A study of Adaptive Replication Technique in routing time-constrained messages (VoIP) in MANET

SWATI SAXENA
Research Scholar
AIM & ACT Banasthali Vidyapith
Banasthali, (Raj.)

Dr. MADHAVI SINHA
Asst. Prof. (HOD)
Dept. of Computer Science & Engineering
BIT Mesra, Jaipur Extension, Jaipur (Raj.)

ABSTRACT

Imposing the constraint of timely delivery on usual messages is referred as time-constrained messages. The utility of such messages depends upon the time at which they arrive at their destination. Due to contention among randomly arriving messages at each node/link and multi-hops between the source and destination that a message must travel, it is difficult to guarantee the timely delivery of such messages. In case of faulty links or node, it is likely impossible for messages to reach at required destination in time. To handle such type of faults, the idea of sending multiple copies or replicated copies is used. The probability of successful message delivery within time will be increased through sending multiple copies through disjoint routes, as at least one copy will be reached within time. But this will degrade the network performance due to congestion and other problems. Therefore, it is require sending only optimum number of copies through disjoint routes. Such copies are estimated on the basis of network load and message deadline. In this paper, we present the method to estimate the optimum number of copies. The system is designed for developing replication strategy named as Adaptive Fault Tolerance Replication Technique (AFTRT) for VoIP applications used for Mobile Ad hoc Network. The parameters such as end-to-end latency, node delivery index and message delivery probability are determine by the destination and send as feedback to the source. Based on this information, source replicates the message. The performance study is conducted through simulation using NS2 simulator.

Keywords: *Deadline, Fault Tolerance, Message Delivery Probability, Node Delivery Index.*

1. INTRODUCTION

Timely deliveries of inter-task messages are the desired requisite in real-time communication. Usual messages, augmented with a new parameter *deadline*, are referred as time-constrained messages. If such messages arrive at their destination after their deadline has expired, they may cause system failure. However, earlier arrivals of such messages also degrade the system performance because this requires buffering overhead. To deliver such messages timely, many approaches have been explored in the literature. In this paper we use the flooding approach in which same copies of the messages are transmitted along disjoint routes. This approach is named as multiple-copy approach [1] or replication approach. (The term multiple-copy and replication can be use interchangeably). Sending duplicate copy through disjoint route will increase the probability of reaching at least one copy of the message within time at its destination. But it may leads to congestion and increases the traffic load. It may also possible that messages with later deadlines affect the messages with shorter deadline. So, it is beneficial to send only required number of copies along disjoint routes. Such number should be estimated based on the current network load and message deadline. Sending out optimal number of copies through disjoint routes will increases the probability of reaching messages within their deadline and network load will remain under control.

Among numerous applications of time-constrained messages over real-time communication, we are using voice applications running over the Internet. It is referred as Internet telephony or Voice over Internet Protocol (VoIP). VoIP is defined as the transport of voice as packets in the IP based network. The IP network performs various functions such as collect calling, gateways into the public voice networks and associated events [2]. In addition to the maintenance of a reliable voice communication in a broadband environment, the development of the best cost-benefit relationship is ensured by the VoIP network. Assurance for specific quality is provided by the QoS parameter along with the supporting providers and users to attain Service Level Agreement (SLA). Based on the codec used for the compression technique, the preferred QoS and the channel capacity indeed vary in the VoIP network. In case of channel security, the encryption method can be changeable which in turn changes the throughput and the compression rate [3].

The paper is organized as follows: In the next section (section 2), we give the overview of related works from the literature about fault tolerant strategies opted by various routing protocols (used for time-constrained messages explicitly for VoIP data). In section 3, we explore the proposed algorithm. Based on the work on section 3, we frame out the proposed Adaptive Fault Tolerant Replication Technique (AFTRT) in section 4. Section 5 explores the simulation parameters used for performance study of the proposed algorithm and a comparative study is given. Section 6 concludes our work.

1.1 VoIP in MANET

A mobile ad hoc network (MANET) is a mobile, multihop wireless network that does not rely on any pre-existing infrastructure. Such networks are characterized by dynamic topologies due to uncontrolled node mobility, limited and variable shared wirless channel bandwidth and wireless devices controlled by battery power [4]. In [5], QoS required for Real-time voice conversations in IP networks is explored and the performance of VoIP in wireless ad hoc network is considered. Unlike the conventional VoIP implementation on fixed nodes, VoIP is implementing in MANET in the current scenario that guarantee the user about conveying the reliability of voice.

Faults in MANET

In order to exchange information, a node requires multiple hops in the MANETs due to restricted transmission power in the network. Therefore, routing discovery and maintenance are the major challenges to consider in MANETs [6]. Due to issues like unpredictability of environment, unreliability of wireless medium, resource-constrained nodes and dynamic topology, MANETs are susceptible to various types of **faults**. These faults can be grouped as follows [7]:

- *Transmission errors*
  Due to high transmission contention and congestion, the MANET systems suffer from high transmission error rate. Therefore, it is important to provide higher reliability for broadcasting operation under dynamic MANET system but it involves severe problems. In [8], a simple broadcast algorithm is proposed to improve the delivery ratio in an environment that has high transmission error rate.
- *Node or link failures*
  In ad hoc networks, packet losses occur mainly due to link failures or node failures. Due to such failures, the effect on the network performance is based on various factors. Among such factors, one of them is the routing protocol. In [9], the behavior of routing protocol is studied in case of path failure and presented an improvement scheme.
- *Route breakages*
  One of the important causes of route failure is the node failure which may be because of power shortage. By determining residual power in a particular node, the node failure can be predicted when the residual power goes lower than threshold value [10].
- *Congested nodes or links*
  Congestion may occur when certain nodes or links may over utilize. This may lead to long delay or many packet losses. In [11], a routing protocol for MANET is suggested that is aware and adaptive about network congestion.

1.2 Problem definition and Proposed solution

The proposed strategy is explored in [12] but it was designed for wired network and wormhole switching technique was used. Such concepts are not suitable for current scenario. The proposed strategy is developed for wireless network.

In [13], the contention based routing in mobile ad hoc networks with multiple copies is proposed. It is based on “spray-select-focus” algorithm where source sprays a few message copies into the network. Neighbors of that node receive a copy towards the destination. The technique of selecting neighbors is not specified in this paper. In most of the previous works based on replication technique assumed that the replication nodes (i.e. nodes responsible to replicate a message) are static. Unlike static nodes, the replication nodes should be adaptively estimates the number of copies based on the delivery probability.

Our objective is to design a replication technique for VoIP data in MANET by estimating the number of copies to be replicated. This is estimated by determining the optimum number of replication nodes. The proposed technique offers an adaptive fault tolerance method for replication of VoIP data packets as the optimum number of copies and the numbers of nodes responsible for replication process are changing according to the network load in hop be hop manner. The proposed strategy is named here as Adaptive Fault Tolerant Replication Technique (AFTRT).

A message will be replicated at either source node or at intermediate node. The source node replicates the multiple copies of the packet and they are destining to the intermediate nodes. The source maintains a forward node counter (FNC) with initial value *k* depending upon the current network load. Initially, the packets are replicated and send to *k*-hop neighborhood. From the neighbor nodes, the packets focus to reach the destination. On reaching the destination node, the average delay taken by the packet and the number of packets successfully received are send as feedback to the source. If the number of packets and the average delay are below some threshold, then source increases the FNC sequentially until the feedback goes above the threshold.

2. Related Works

A store-and-forward based routing (e.g. multi-copy relaying) for Intermittent Connected MANETs (ICMANs) is proposed in [14]. It replaces traditional routing technologies that were designed for fully connected paths. However, such multi-copy relaying strategies do not adapt to the frequent variations of the network conditions as they rely solely on the source to control the relaying process. The proposed approach provides an efficient way for packet delivery.

An adaptive coding control scheme is proposed in [15], to improve the quality of voice transport over wireless ad hoc network. The basic idea used here is to adapt the voice coding bit rate to the available network bandwidth so as to maximize the voice quality. The MOS standard is used here for mapping between the packet losses rates to the MOS value to control voice encoding bit rate.

A robust and secure framework for voice transmission over multipath MANET is proposed in [16]. The framework is robust not only against dynamically changing topology but also against adverse environment. A security analysis of the proposed scheme and the performance evaluation of framework are provided.

A fault tolerant multi path protocol to reduce the packet loss due to route breakage is proposed in [17] which uses a new route discovery mechanism. Nodes determine multiple disjoint routes with more battery power and residual energy, to every active destination. In this fault-tolerant mechanism, the received signal strength is measured and based on this value it can send warning packets to the previous node. The AOMDV protocol is used as a base for the multipath routing.

In [18], a novel bio-inspired protocol named as Eramobile (Epidemaic based Reliable and Adaptive Multicast for Mobile ad hoc networks) is proposed that aims to deliver multicast data reliably with minimal network overhead, even under adverse network conditions. With an epidemic-based multicast method, it copes with dynamic and unpredictable topology changes due to mobility. Also the mechanism used doesn't require maintaining any tree-like or mesh-like structure for multicasting. Equipped with many other distinguished features, the protocol is capable to deliver data reliably in both sparse and dense networks.

3. Proposed Work

In this section, we describe the topology learning, estimation of delay, end-to-end latency, Node Delivery Index, Message Delivery probability. On the basis of these parameters, an optimal number of replicated copies will be formulized.

3.1 Topology Learning

Using reliable path based topology learning technique, it is essential to enable the source to determine the path towards the destination. Considering the network consisting of several nodes, the source learns the topology in order to determine the possible efficient route to the sink by the following technique:

Initially the source sends a Topology Learning request (TLREQ) message to the nearest neighbors. The TLREQ message includes the information related to the source id, destination id and will also append the id of the nodes that forward the message towards the destination. Thus as the TLREQ message moves towards the destination, it includes all the information about the nodes involved in the transmission. On reception of the TLREQ message at the sink, it responds by sending a route reply (TLREP) message to the source through the reverse path.

Based on the number of TLREP messages received at the source, the source increments or decrements the forward node count (*FNC*). The source has a threshold value ($threshold_{TLREP}$) for the number of RREP messages and initially the FNC is set to a value *k* by the source.

If number of TLREP < $threshold_{TLREP}$, then FNC = FNC + 1

If number of TLREP > $threshold_{TLREP}$, then FNC = FNC – 1

(The FNC is the number of nodes that will receive the replicated copies.)
Fig. 1 shows the TLREQ message transmission from the source to the sink through the intermediate nodes. During the transmission, request transmitted across *src-d-i-k-n-sink*, *src-a-f-l-sink* and *src-e-g-j-m-sink* successfully reaches the sink. But the request transmitted across *src-b-h* and *src-c* are lost in the network. As the message gets forwarded, the *id* of every node is appended in the message.

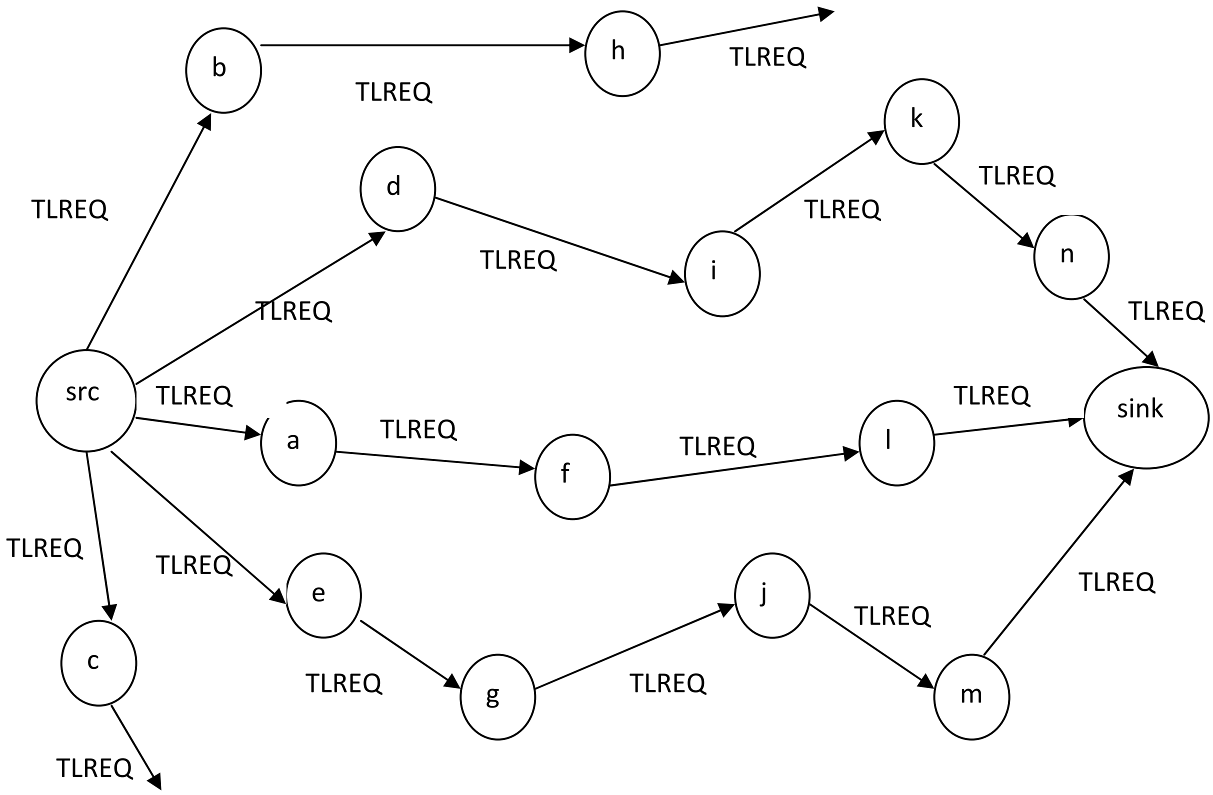

Fig.1: Transmission of TLREQ message from source to sink

Fig. 2 shows the TLREP message transmission from the sink to the source. On reception of the TLREQ message at the sink, it replies back by sending the TLREP message to the source through the same path used by the TLREQ message. The sink sends the TLREP message through the path used for corresponding TLREQ message by using the information appended during the transmission of the TLREQ message towards the sink. Out of the 5 TLREQ messages sent by the source, the total number of responses received is 3. The source on receiving the TLREP message now compares it with the total number of messages received with the threshold value set by it. If the threshold value set up by the source is 2 then since the number of received TLREP message is greater than 2, the FNC is reduced by 1.

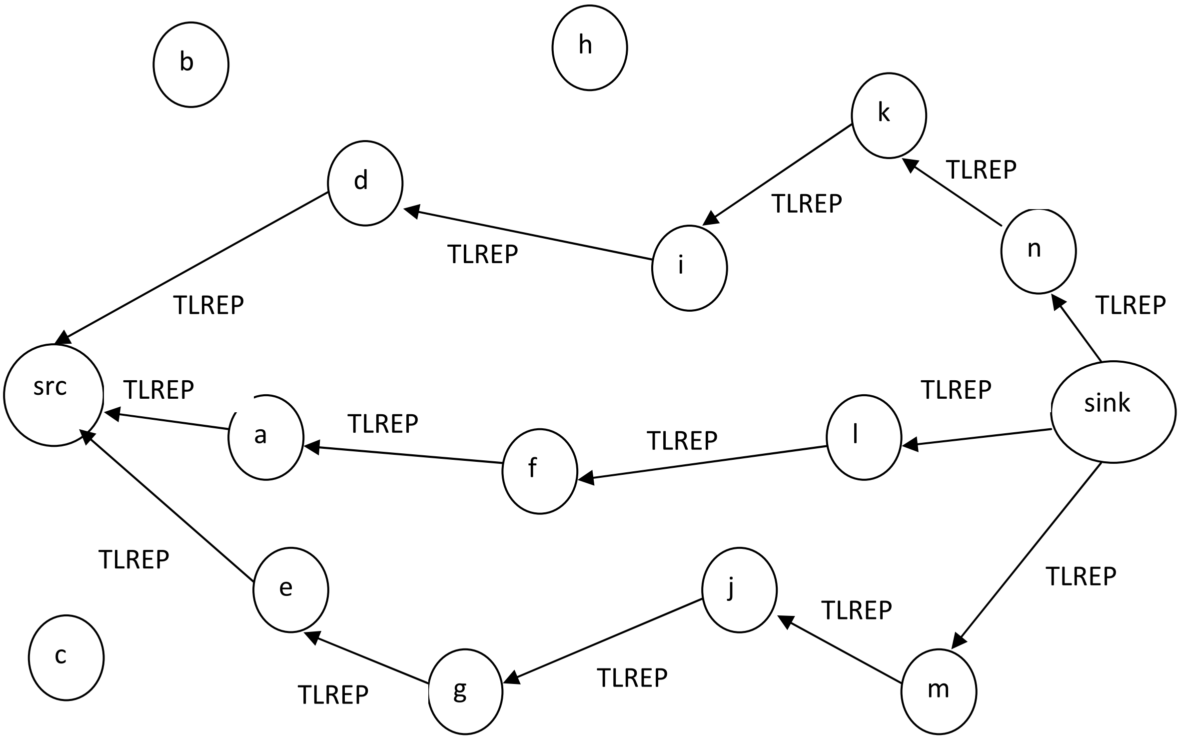

Fig.2: Transmission of TLREP message from sink to source

This process continues until the number of received TLREP messages at the source is greater than the threshold value $threshold_{TLREP}$. The aim of $threshold_{TLREP}$ is to pre-define the maximum number of reply received before a fractional part of deadline. It is not possible to wait for as much as reply those are receiving beyond deadline. Its value should be set by source based on task deadline and message deadline. Here, we have used some fixed value for the sake of simplicity.

3.2 Estimating Delay

We calculate the delay based on the probability function as follows. Initially we consider the delay in transmission to a node through one link [routing path =1]. Let us consider two hops m and n such that there exists a link l = (m,n). Hence the transmission latency of the message from m to n is characterized by the random variable defined as D_m and probability distribution function (pdf) is defined as the $P(D_m)$ such that the probability that m introduces a delay of at most $\in$ in forwarding the message to the next hop i.e.,

$$p_m(\in) = P(D_m \leq \in) \quad \ldots\ldots\ldots\ldots.. \quad (1)$$

The time interval between the messages entering the node t_{in} and acknowledge message reception from the receiver t_{ack} is regarded as the transmission latency of a message δ. But an extra time will be consumed for the reception of the acknowledge message and it is depicted by ρ. Hence transmission latency of the message is given by

$$\delta = t_{ack} - t_{in} - \rho \quad \ldots\ldots\ldots\ldots\ldots\ldots.. \quad (2)$$

Eq (2) depicts the delay at only one hop for every message, hence for the calculation of the delay during the transmission of the message through several hops i.e., throughout its path from source to destination. Therefore the total delay in the message transmission is obtained by the summation of the delay involved in every hop during the transmission from the source to the destination. For every hop, a particular value of ρ is obtained, so overall an increasing sequence of value $\rho_0, \rho_1, \ldots, \rho_k$ is generated. Each of these values represents a sample of the random variable D for the given hop. If the distribution of D was known, finding out the expected value and its probability or the probability of any given delay would be reduced to trivial. But if the value of *D* is not known then the sample mean and sample variance which characterizes the distribution should be used for calculation.

3.3 Estimating End-to-end latency

The end-to-end latency of a path *rp* (say) is also a random variable, D_{rp}, formed by the composition of the delays of its intermediate links:

$$D_{rp} = \sum_{\forall (i,j) \in rp} D_{(i,j)} \qquad \ldots\ldots\ldots\ldots\ldots\ldots \qquad (3)$$

$$p_{D_{rp}}(\tau) = P(D_{rp} \le \tau) \qquad \ldots\ldots\ldots\ldots\ldots\ldots \qquad (4)$$

Eq (4) indicates the probability for end to end latency where τ represents the at most value of end-to-end latency introduced in forwarding the message.

3.4 Estimating Node Delivery Index (NDI)

The data transmission is based on the parameter *Node Delivery Index* (*NDI*). It is the probability that a node correctly delivers data to the destination. NDI is useful in selecting routes based on its value.

Let NDI_i denotes the delivery index of a node N_i. The value of NDI_i initially set to zero and updated whenever there is a message transmission or timer expiration. Whenever a node Ni transmits a data packet to another node N_K, NDI_i should be updated such that

$$NDI_i = (1-\rho)\ NDI_i + \lambda\ NDI_k, \qquad \ldots\ldots\ldots\ldots\ldots\ldots \qquad (5)$$

Where NDI_k is the NDI of node N_k and $0 < \lambda < 1$ is a constant employed to keep partial memory of historic status. Clearly, NDI_i is always between 0 and 1. So if N_k is the destination, $NDI_k = 1$, since the message is already delivered to the destination successfully, otherwise, $NDI_k < 1$.

Also each node maintains a timer t_1. If there is no message transmission within an interval of ∂, then the timer t_1 expires. The timer expiration indicates that the node couldn't transmit any data during ∂. So NDI_i should be updated as

$$NDI_i = (1-\lambda) NDI_i \qquad \ldots\ldots\ldots\ldots\ldots\ldots \qquad (6)$$

So from (1) and (2), we arrive that, the node delivery index (NDI) of node N_i is updated as

$$= (1-\lambda)\ NDI_i + \lambda\ NDI_k, \qquad \text{if there is a data Transmission}$$
$$= (1-\lambda)\ NDI_i, \qquad \textit{if there is a Timeout} \qquad \ldots\ldots\ldots \qquad (7)$$

3.5 Estimating Message Delivery Probability (MDP)

The Message Delivery Probability (MDP) is used to represent the amount of redundancy and to indicate the importance of a given message. The MDP is defined to be the probability that at least one copy of the message is delivered to the destination within time in the network. We assume that each message copy carries a field to denote the MDP. When a message is generated, its MDP is initialized to be zero.

Let us consider a node N_i which is transmitting *k* copies of a data message j. Let $MDP^j{}_i$ denote the MDP of message j in the ready queue of messages in node N_i. The message transmitted to a node N_r is associated with a MDP of

$$MDP^j{}_{Nr} = 1 - (1 - MDP^j{}_i)\,(1 - \mathrm{NDI_i})\sum_{m=1}^{k}(1 - MDP^j_m) \quad \ldots\ldots\ldots \ (8)$$

and the MDP of the message at node N_i *is* updated as

$$MDP^j{}_i = 1 - (1 - MDP^j{}_i)\sum_{m=1}^{k}(1 - MDP^j_m) \quad \ldots\ldots\ldots. \ (9)$$

The above process repeats at each time when message *j* is transmitted to another node. In general, the more times a message has been forwarded, the more copies of the message are created, thus increasing its delivery index. As a result, it is associated with a larger MDP. Further, MDP is used to estimate the number of copies to replicate.

4. Algorithm of Proposed Adaptive Fault Tolerance Replication Technique (AFTRT)

The algorithm for our fault tolerant replication technique in the MANET considers the latency involved and the data delivery ratio in the network. The steps involved in the algorithm are as follows:

Step 1: The source (*S*) in need of service sends a Topology Learning Request (TLREQ) to all its nearest neighbors (*N*). This message is then forwarded by the neighbor node to its neighbor and it continues till the destination (S_k) is reached.

$$S \xrightarrow{TLREQ} N_1 \quad \ldots\ldots\ldots\ldots\ldots.. \quad N_n \xrightarrow{TLREQ} S_k$$

Step 2: In response to the request, the destination sends the Topology Learning Reply (TLREP) message through the path used for corresponding TLREQ message by using the information appended during the transmission of the TLREQ message towards the sink.

$$S \xleftarrow{TLREP} N_1 \quad \ldots\ldots\ldots\ldots\ldots.. \quad N_n \xleftarrow{TLREP} S_k$$

Step 3: Based on the number of the TLREP messages received, the source increments or decrements the forward node count (*FNC*). The source maintains a threshold value ($threshold_{TLREP}$) for the number of TLREP messages and initially the FNC is set to a value k by the source.

If number of TLREP < $threshold_{TLREP}$,
FNC = FNC + 1
else
FNC = FNC – 1

Step 4: For any link l = (m,n), probability $p_m(\in)$ that m introduces a delay of at most $\in$ in forwarding the message to the next hop is calculated as

$$p_m(\in) = P(D_m \leq \in)$$

where D_m is the random variable which characterizes the transmission latency of the message from *m* to *n*

Step 5: Transmission latency of the message, δ is given by

$$\delta = t_{ack} - t_{in} - \rho$$

where

t_{in} is the time at which the message enters the node

t_{ack} is the time at which the acknowledge message is received from the receiver

ρ is the extra time consumed for the reception of the acknowledge message

Step 6: The end to end latency, D_{rp} of the path *rp* (say) is represented as

$$D_{rp} = \sum_{\forall (i,j) \in rp} D_{(i,j)}$$

Step 7: The probability of end to end latency is represented as

$$p\, D_{rp}(\tau) = P(D_{rp} \leq \tau)$$

Step 8: The Node Delivery Index (NDI) represents the probability that a node correctly delivers data to the destination.

If there is a data transmission

$$NDI_i = (1-\lambda)\, NDI_i + \lambda\, NDI_k$$

else

$$NDI_i = (1-\lambda)\, NDI_i$$

Step 9: The MDP represents the probability that at least one copy of the message is delivered to the destination by other nodes in the network. The message delivery probability (MDP) of message j in the queue of node Ni, which is transmitting k copies to node Nr is given by

$$MDP^j{}_{Nr} = 1 - (1 - MDP^j{}_i)\,(1 - \mathrm{NDI_i}) \sum_{m=1}^{k} (1 - MDP^j_m)$$

and the MDP of the message at node Ni *is* updated as

$$MDP^j{}_i = 1 - (1 - MDP^j{}_i) \sum_{\mathrm{m=1}}^{\mathrm{k}} (1 - MDP^j_{\mathrm{m}})$$

Step 10: The destination determines the overall Node Delivery Index (NDI) along the path by adding the *NDI* values at every node.

$$NDI = \sum_{i=1}^{n} NDI_i$$

11] The calculated end to end latency, MDP and the NDI values of the path are transmitted as a feedback to the source by the destination. Based on this feedback, FNC value is incremented or decremented by the source accordingly.

The source maintains a threshold for the latency value $threshold_{LATENCY}$ and threshold for the NDI as $threshold_{NDI}$

If $D_{rp} >$ $threshold_{LATENCY}$ and $NDI_i < threshold_{NDI}$

FNC = FNC +f

Else

FNC = FNC –f

Where f is the scale factor used to increment or decrement.

Then the source replicates the packets according to the value of MDP and transmits to FNC number of nodes.

Number of replicated copies = MDP × θ

Where θ is the number of immediate neighbors of node N_i.

Thus, the algorithm considers the latency and the node delivery index value to replicate the packet in order to efficiently enable data transmission through reliable paths.

5. Simulation

In this section, we conduct the simulation-based performance evaluation of the proposed AFTRT scheme.

5.1 Defining parameters for simulation model

The performance of AFTRT scheme is evaluated through NS2 [19], network simulator. The channel capacity of mobile hosts is set fixed as 2 Mbps. For wireless LAN, the distributed coordination function (DCF) of IEEE 802.11 is used here as MAC layer protocol. Mobile nodes are assumed to move in a 1000 m × 1000 m region for 100 seconds simulation time. We performed the analysis by varying the network size as 25, 50, 75 and 100 nodes and the pause time for the mobile node is assumed to be 10 seconds. Nodes are randomly distributed in squared area. For the sake of simplicity, the speed of the mobile node is set fixed as 5 m/s. All the nodes are assumed to have the same transmission range of 250 meters. Each and every node may behave like a source or an intermediate or a receiving node.

The data traffic used here for simulation is VoIP. The VoIP Codec used is GSM.AMR, VoIP model used is one-to-one, VoIP Encoder used is Application/VoIPEncoder and VoIP Decoder used is Applicaition/VoIPDecoderOptimal. The packet size is considered as 512 b and rate of transmission is taken as 250 kb which can changes to 500 kb for another run of experiment. The number of VoIP frames per packet used is 2 and number of flows considered are 5.

Parameters defined in algorithm are initialized as: $\lambda=0.2$, k = 1, NDI = 0.

5.2 Performance metrics used for simulation

The performance of the AFTRT scheme is studied regarding its ability to adapt the network conditions and compared with the Adaptive Multi-Copy Routing (AMR) [18] protocol. To show that the proposed work is reliable and more packets delivered within time, it is required to choose some parameters. We use four metrics as overhead, average end-to-end delay, Packet delivery ratio and drop. Overhead may be defined as the total number of routing packets normalized by the total number of received packets. The average end-to-end delay is averaged over all surviving data packets from source to the destinations. The packet delivery ratio is the ratio of the number of packets received successfully and the total number of packets sent. Drop is defined as the number of packets drop or not received within time. We perform the analysis in two segments i.e. these metrics are studied for two protocols on the basis of varying the number of nodes and on the basis of changing the rates.

5.3 Results

A. Based on varying the number of nodes

First, we'll study the performance of metrics on varying the number nodes. The idea behind varying the number of nodes is to study the performance when network size increases gradually (not infinitely).

Fig. 3 represents the packet delivery ratio for the two protocols. It is clear that AFTRT achieves good delivery ratio as compared to AMR.

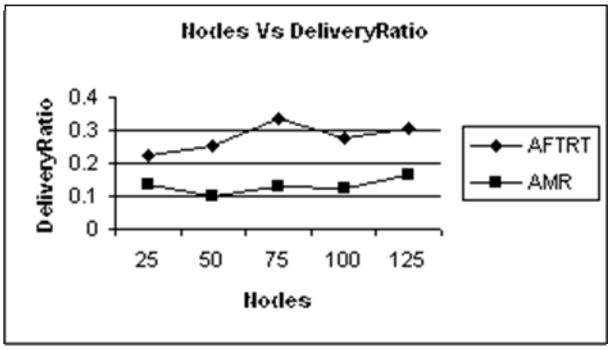

Fig. 3: Nodes vs. Delivery ratio

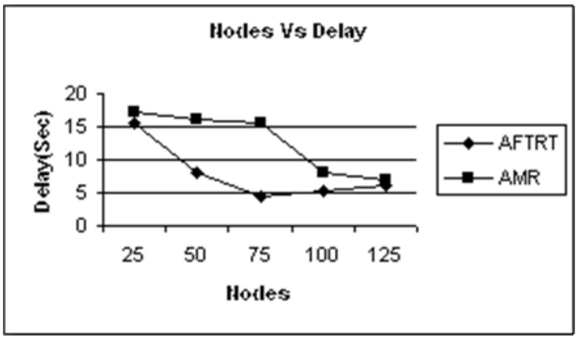

Fig. 4: Nodes vs. Delay

Fig. 4 shows that average end-to-end delay of the proposed AFTRT protocol is less than compared to the AMR protocol.

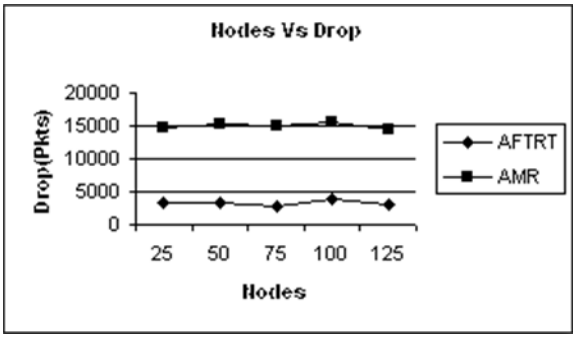

Fig. 5: Nodes vs. Drop

Fig. 5 shows the result of drop metric, which shows that AFTRT scheme has lower drop rate than that of AMR scheme.

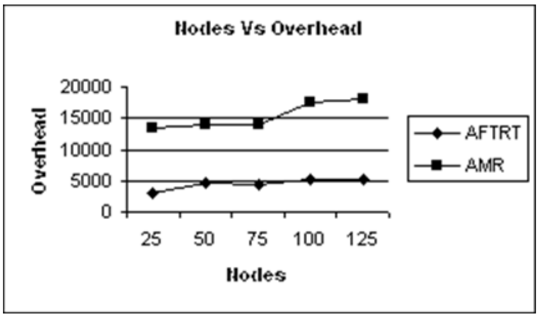

Fig. 6: Nodes vs. overhead

Fig. 6 ensures us that the overhead is less for AFTRT than that of AMR.

B. Based on varying the Rate

Now, in the second experiment we study the behavior of metrics when rate is varied as 250, 300, 350, 400, 450 and 500.

Fig. 7 shows the delivery ratio for the two protocols under varying the rates. It is clear that AFTRT achieves good delivery ratio as compared to AMR protocol again.

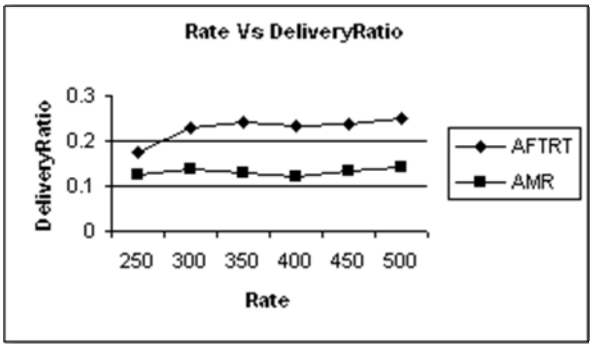

Fig. 7: Rate vs. Delivery ratio

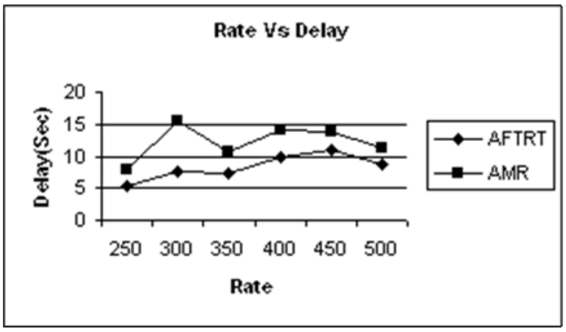

Fig. 8: Rate vs. Delay

From fig. 8, we can observe that the average end-to-end delay of the proposed AFTRT protocol is less compared to the AMR protocol.

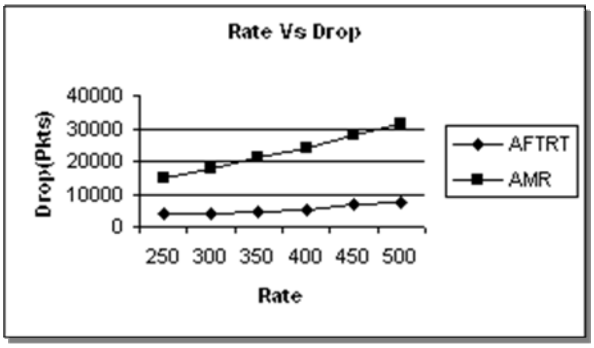

Fig. 9: Rate vs. Drop

Fig. 9 represents the result of packet drop. Again AFTRT scheme perform superior to AMR scheme regarding drop metric.

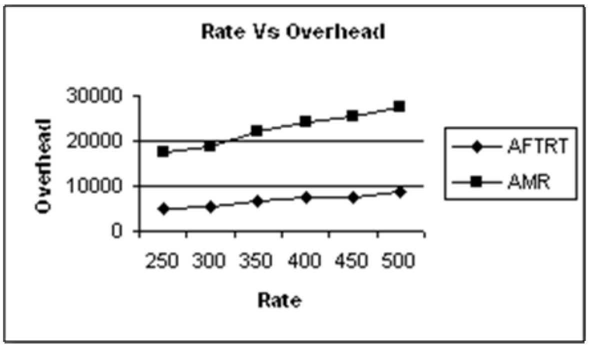

Fig. 10: Rate vs. overhead

From fig. 10, we can ensure that the overhead is less for AFTRT as compared to AMR.

6. Conclusion

Timely delivery of time-constrained messages is the foremost requirement for real-time communication applications. To make routing as fault tolerant, we proposed a multiple-copy or replication strategy that is adaptive. In this paper, we proposed Adaptive Fault Tolerance Replication Technique (AFTRT) to replicate the data packets with fault tolerance. Adaptive in the sense that it adapts current network conditions to estimate the number of replicate copies. Initially, the source in need of service performs topology leaning by issuing the topology learning request (TLREQ). After the reception of the topology learning reply (TLREP) from the destination, the source calculates the delay and node delivery index (NDI). One the NDI for a particular pair of link is determined, and then overall NDI is calculated from source to destination. The source maintains the threshold for the latency and NDI values. On estimating the latency and the overall NDI value, the source compares it with the threshold value and then the FNC value is incremented or decremented accordingly. This process is continued until the threshold value is reached. The source also estimates the message delivery probability (MDP). Then it replicates the packets according to the value of MDP and transmits to FNC number of nodes.

7. References

[1] K.G. Shin, C. M. Krishna, "*Real-time Systems"*, Tata McGraw Hill Publications

[2] Eduardo B. Fernandez, Juan C. Pelaez and Maria M. Larrondo-Petrie, "*Security Patterns for Voice over IP Networks"*, Vol 2, No.2, August 2007

[3] Edward Paul Guillen, Diego Aljandro Chacon, "*VoIP Networks Performance Analysis with Encryption Systems"*, World Academy of Science, Engineering and Technology 2009.

[4] Mahesh K. Mishra, Samir R. Das, "*Ad hoc on-demand multipath distance vector routing"*, Wireless Communications and Mobile Computing, 2006 pp. 969-988, published online in Wiley InterScience.

[5] Hui Yao Zhang, Marek E. Bialkowski, Garry A. Einicke and John Homer, "*An Extended AODV Protocol for VoIP Application in Mobile Ad Hoc Network*", Transactions on Electrical, Engineering, Electronics and Communications ECTI, vol 7, No. 2, August 2009.

[6] Fujian Qin and Youyuan Liu, "*Multipath Based QoS Routing in MANET*", Journal of Networks, vol. 4, no. 8, October 2009.

[7] Stephen Mueller, Rose P. Tsang, Dipak Ghosal, "*Multipath Routing in Mobile Ad hoc Networks: Issues and Challenges*", Lecture Notes in Computer Science, vol. 2965, April 2004, pages: 209-234.

[8] R. Balakrishna and U. Rajeswara Rao, G. A. Ramachandra, "*Reliability in MANET's Using Enhanced Double Coverage Broadcasting (EDCB)*", International Journal of Advanced Networking and Applications, vol 01, Issue 03, pg: 147 – 153, 2009.

[9] X. Hou and D. Tipper, "*Impact of Failures on Routing in Mobile Ad Hoc Networks Using DSR*", Proceedings of Communication Networks and Distributed Systems Modeling and Simulation Conference, January 2003, Orlando, FL.

[10] M. A. Razzaque, Simon Dobson and Paddy Nixon, "*Cross layer self routing: a self-managed routing approach for MANETs*", In proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications. IEEE Press. pp 284- 290, 2008.

[11] Duc A. Tran, Harish Raghavendra, "*Routing with Congestion Awareness and Adaptivity in Mobile Ad hoc Networks*", Journal of IEEE Transactions on Parallel and Distributed Systems archive, vol 18, Issue 7 July 2007.

[12] Swati Saxena, "*An Approach to Fault-tolerant Routing in time-constrained messages (using multiple-copy)*", National Conference on Advancements inInformation & Communication Technology (NCAICT - 2008), organized by Computer Society of India, Allahabad Chapter, March 15-16 2008.

[13] Ms. E. Jenefa Jeba Jothi, Dr. V. Kavitha and Ms. T. Kavitha, "*Contention Based Routing in Mobile Ad Hoc Networks with Multiple Copies*", International Journal of Engineering and Technology vol.2(2), pp.93-96, 2010

[14] Zhoqun Li, Lingfen Sun, Emmanuel C. Ifeachor, "*Adaptive Multi-Copy Routing for Intermittently Connected Mobile Ad Hoc Networks*", In Proceedings of GLOBECOM' 2006.

[15] Hongqi Zhang, Jiying Zhao and Oliver Yang, "*Adaptive Rate Control for VoIP in Wireless Ad Hoc Networks*", In Proceedings of GLOBECOM' 2006.

[16] Binod Vaidya, Mieso K. Denko and Joel J.P.C. Rodrigues, "*Secure Framework for Voice Transmission Over Multipath Wireless Ad-Hoc Network*", Proceedings of the 28th IEEE conference on Global telecommunications (GLOBECOM), pp. 4299-4304, 2009.
[17] G. Rajkumar, K. Duraisamy, "*A Fault Tolerant Multipath Routing Protocol to Reduce Route Failures in Mobile Ad Hoc Networks*", European Journal of Scientific Research, Vol.50, no. 3, pp. 399-408, 2011.
[18] Öznur Özkasap, Zülküf Genç, Emre Atsan, "*Epidemic-based reliable and adaptive multicast for mobile ad hoc networks*", Journal of Computer Networks 53(9): pp 1409-1430 (2009).
[19] Network Simulator, http://www.isi.edu/nsnam/ns

AUTHOR'S PROFILE:

Swati Saxena
Research Scholar
AIM & ACT, Banasthali Vidyapith,
Banasthali, (Raj.)

Dr. Madhavi Sinha
She received her Ph.D. degree from Banasthali Vidyapith, Banathali (Raj.) and currently working as Associate Professor and Head of Department (Computer Science & Engineering) at Birla Institute of Technology, Jaipur (Raj.). She has 25 years of teaching experience and published many National and International publications. Her research interests are Artificial Intelligence, soft and language computing.