IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

# Oppurtunistic Routing Through Delay Analytical Methods in Ad-Hoc Wireless Networks

**M. Thenmozhi[1*], N. Tamilarasi[2]**

[1,2]Dept. Of Computer Science, Sri Akilandeswari Women's College, Wandiwash, India

[*]*Corresponding Author: thenmozhimscit@gmail.com, Tel.: +91-9677335452*

**Available online at: www.ijcseonline.org**

Accepted: 17/Nov/2018, Published: 30/Nov/2018

***Abstract*—** Many researchers are showing a keen interest in opportunistic routing and are becoming very popular. This is mainly due to its specific characteristic that it posses for improving the performance and efficiency of the wireless ad-hoc networks. A broadcasting feature of wireless ad-hoc networks is made use in opportunistic routing which increases the network's overall reliability and throughput. This research paper focuses on an efficient analytical model which is capable of transmitting the data packets both in known and unknown topologies. This is done by making use of single and multiple forwarders. The proposed approach is designed in such a way that it reduces the probability of packet loss in the network. Furthermore this paper concentrates on the security aspects of the network and provides a proper authentication mechanism before the data packets are delivered to the receiver.

***Keywords*—** Wireless ad-hoc networks, Opportunistic Routing, encryption, decryption, analytical model

## I. INTRODUCTION

The emergence of wireless networks since the 1970s has become very popular in the computing industries. This is predominantly true when it comes to the last decade, which has seen many wireless networks being adapted in order to facilitate mobility. Mobile wireless networks are majorly classified into two types. The first one being "Infrastructural Network" where a network has a fixed number of gateways. The networks have base stations which form a bridge between the networks. Applications for this type of networks include wireless office local area network (WLANs)[1]. Mobile wireless networks universally called "Ad-hoc Networks" form the second type of networks. Mobile ad-hoc networks do not have any routers that are fixed at any point. They are capable of moving anywhere. The nodes present in these type of networks work as routers whose main work is to discover and maintain various routes present to other nodes in the network. Performing emergency search and rescue operations during crisis time could be one of the typical application of Ad-hoc[2].

Wireless Ad-hoc networks are used in numerous applications these days. Generally, a network consists of several nodes and these nodes need to communicate with one another in order to perform various operations assigned to them. Routing is a process used to select a path between the nodes or across multiple networks[3]. Its main work is to decide on a decision that is based on directing the network packets from source node to destination node. This is achieved through intermediate nodes. Routing plays an important role in various types of networks which also includes circuit switched networks[4]. Routing is one of the most crucial research areas in Wireless Ad-hoc networks. Route selection and Packet forwarding are the tasks included in the routing process. In route selection, one or more routes are selected that connects one or more pair of nodes. The one-hop decision is taken to forward the packets by selecting a neighbour node across the chosen routes. Routing is one of the challenging problem encountered in the wirelessmedium as it is dynamic and lossy in nature. Fig 1. shows a diagrammatic view of a wireless ad-hoc network. The source and destination have intermediate nodes through which the packets are transmitted.

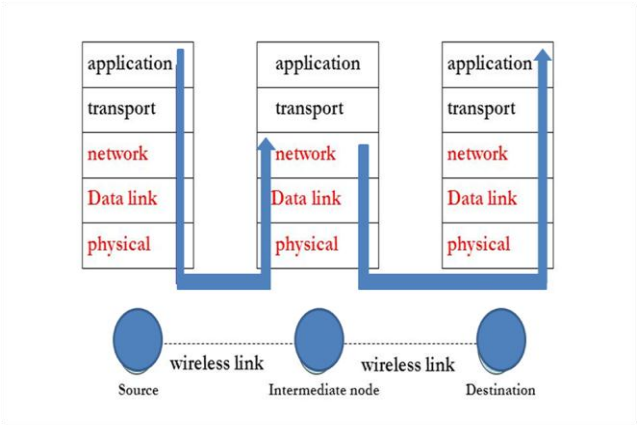


Fig.1 Architecture of Wireless Ad-hoc Network

 

Conventional routing protocols designed for wireless networks selectan optimized fixed route before the transmissions start. Transmission of packets in each hop occurs between the predetermined neighbours. This may be suitable for the static wireless environment but not for dynamic environments where frequent transmission failure occurs. In order to overcome this drawback, Opportunistic Routing(OR) also called as opportunistic forwarding was introduced. OR is mainly used to overcome the disadvantage of unreliable wireless transmission. This is done by making use of the broadcasting behaviour of the wireless medium. Transmitting a packet in such a way that it could be heard by multiple neighbours in a wireless ad-hoc network is called as Broadcasting. The packets are forwarded in a single route in such a way that at least one neighbour is able to receive the packets.

The capability of routing or transporting data from a source to a destination is one of the fundamental ability that a communication network should include. Delay and Disruption-Tolerant networks (DTNs) mainly lack in proper connectivity across the networks that in turn results in lack of immediate end-to-end paths. Existing works in DTNs have majorly concentrated on the performance delay occurring within the networks. This paper proposes an analytical model suitable for three OR scenarios: Single Forwarder with Known Topology(SF/KT), Multiple Forwarders with Known Topology (MF/KT), and Multiple Forwarders with Unknown Topology (MF/UT). The accuracy of the proposed analytical models was verified using NS2 simulator.

VARIOUS OPERATIONS OF OPPORTUNISTIC ROUTING :

Opportunistic routing increases the probability of packet transmission in a wireless network. It aims that at least one potential node receives the transmitted packet in the network.

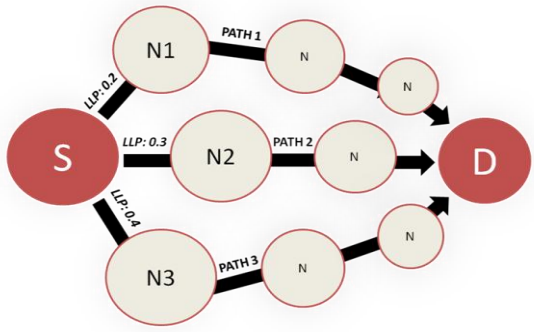


Fig.2 Connections in a Wireless Network to illustrate the benefits of Opportunistic Routing

Figure 2. Describes the transmission in a wireless network.

The source node is symbolized by Sand symbolizes the destination node. The source node sends a packetto the next neighbour. Each link in the layer has some loss probability(LPP). A loss probability of 0.2 will occur when the packet is transmitted from S-N1.Whereas from S-N2 and S-N3 has a loss probability of 0.3 and 0.4 respectively. In traditional routing, the packet is sent to the neighbouring node with minimum loss probability so the packet would be sent to node N2. In Opportunistic routing, the packets would be broadcasted to all the three neighbors to minimize the probability of packet loss. The operations involved in opportunistic routing could be better understood with the following sequential phases:

Candidate Selection (Cs): A set of nodes from IP stack is selected that allows the transmission of the packet from source to destination. This set of nodes are called as forwarding candidates. The nodes are ordered by making use of some criteria. The addresses of these nodes are suggested to be stored in bloom filters as in [5] rather than storing in packet headers that consume a lot of space. V – values, S – Source, D – Destination, OR - opportunistic routing

$$S+D= Cs + V \quad (1)$$

$$S+D=OR \quad (2)$$

Candidate Priority Assignment: Whenthe source node of the networkrepeatedlyupdatesregardingits forwarding candidates, it in turn also instructs them to act as the relaying nodes. The relay nodes combined together to forma relay set that plays a prominent role in opportunistic routing protocols.

$$A = OR + DATA \quad (3)$$

Data Transmission: Opportunistic routing protocols are basically supported by transmitting the broadcasted packets. These packets in the network are received by multiple neighbouring nodes that are present. Apart from this,some opportunistic routing protocols also allow data packets to be transmitted in a unicast way[6].

$$OR + DATA + P = RC \quad (4)$$

Receiver coordination (RC) : The coordination should occur between the forwarders to avoid multiple retransmissions. The coordination involves the ordering of the forwarders using certain metrics[7].

Rest of the paper is organized as follows, Section II contains the review of literature pertaining to this paper, and proposed methodology is discussed in Section III. Section IV explains the architectural design and Section V describes simulation process. Section VI shows the results and discussion and Section VII concludes research work.

## II. RELATED WORK

***Three Step forwarding strategy:***

Dazhi Chen Jing Deng Pramod K. Varshney propose three step forwarding strategy to forward the packets. A mathematical framework on average single hop packet progress is framed to forward the packets. The Three

 

different types for forwarding methods based on the nodes through different forwarding area.

Maximum forwarding area,
Maximum communication area and
60 degree radian area

was found as forwarding area for the nodes to forward the packets. The framework, validated by numerical results and extensive simulations, can also serve as a performance evaluation technique for the CGF protocols that have been designed previously.

***Reliable link Protocol:***

Sahaya Rose Vigita.E, Golden Julie.E propose a reliable link POR protocol where linking is the main problem while transferring the packets. Opportunistic Routing (L-POR) protocol which chooses a forwarder based on the reception power of node has been proposed. A back-up method is also proposed to handle communication holes. Neighbouring nodes are selected according to the link stability. As the distance of the node towards the destination has not been considered for forwarder selection, the path length may not be always minimal causing a varying end-to-end delay. Hence disadvantage is hop count thus ensuring a lower end-to-end delay will be reduced.

***Opportunistic Multipath Scheduling (OMS):***

This technique for exploiting short term variations in path quality to minimize delay, by simultaneously ensuring that the splitting rules dictated by the routing protocol are satisfied. OMS uses measured path conditions on time scales up to several seconds to opportunistically forever low-latency and high-throughput paths. But, a naive policy that always selects the highest quality path would violate the routing protocol's path weights and potentially lead to oscillation. Thus, OMS ensures that over longer time scales relevant for traffic management policies with is spitted according to the ratios determined by the routing protocol.

## III. METHODOLOGY

We have proposed an analytical model in this paper, which can work in three various Opportunistic scenarios. The first scenario is where there is a single forwarder with known topology(SK/KT), the second scenario is where there are multiple forwarders with known topology(MF/KT) and the third scenario is where there are multiple forwarders with unknown topology(MF/UT). The accuracy of the proposed analytical models is verified using the NS2 simulator. The data transmission from the source to the destination is improved when the data packet is transmitted as a payload and the TCP-UDP as a Header in the network.

**Opportunistic Routing Scheme:**

The ExOR(Extremely Opportunistic Routing) protocol[8] assumes that all the nodes in the wireless network know the loss rate of every link in the network. The ExOR protocol consists of three stages: 1) Opting the forwarding nodes, 2) Acknowledging the transmissions and 3) Coming to a decision whether to forward the received packet. A matrix consisting of an approximation of loss rate for each node is assumed to direct the radio transmission between every pair of nodes. The matrix is built using a link-state flooding scheme, in which the nodes measure the loss rate and periodically updates the statistics. This could help in bringing the packet closer to the destination. Immediately after the transmission, each ode that receives the packets checks for its addresses in the node list located in the header. Each and every node in the network lookout for the set of acknowledgments that it receives to decide whether to forward the packet or not. The forwarding node rewrites the ExOR frame header with a new set of nodes and again transmits the packet. There are various phases involved that are involved in this schemeand are discussed as follows:

***Selection of node Forwarder Set***

Performance of the ExOR is determined by the routing is done by the ability of the protocol to choose a prioritized set of nodes. Merelypicking a set of nodes which is based on the smallest number of hops could result inexcellent performance. The selection of the prioritized node list is done by recognizing the shortest path to the destination node and then breaking the ties that occur between the equal short paths. This is done by using the information from the delivery ratio matrix. The highest priority is given to the first node that is chosen in the path. It then again finds the shortest route and makes use of the first hop on that route as the node with the second priority.

***Receiver's Acknowledgment(ACK)***

One of the major challenges of opportunistic routing is to decide which node have to forward the packet to the next corresponding node. A model is proposed in the paper that uses a modified version of 802.11 MAC. It reserves multiple slots of time that is used for receiving the return acknowledgments. The acknowledgment is an indication that thepacket is transmitted and it also contains the ID of the highest priority recipient known to the ACK's sender. In case if node A hears a transmission in the network, then A is the highest priority node. It sends an ACK to the sender. The nexthighest priority node won'tbe able to hear the ACK, but node Cisable to hear the ACK. If ACKs doesn't contain IDs, then node B would forward the packet, as to its knowledge it is the highest-priority recipient. As node C's ACK contains node A's ID, it indirectly notifies node B that node A has not received the packet.

***Deciding on Packet forwarding***

When a slotted acknowledgment window is created, each candidate in the network must take a local decision on forwarding or discarding the packet. The nodes which have

 

not yet received the acknowledgments andalso has the ID of the next higher priority candidate is eligible to forward a packet in the network. Some situations arise wherein multiple nodes tend to forward a packet due to acknowledgment reception failure. For this reason, each packet also contains a random nonce which is an arbitrary number that could be used only once.

**Trust-Based Opportunistic Routing Scheme**

Trust-based routing schemes include network security. In trust-based opportunistic Routing Scheme, security is added in the OR protocol. Security improvement of the network is increased while transferring various packets in the network, happening from source to destination.

***RSA Encryption Method***

RSA is one among the widely used security encryption system that is fully based on the number theory. RSA always ensures that the information that is passed along the network is confidential and is authenticated properly. This helps in providing secure communication over the network channel. The principle used in RSA is prime factorization that acts as the trapdoor for encryption. It makes use of public key where the receiver having the same public key alone can encrypt the data sent by the sender. On the other hand, it aims at providing a private key which is used to decrypt the information.

*Limitations of RSA Encryption Method*

One of the limitations of RSA encryption technique is its computational speed. It takes some time to compute the mathematical operations present in the RSA encryption algorithm. The public key is used for encryption and it needs to be authenticated. If the hacker is aware of the factors of large prime numbers then it would be very easy for him to crack the public key.

*Offline Storage of Public and Private Key*

The security and the speed of the RSA encryption are handled in the proposed method. They are increased by storing the parameters of the key through an offline storage. All the parameters used in the RSA encryption technique are stored in this offline storage database before the start of the algorithm. Two tables are present inside this database that is used to save the parameters of the keys.

***Flow Opportunistic Routing with flow node***

The flow is introduced in Opportunistic routing to select the forwarding node from the incoming nodes. If the incoming flow rate is large then the backlog traffic is rejected by the node. The node needs enough energy to receive and forward the packets in the network. Hence, the energy needs to be considered in a multi-hop wireless network. It gets affected by the new flow rate.

***Bandwidth***

All nodes in wireless ad-hoc networks have a limited bandwidth which serves as the new incoming traffic. Let us take k to be the number of incoming nodes and the set of total classes are denoted by (1,2,.....j,...,m). The class flow set is denoted as (1,2,.....,k,.....,$p_j$) where j node has $p_j$ flow with an intermediate node. When a new flow node needs to access an intermediate forwarding node it needs to consider the bandwidth allocation of the flows based on the average rate in the wireless ad-hoc network.

***TBOR Forwarding Scheme:***

A TBOR scheme is introduced in the proposed forwarding scheme. This scheme consists of three components.: 1) forwarding node set selection 2) Candidate's privatization 3) Opportunistic forwarding scheme. The former two parts determine the methods for selecting the forwarding node and the privatization policies for the forwarding node. The latter one determines when a node needs to update its node list and how to provide various QoS for different types of flows.

*Forwarding Candidate Set Selection*

An appropriate metrics for determining the forwarding candidates set are very essential. In the TBOR protocol, a new technique is projected to opt for the forwarding candidates set which are based on the flow node control and the trust value of the node $i^{th}$ candidate set. At the beginning of the algorithm, the distance between any two nodes in the network should be calculated using the location service module. A node's one-hop neighbours can be determined while setting the transmission range of the nodes. The nodes are selected based on the distance between each other and the destination node. In the TBOR scheme that is proposed in the paper, use of the priority metrics is done to decide the priorities of the node. The forwarded delivery ratio of the node indicates the probability that a data packet can be successfully transmitted to a recipient. The weight factors of the nodes are given by n1,n2,and n3. which determines the requirements of the application. It pays more attention to the bandwidth, energy, link delivery ratio requirements and the distance to the destination.

## IV. ARCHITECTURAL DESIGN

The architectural design of the proposed RSA model is shown in Fig.3. The design consists of a sender and a receiver node. The data being transmitted from node 1 are stored as n1 and the encrypted data is stored as e1. The values of n1 and e1 are stored in the database. The message is encrypted using KU - Unrestricted Public key where KU=(e1,n1). At the receiver end, the destination node fetches the value[9] of d1 and n1 from the database instead of fetching it from the actual values (d,n). The values are updated simultaneously in the database and the decryption of the message occurs using the value KU=(d1,n1). The messages transmitted from the

 

sender side to the receiver side are always authenticated. This is done to make the messages secure and no user without proper authentication can access or hack the packets being transmitted in the network.

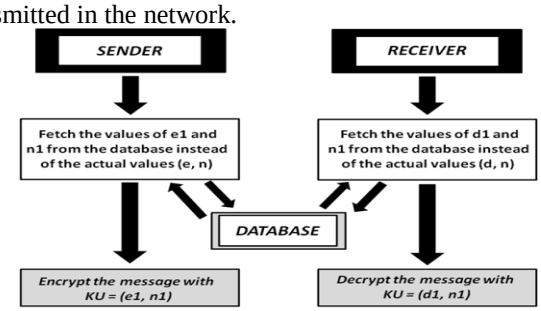


Fig.3 Architecture of Proposed RSA model

Fig.4 shows the two main operations that are being performed on the packets transmitted. The first operation is SECURITY where the trust level is built. The second operation is ADMISSION CONTROL where factors like bandwidth, backlog traffic and energy of the wireless networks are considered.

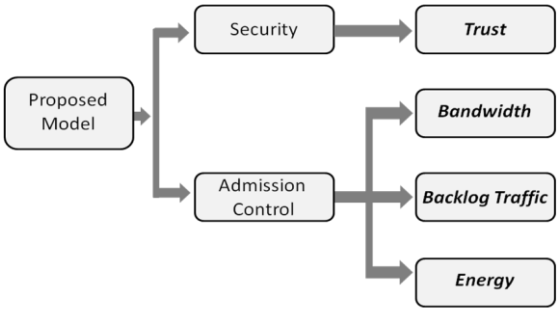


Fig.4 Operations performed in the Proposed Model

**Experimental setup**

The experiment was carried out using Linux OS along with NS2.34. C and C++ compilers were used for compiling the programs. The proposed model needed a hard disk with a capacity of more than 20GB and RAM size more than 513Mb. Pentium IV processor was used for processing the data. The hardware and software interfaces are discussed as follows:

*Hardware Interface:*

Linux and Unix environment was used. Random Access Memory is majorly used to the data in the system. The routeris intended to act as an internetworking device which helps to forward the packets between various networks. This is done by processing information that is found in the datagram. In most of the situations, the information is generally processed in combination with the routing table which is also known as a forwarding table. Routers, generally use routing tables in order to determine the interface that could be used to forward packets.

*Software Interfaces:*

The application was developed using NS2.34 in the front-end. Linux Ubuntu 11.04 Operating system was used. The software is also designed in such a format that it could interact with the TCP/IP protocol. The software was made permissible to interact with the Server Socket and TCL.

## V. SIMULATIONS

The simulations were performed using the NS2 simulator. The other parameters that were considered while simulating the proposed model are discussed as below:

Table 1 Simulation Parameters

| | |
|---|---|
| Simulation Software | Network Simulator 2 |
| Channel Used | Wireless |
| Runtime of Simulation | 100 seconds |
| The area in which nodes move | 1053X597 |
| Packet size | 1024bytes |
| Speed | 1m/s to 10 m/s |
| Routing Protocol | DSDV |
| Propagation model | Two Ray Ground |
| Type of Network Interface | Physical - Wireless |
| Queue - Type | Drop Tail |
| IFQ – Length | 50 packets |
| MAC - Type | Mac/802.11 |
| Antenna - Type | Omni Antenna |

**Test Cases**

The proposed analytical model was compiled and executed in the NS2 simulator and the following observations were recorded:

Table 2 Module and test cases of proposed model

| Module | Test case ID | Input | Expected Output | Actual output |
|---|---|---|---|---|
| Packet size | TC 01 | 1000 | As rate is 1000k, the packet transmission should begin. | Packet transmission started. |
| Input file (tcl file) | TC 02 | .tcl file | After successful execution of the .tcl file, name file are created. | Nam file is created and tcl file is executed. |
| Output file | TC 03 | .tcl file | Nam file should be Created. | Nam file created and Out.nam is created. |

 

| | | | | |
|---|---|---|---|---|
| Trace file | TC 04 | .tcl | Graphs must be displayed | .tr files generated |

## VI. RESULT AND DISCUSSION

The experiment was simulated in NS2 and the results were obtained as follows. Figure 5 & 6 shows the communication of sensor nodes in a network. The circles represents the transmitting range of a wireless sensor node.

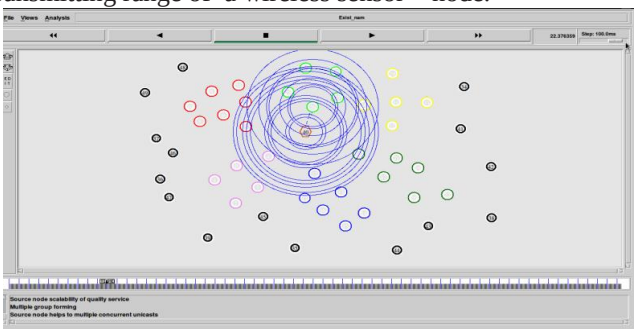

Figure 5 Nodes creation

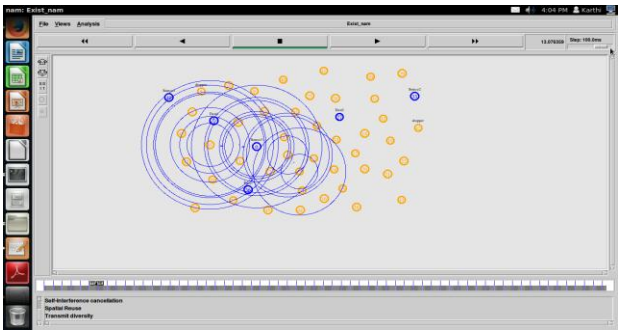

Figure 6 Nodes and Routes of an Opportunistic Routing Network

In Figure 7, the throughput of the Trust-based Opportunistic Routing (TBOR) was compared with that of the traditional Opportunistic Routing(OR) . The throughputs are calculated using the formula packet ratio x $10^3$.

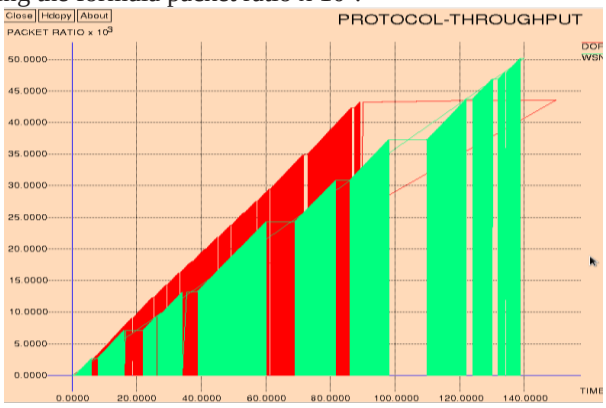


Figure 7 Protocol Throughput

Figure 8 shows the variation of the throughput and channel measurement of both the routing protocols in Traditional OR and Trust Based OR. The channel is measured by channel frequency x $10^3$.

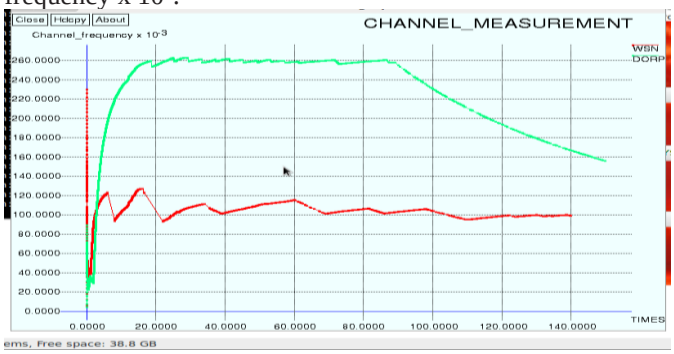


Figure 8 Channel Measurement

Figure 9 shows the delay measurement of TBOR and traditional OR.

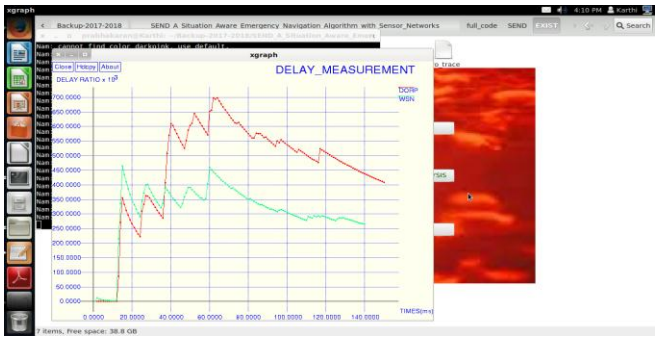


Figure 9 Delay Measurement

## VII. CONCLUSION

Opportunistic Routing (OR) is one of the predominant types of routing when it comes to broadcasting a packet in a network. All the nodes in the network are able to receive the packets and hence this reduces the probability of packet loss function. An analytical model is proposed in this paper, which is able to transmit a packet both in known and unknown topologies using single and multiple forwarders. The accuracy of the proposed model was verified using the NS2 simulator and the results showed an efficient result when compared to the previous models. A Trust-based Opportunistic Routing was also introduced to provided confidentiality and security to the packets being transmitted in the network. The future work can include an enhancement in the security aspect of the packets being transmitted in the wireless ad-hoc networks.

## REFERENCES

[1]. Royer, E.M.,andToh, C.K., 1999. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Commun., 6(2), pp.46-55[1].

 

[2]. Ballardie, "Core Based Trees (CBT Version 2) Multicast Routing - Protocol
Specification," RFC-2189, September 1997[2].
[3]. Li, J., Blake, C., De Couto, D.S., Lee, H.I. and Morris, R., 2001, July. The capacity of ad hoc wireless networks. In Proceedings of the 7th annual international conference on Mobile computing and networking (pp. 61-69). ACM[3].
[4]. Westphal, C., 2006, October. Opportunistic routing in dynamic ad hoc networks: The OPRAH protocol. In Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on (pp. 570-573). IEEE[4].
[5]. Nassr, M.S., Jun, J., Eidenbenz, S.J., Hansson, A.A. and Mielke, A.M., 2007, May. Scalable and reliable sensor network routing: Performance study from field deployment. In INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE (pp. 670-678). IEEE[5].
[6]. Yuan, Y., Yang, H., Wong, S.H., Lu, S. and Arbaugh, W., 2005, September. ROMER: resilient opportunistic mesh routing for wireless mesh networks. In IEEE workshop on wireless mesh networks (WiMesh) (Vol. 12)[6].
[7]. Jain, S. and Das, S.R., 2008. Exploiting path diversity in the link layer in wireless ad hoc networks. Ad Hoc Networks, 6(5), pp.805-825[7].
[8]. Biswas, S. and Morris, R., 2004. Opportunistic routing in multi-hop wireless networks. ACM SIGCOMM Computer Communication Review, 34(1), pp.69-74[8].
[9]. Zhou, X. and Tang, X., 2011, August. Research and implementation of RSA algorithm for encryption and decryption. In Strategic Technology (IFOST), 2011 6th International Forum on (Vol. 2, pp. 1118-1121). IEEE[9].
[10]. Issariyakul, T. and Hossain, E., 2012. Introduction to Network Simulator 2 (NS2). An Introduction to Network Simulator NS2(pp. 21-40). Springer, Boston, MA[10].

**Authors Profile**

The author M.Thenmozhi is currently pursing MPhil in Department of Computer Science, Sri Akilandeswari Women's College, Wandiwash.She has completed her M.Sc., Information Technology from University of Madras and B.Sc., Computer Science from Sri Akilandeswari Women's college – Wandiwash.

The author N.Tamilarasi is Working as an Assistant Professor and HOD in the PG and Research Department of Computer Science at Sri Akilandeswari Women's college – Wandiwash. She is having ten years of teaching and Research experience in the field of Computer Science. She has completed her B.Sc., Computer science from Shanmuga Industries Arts & Science college – Tiruvannamalai. M.C.A., and M.Phil., Computer science from Annamalai University – Annamalai Nagar. B.Ed from Pondicherry University – Pondicherry.And also she has Passed State level eligibility test(SET) in the year 2012 and National Eligibility test (NET) in 2018.she has published 13 International Journals and 2 National Journals.Currently she is doing Ph.D at Annamalai University.

 