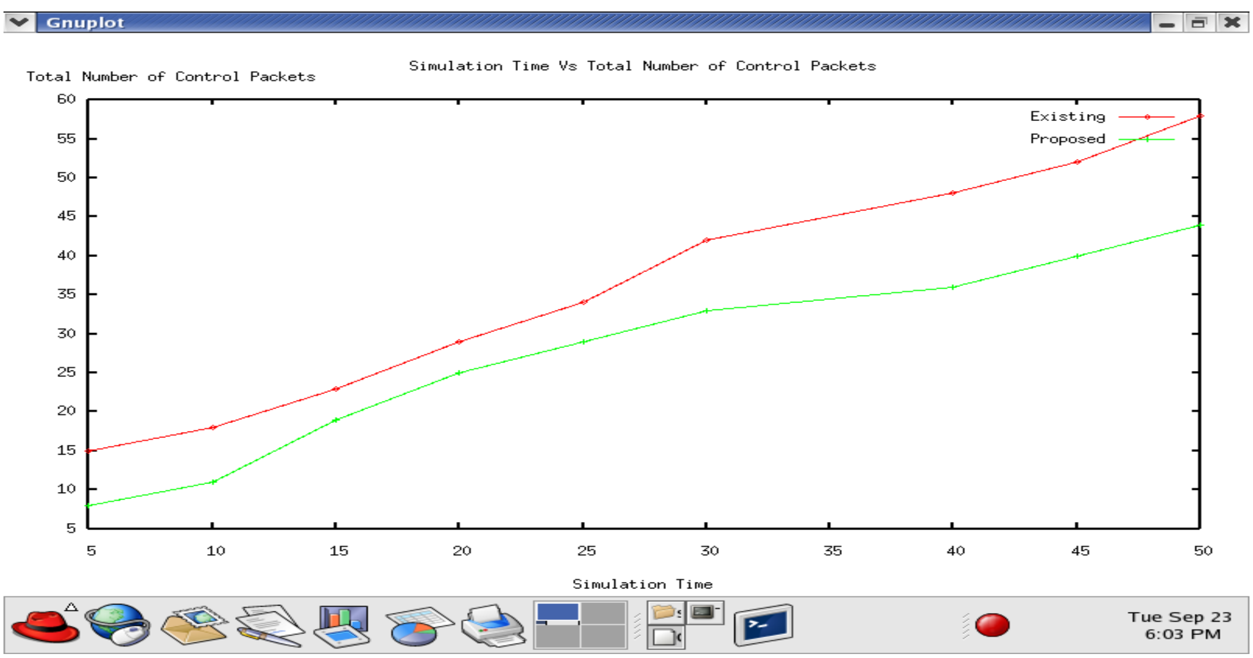
Number of nodes Vs Average latency

The process over means remaining calculation will be the how much packet will be transmitting calculate the ratio for packet delivery.



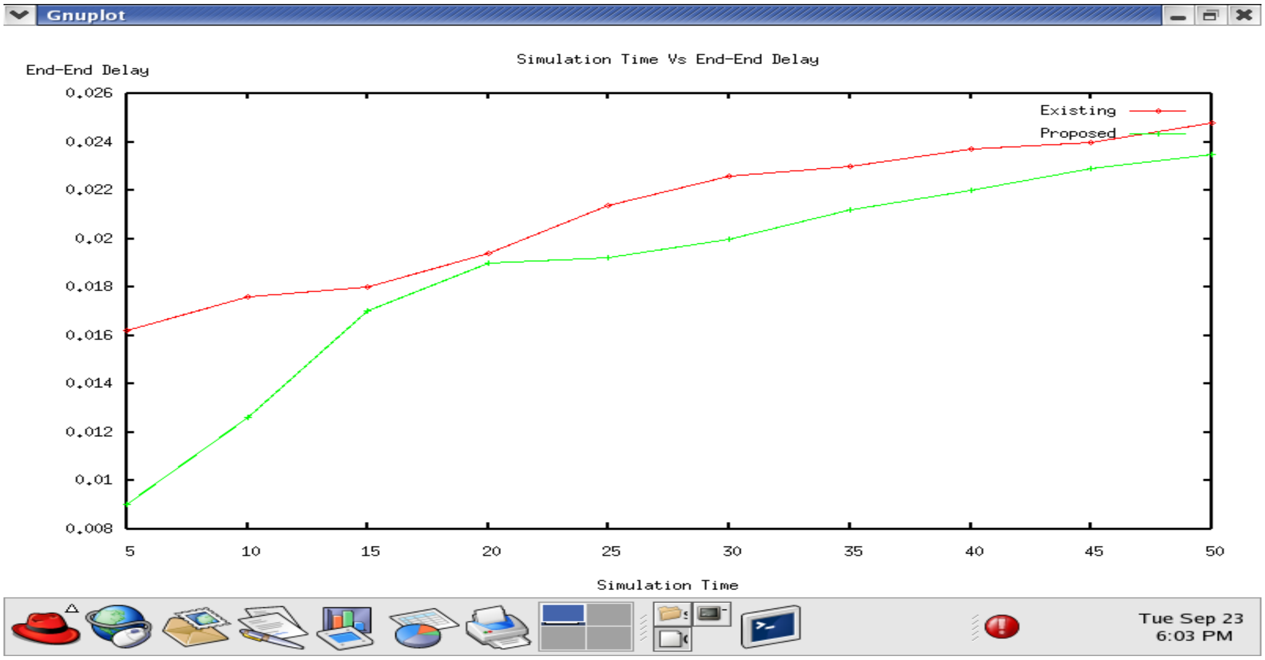
Number of nodes Vs Packet delivery ratio(z)

The proposed system analysis the result both existing and proposed system comparison in that graph. They will analysis the result what will be the control packet in that network.



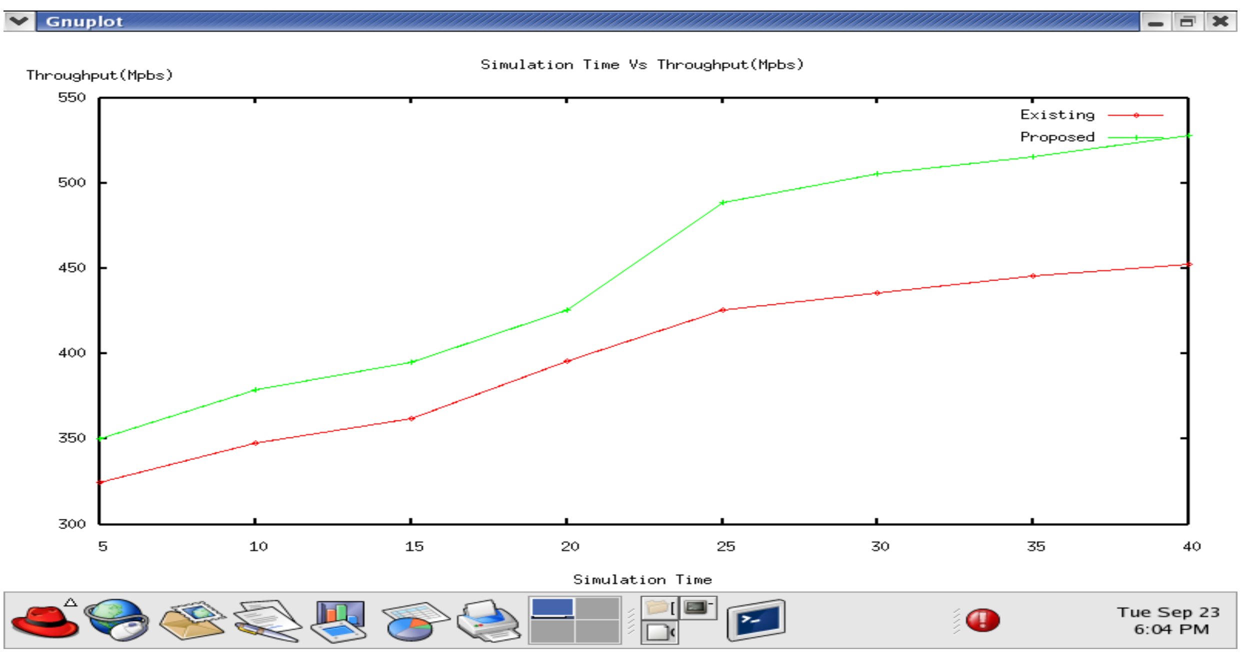
Simulation time Vs Total number of control packets

That analysis the end to end delay during the data transmission both existing and proposed system.



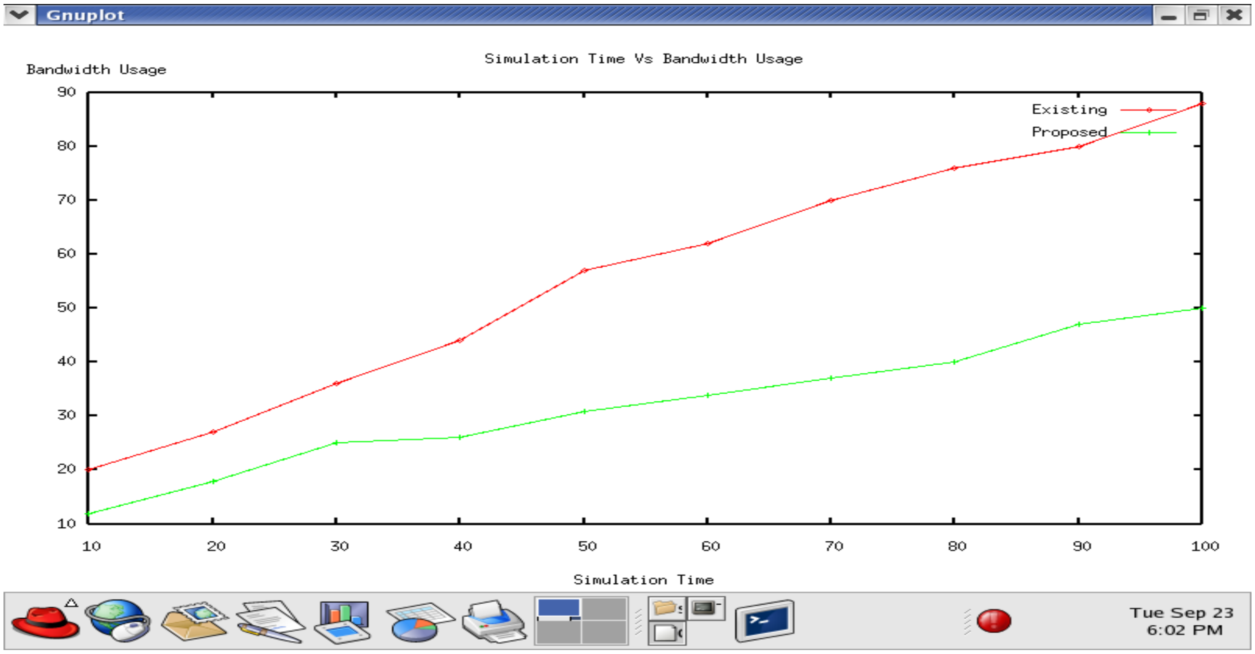
Simulation Time Vs End-End Delay

Then identify the throughput for the both existing and proposed system for overall network. They conclude the result when compared to the existing and proposed system proposed system will be the high throughput.



Simulation Time Vs Throughput

Then bandwidth usage for both existing and proposed system if less amount of band width usage in proposed system but they get the high through put. And high network life time.



Simulation Time Vs Bandwidth Usage

5. CONCLUSION AND FUTRUE ENHANCEMENT

The study a multicast communication problem in a multi-hop ad hoc network the each node is equipped with a cognitive radio (CR). The goal is to minimize the required network-wide resource to support a set of multicast sessions, with a given bit rate requirement for each multicast session. In this proposed system they are using hash tree algorithm used. The show that the proposed algorithm can provide a solution that is close to the optimum. A primary challenge being addressed is the identification of technical enablers for CR, i.e., theories, concepts, and practical algorithms to implement these mechanisms at a reasonable operational cost on flexible radio platforms. There have been many advances in the field of CR in recent years with respect to enabling environmental (spectrum) awareness and designing robust and flexible transmission techniques for hostile CR communication environments with varying channel conditions. However, there are still a number of open issues and research challenges to be addressed before CR technology can become truly flexible and practical. Issues with efficient spectrum management, real time implementation, CR security and applications, as well as regulatory and standardization aspects, all require significant attention for operation in cognitive networks.

REFERENCES

[1] I. Akyildiz, W. Lee, M. Vuran, and S. Mohanty, "**NeXt Generation/ Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey**," Computer Networks, vol. 50, no. 13, pp. 2127- 2159, 2006.

[2] B. Wang and K. Liu, "**Advances in Cognitive Radio Networks: A Survey**," IEEE J. Selected Topics in Signal Processing, vol. 5, no. 1, pp. 5-23, Feb. 2011.

[3] H. Kim and K. Shin, "**Efficient Discovery of Spectrum Opportunities with MAC-Layer Sensing in Cognitive Radio Networks**," IEEE Trans. Mobile Computing, vol. 7, no. 5, pp. 533-545, May 2008.

[4] G. Cheng, W. Liu, Y. Li, and W. Cheng, "**Spectrum Aware On- Demand Routing in Cognitive Radio Networks**," Proc. IEEE Second Int'l Symp. New Frontiers in Dynamic Spectrum Access Networks (DySPAN), 2007.

[5] G. Cheng, W. Liu, Y. Li, and W. Cheng, "**Joint On-Demand Routing and Spectrum Assignment in Cognitive Radio Networks,**" Proc. IEEE Comm. Int'l Conf. (ICC), 2007.

[6] I. Filippini, E. Ekici, and M. Cesana, "**Minimum Maintenance Cost Routing in Cognitive Radio Networks,**" Proc. IEEE Sixth Int'l Conf. Mobile Adhoc and Sensor Systems (MASS), 2009.

[7] K. Chowdhury and M. Felice, "**SEARCH: A Routing Protocol for Mobile Cognitive Radio Ad-Hoc Networks**," Computer Comm., vol. 32, no. 18, pp. 1983-1997, 2009.

[8] J. Chen, H. Li, J. Wu, and R. Zhang, "**STARP: A Novel Routing Protocol for Multi-Hop Dynamic Spectrum Access Networks**," Proc. ACM Workshop Mobile Internet through Cellular Networks, 2009.

