ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Efficient Node Approach For Reducing Congestion By Using Traffic Aware Routing Protocol In Ip Networks

Priyadharshini.S [1], Govindaraj.v [2]

P.G. Student, Muthayammal Engineering College, Rasipuram, Namakkal, Tamilnadu, India[1]

Assistant Professor, Muthayammal Engineering College, Rasipuram, Namakkal, Tamilnadu, India[2]

ABSTRACT: Backup paths are frequently used in IP networks to prevent from IP links failures. In existing systems such as the independent model and dependent model do not precisely find the correspondence between IP link failures, and it cannot choose dependable backup paths. A lightweight proactive source routing protocol can also be developed for the information exchange among neighbouring nodes it causes overloading of packets. We propose a efficient node approach for reducing congestion by using Traffic aware routing protocol in IP networks. We develop a probabilistically correlated failure (PCF) model to measure the impact of IP link failure on the dependability of backup paths. Then we proposed a new traffic aware dynamic routing protocol called TAR to relieve congestion in MANET. With new improved TAR we have minimize delay and traffic and increase throughput while maintaining file sharing.TAR avoid congestion by detecting Hot Spot and reducing traffic. This method helps nodes and sinks to find location of all the nodes in the network, which will make the node to find traffic areas and transfer the file through high efficient nodes, which will improve the network performance.

KEYWORDS: Routing, Traffic aware routing protocol, congestion, IP networks, MANET.

INTRODUCTION

IP link failures are common in the Internet for various reasons. In high speed Internet Protocol networks like the Internet backbone, detachment of a link for several seconds can lead to millions of packets being dropped [1]. In this layered structure, the IP layer topology i.e., logical topology is embedded on the optical layer topology, and each IP link is mapped to a light path in the physical topology. An IP link consists of multiple fiber links, and a fiber link is distributed by multiple IP links. All the logical links will fail concurrently because of fiber link failure. Logical link failures were considered as dependent failures or modelled as a Shared Risk Link Group (SRLG) model. [2].In Lightweight Proactive source routing protocol which frequently share the information among the neighbour nodes for update the network topology information [3]. Reactive two- phase rerouting (RTR) approach is used it has two phases of works. In first phase RTR first forwards packets around the failure area to gather information on failure. In the second phase, RTR determines a new shortest path and forwards packets along it via source routing**.** [4]. A node re-routes a packet around the failed link without the knowledge of the second link failure. In this RTF and STF schemes are used for packet forwarding. [4]. In the Weighted – Shared risk link group (WSRLG) scheme binary search algorithm is used. Where WSRLG control the weight of the SRLG factor by using a binary search algorithm, while fulfil the required number of disjoint paths between source and destination nodes. [5] A cross-layer approach for IP link protection is based on the topology mapping, a correlated failure probability model can be developed to calculate the impact of IP link Failure on the dependability of backup paths. With this model, a heuristic algorithm and multiround algorithm can be proposed to choose the backup paths with minimum failure probability and it considers the bandwidth constraint in backup path selection. It aims at choosing backup paths to minimize the traffic disruption caused by link failures.[6].In this Routing Configurations recovery scheme is used for both the node and link failures. Due to the load distribution congestion can be occurred. MRC is used to overcome this problem. It is connectionless, and deduce only destination based hop-by-hop forwarding. It can be implemented with only Small changes to existing systems. In Fig. 1,

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

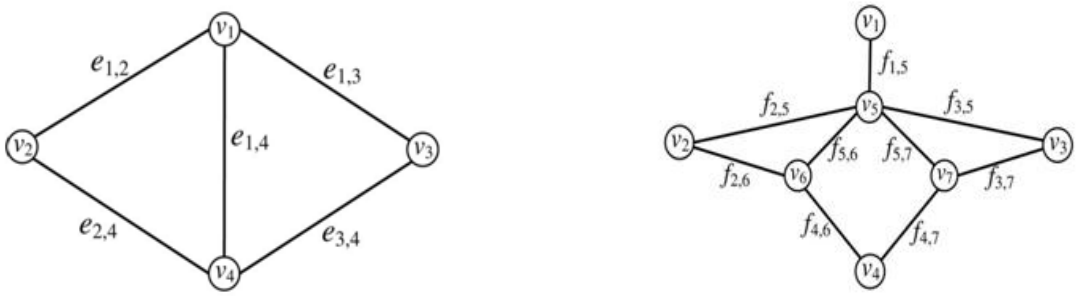
Vol. 4, Special Issue 6, May 2015

First while fiber link $f_{1,5}$ fails, then logical links $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ will fail jointly. This shows that the $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ are considered as independent failures. Second, sharing fiber links will cause logical links fails together in the same SRLG must be fail together. For example, $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ are in the similar SRLG method. While $e_{1,4}$ fails, it does not specify the $e_{1,2}$ and $e_{1,3}$ must also fail. If the failure of $e_{1,4}$ is affected by fiber link $f_{4,7,}$ $e_{1,2}$ and $e_{1,3}$ may be survive. In up to date Internet measurements of [7], illustrate that independent failures and correlated failures coexist in the Internet. [9]. Failures are first distinguish based on patterns experiential at the IP-layer; where it is possible to additional deduce their probable basis, such as protection activities and router-related activities.

Key sequential and spatial features of each class are examined and, when suitable, constraint using predictable distributions. Our results delegate that 20% of failures occur during a period of scheduled protection activities of the unexpected failures, nearly 30% are joint by multiple links and are generally probable due to router-related and optical equipment- related inconvenience; whereas 70% change a single link at a time. In our categorization of failures make known the original and level of failures in the race of IP backbone. [8].A probabilistic outlook of network failures are obtained where multiple failure consequence can occur concurrently, and expand algorithms for discovery of diverse routes with smallest amount of joint failure probability. Additionally, expand a narrative Probabilistic Shared Risk Link Group (PSRLG) framework for representing correlated failures.[10]. A backup path is chosen to be disjoint path from the main path, or in the network level, backup paths are deals with all links. The validity of this simple choice is based on 1) all the links may fail with equivalent probability; and 2) realize the high protection condition today, having links not defended or sharing links between the primary and backup paths immediately just look weird. Then vigilantly examine the functioning details and the overhead for common backup path schemes of the Internet at present. Originate an optimization problem where the routing performance should be definite and the backup cost should be diminished. This cost is exceptional as it occupies computation overhead.

When $e_{1,4}$ fails, it may be considered as independent or correlated failure due to shared fiber links. Consequently, $e_{1,2}$ and $e_{1,3}$ might be fail with a definite probability, i.e., failures of $e_{1,2,}e_{1,3,}$ and $e_{1,4}$ links are probabilistically correlated. These features cannot be determined and has not been enquired in backup path selection.

Fig.1. Mapping between the logical and physical topologies.



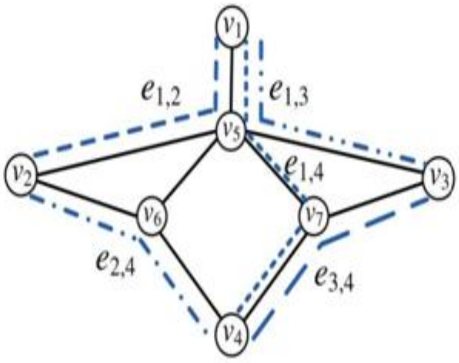
(a)Logical topology (b) Physical topology

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015



(c) Connected between the logical and fiber links

New method is different from previous works in three aspects. First, it is based on a multiple backup path, which considers the connection between logical and physical topologies. The proposed PCF model can reveal the probabilistic correlation between logical link failures. Second, each logical link can be sheltered with multiple backup paths to productively reroute traffic and prevent from link overload, then most prior works select single backup path for each logical link. Third, our method considers the traffic load and bandwidth constraint. It assured that the rerouted traffic load does not exceed the usable bandwidth, yet when multiple logical links fail concurrently.

I. EXISTING SYSTEM

In existing system two methods are developed for link failures but it does not exactly find the connection between the IP link failure.[4].In first method Shared Risk Link Group (SRLG) model Binary search algorithm is used to find the path from a given network topology. It does not accurately reflect the correlation between IP link failures. [2]. Lightweight Proactive source routing protocol which frequently share the information among the neighbour nodes for update the network topology information which causes congestion of nodes. [5].In second method correlated failure probability (CFP) model has two algorithms Heuristic algorithm and multi-round algorithm is used. The first algorithm concentrates on choosing the backup paths with smallest amount of failure probability. Then the second algorithm additionally believe that the bandwidth constraint and aims at minimizing the traffic disruption caused by failures. It causes low recovery rate. In existing traditional methods supporting P2P MANETs are either flooding-based or advertisement-based. The former methods rely on flooding for file searching. However, they lead to high overhead in broadcast. In the latter methods, nodes advertise their available files, build content tables, and forward files according to these tables. But they have low search efficiency because of expired routes in the content tables caused by transient network connections. Also, advertising can lead to high overhead.

II. METHODOLOGY

3.1 THE PCF MODEL

The PCF model is built on three types of in formations, i.e., Topology mapping, failure possibility of fiber links, and failure possibility of logical links, all of which are already collected by ISPs. In real ISPs built their topology mapping and they have this information. The failure possibility of fiber links and logical links can be obtained with Internet measurement approaches [7], [8] arranged at the optical and IP layers. Observing mechanisms at the Optical layer can notice fiber link failure in SONET alarms. These sequences of logical link failures can be getting from routing updates. ISPs also maintain failure sequences, because they observe the optical and IP layers of their networks. In carry out, it may get $p_{i,j}$ and $q_{m,n}$ based on preceding logical link and fiber link failures. Let $a^{i,j}_{m,n}$ distinct in Eq.(1) position the mapping between logical link ei,j and fiber link $f_{m,n}$

$$a_{m,n}^{i,j} = \begin{cases} 1 & \text{if } e_{i,j} \text{ is embedded on } f_{m,n} \\ 0 & \text{otherwise.} \end{cases} \quad (1)$$

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

$F_{i,j}$ is defined by Eq.(2) deduce that a fiber link $f_{m,n}$ holds $e_{i,j}$, i.e., $a^{i,j}_{m,n=1.}$ If there is an one more logical link $e_{s,t}$ is also carried by $f_{m,n}$, $f_{m,n}$ is in the set $F_{i,j}$

$$F_{i,j} = \{f_{4n} | a^{ij}_{m,n} a^{st}_{m,n} = 1, e_{i,j} \in E_L, \exists e_{S,t} \in EL, \forall f_{M,n} \in F_P\} \quad (2)$$

As fiber link failures are independent, $p^c_{i,j}$ is work out by Eq.(3). If $e_{i,j}$ does not distribute a fiber link with other logical links, its correlated failure probability is 0

$$p^C_{i,j} = \begin{cases} 0 & \textbf{if } F_{i,j} = \emptyset \\ 1 - \prod_{f_{m,n} \in F_{i,j}} (1 - q_{m,n}) & \textbf{otherwise.} \end{cases} \quad (3)$$

If the independent failure probability of $e_{i,j}$ is p^Ii,j. The relation shown in Eq. (4), since failures of $e_{i,j}$ are moreover independent or correlated. In Lemma 1 shows that $p^I_{i,j}$ must be rigorously less than unity

Ошибка! Источник ссылки не найден. (4)

Lemma 1. $p^I_{i,j} \in [0,1)$.

Proof. According to Eq. (4), $p^I_{i,j} = \frac{p_{i,j} - p^C_{i,j}}{1 - p^C_{i,j}}$. Since $q_{m,n} \in [0,1)$ for each fiber link $q_{m,n}$, we have $p^C_{i,j} \in [0,1)$. Together with $p_{i,j} \in [0,1)$, we have $p^I_{i,j} < 1$. Therefore, $p^I_{i,j} \in [0,1)$. □

Case1: In $e_{i,j}$ is not implanted on $f_{m,n}$. It means that the breakdown of $e_{i,j}$ is not connect with $f_{m,n}$. Hence,**Ошибка! Источник ссылки не найден.Ошибка! Источник ссылки не найден.** is equal to $q_{m,n}$.

Case2: In $f_{m,n}$ just carries $e_{i,j}$, then a failure of $f_{m,n}$ conduct to an independent failure of $e_{i,j}$. In this case, **Ошибка! Источник ссылки не найден.**is computed by Eq.(5),where **Ошибка! Источник ссылки не найден.** is the probability of that $e_{i,j}$ has an independent failure. While it becomes failure, and **Ошибка! Источник ссылки не найден.**is the probability of independent failure is happened by $f_{m,n}$

$$P(f_{m,n} | e_{i,j}) = P(e^I_{i,j} | e_{i,j}) * P(f_{m,n} | e^I_{i,j}) \quad (5)$$

In Eq.(6), **Ошибка! Источник ссылки не найден.**is the failure probability of $e_{i,j.}$ when its independent failures occur, which is set to be 1. **Ошибка! Источник ссылки не найден.** is the independent failure probability of $e_{i,j}$,

$$P(e^I_{i,j} | e_{i,j}) = \frac{P(e_{i,j} | eI_{i,j})}{P(e_{p,j})}$$ **Ошибка! Источник ссылки не найден.**

= **Ошибка! Источник ссылки не найден.** (6)

Ошибка! Источник ссылки не найден. (7)

Where the conditional failure probability of $P(f_{m,n} | e_{i,j})$ is given by Eq. (8), It is just defined for $e_{i,j}$ whose failure probability of $p_{i,i}$ is not 0. If $p_{i,i}$ is 0, $e_{i,i}$ certainly not fails, and they do not need to select backup paths for it

$$P(f_{m,n} | e_{i,j}) = \begin{cases} q_{m,n} & a^{i,j}_{m,n} = 0 \\ \frac{q_{m,n}}{p_{i,j}} & a^{i,j}_{m,n} = 1. \end{cases} \quad (8)$$

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Lemma 2. *If $f_{m,n}$ carries $e_{i,j}$ and $q_{m,n} > 0$, $P(f_{m,n}|e_{i,j}) > q_{m,n}$.*

Proof. If $f_{m,n}$ carries $e_{i,j}$, the second case of Eq. (8) holds, i.e., $P(f_{m,n}|e_{i,j}) = \frac{q_{m,n}}{p_{i,j}}$. Since $q_{m,n} > 0$, the failure probability of $e_{i,j}$ is above 0. Since $p_{i,j} \in [0,1)$, we have $p_{i,j} \in (0,1)$. Therefore, $P(f_{m,n}|e_{i,j}) = \frac{q_{m,n}}{p_{i,j}} > q_{m,n}$. □

$$P\left(\epsilon_{s,t}^{C}|e_{i,j}\right) = \begin{cases} 0 & \text{if } F_{s,t} = \emptyset \\ 1 - \prod_{f_{m,n} \in F_{s,t}} \left(1 - P(f_{m,n}|e_{i,j})\right) & \text{otherwise.} \end{cases} \quad (9)$$

Found on this, Eq. (10) computes the failure probability of $e_{s,t}$ below the condition that $e_{i,j}$ fails, which is denoted by **Ошибка! Источник ссылки не найден.**

Ошибка! Источник ссылки не найден. (10)

3.2 AD-HOC ROUTING PROTOCOL

An ad-hoc routing protocol is standard, that controls how nodes choose which way to route packets between computing devices in a mobile ad hoc network .In ad-hoc networks, nodes are not familiar with the topology of their networks. Alternatively, they have to determine it. The fundamental idea is that a new node may declare its presence and should listen for declaration broadcast by its neighbours. Each node learns about adjacent nodes and how to reach them, and may announce that it too, can arrive them. Note that in a extensive sense, ad hoc protocol can also be used accurately, that is, to denote an spontaneous and often protocol is established for a specific purpose.

3.2.1 Table-driven (Pro-active) routing

This type of protocols maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network.

3.2.2 On Demand (Reactive) routing protocol

This type of On-demand routing protocol finds a route by flooding the network with Route Request packets.

3.2.3 Optimized Link State Routing Protocol (OLSR)

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad hoc networks, can be employed on other wireless ad hoc networks. Where OLSR is a proactive link-state routing protocol, which uses hello packets and topology control (TC) messages to discover and then disseminate link state information is right through the mobile ad hoc network. Particular nodes use this topology information to process next hop destinations for all nodes in the network using shortest hop forwarding paths. Being a proactive protocol, OLSR uses power and network resources in order to propagate data about possibly idle routes. Whereas this is not difficulty for wired access points, and laptops, it makes OLSR inappropriate for sensor networks that try to sleep most of the time. In place of small scale wired access points with minimal CPU power, the open basis OLSR project illustrate that large scale mesh networks can run with OLSR on thousands of nodes with very little CPU power on 200 MHz embedded devices.

3.3 MANET

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized organization. Where Mobile Ad-hoc networks are self-organizing and self-configuring multihop wireless networks while, the arrangement of the network changes dynamically. This is mostly due to the mobility of the nodes. Where nodes in these networks employ the same random access wireless channel, work together in a friendly manner to appealing themselves in multihop forwarding. Where the nodes in the network are not only act as hosts but also act as routers that route data to/from other nodes in network. Then in mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and given that a destination node capacity will be out of range of a source node transmitting packets; a routing
Procedure is always needed to find a path so as to forward the packets appropriately between the source and destination. Inside a cell, a base station can attain all mobile nodes without routing via broadcast in regular wireless networks. In

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

the system of ad-hoc networks, each node have to be able to forward data for other nodes in the networks. This creates supplementary problems with the length of the problems of dynamic topology which is unpredictable connectivity changes.

Network Formation:

Here, we have to create nodes. We select the source and destination. After selecting the source and destination, source wants to send the data to destination. So we need a route for data sending and receiving acknowledgements. In this module each and every nodes assign its position in network for communicate each others.

Multiple Node Sharing

In this module we shows the all the shared files are stored in the multiple peer for this reason we can easily search the file from multiple peer. It will reduce the file searching content from all peer and reduce the time consuming.

Traffic Aware Routing

In this we define the how to reduce the traffic to get the file from multiple nodes in existing we select the single path for file sharing and now we use the traffic aware routing for reduce the traffic that means our searching file is fetching from correct peer it will select only one path for this reason all data over the same path with same node its way to create the traffic. So we use TAR whenever the traffic occurs it will select the other path with efficient node.

III. RESULTS AND DISCUSSIONS

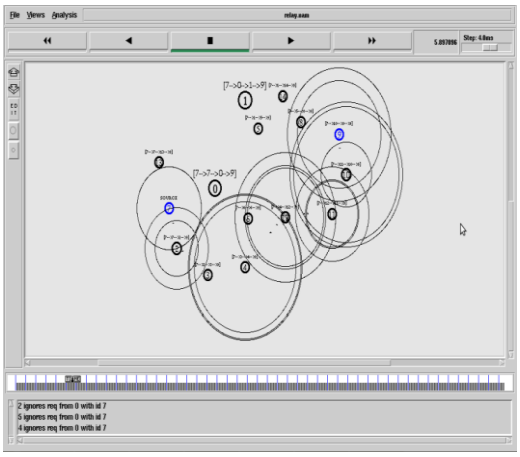


Fig 4.1 Signal broadcasting

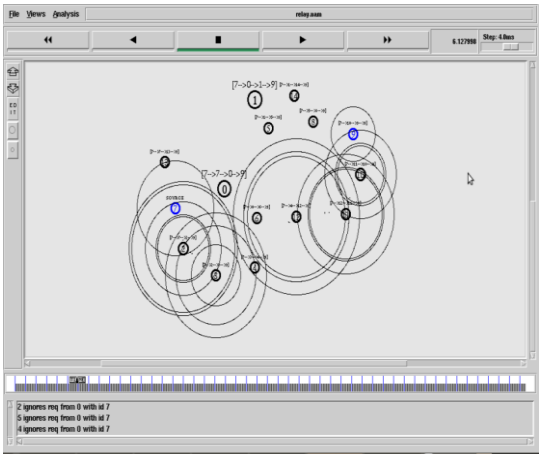


Fig 4.2 packet transfers from source to neighbour node

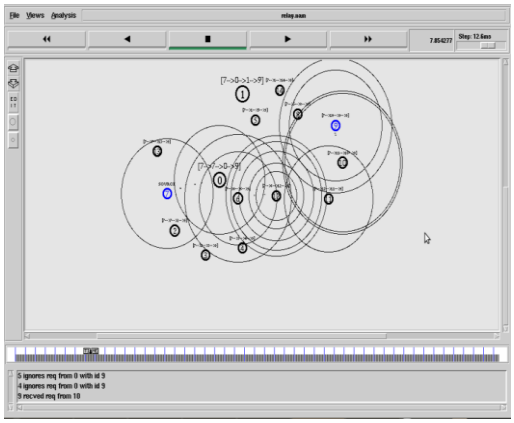


Fig 4.3 Source node receiving ack from neighbour node

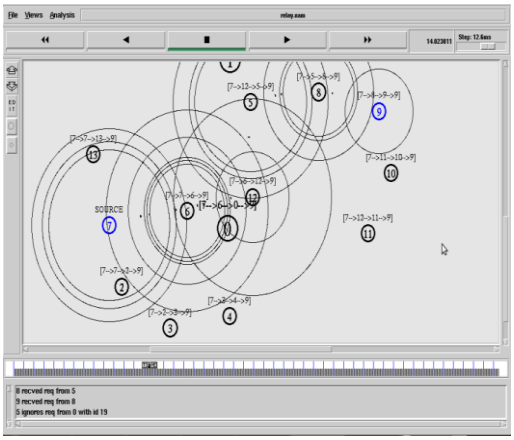


Fig 4.4 node moves and exceeds the coverage area

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

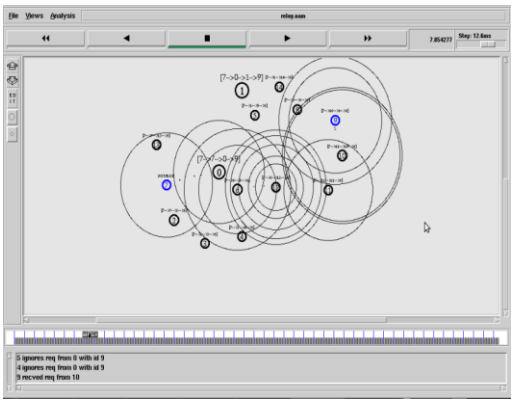


Fig 4.5Source reroute the packets to next neighbor node

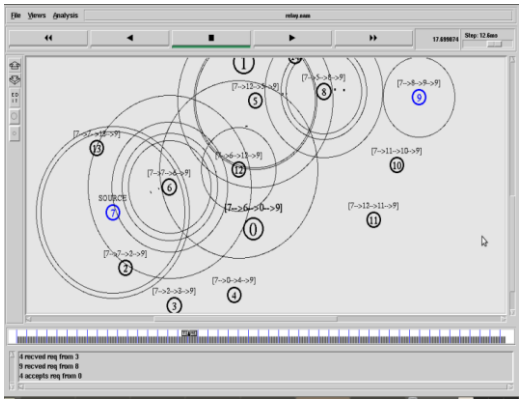
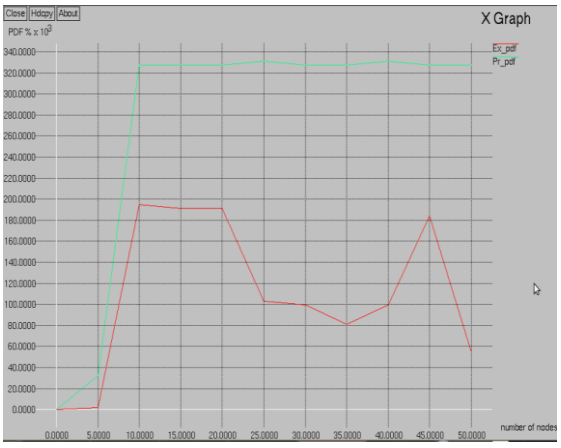
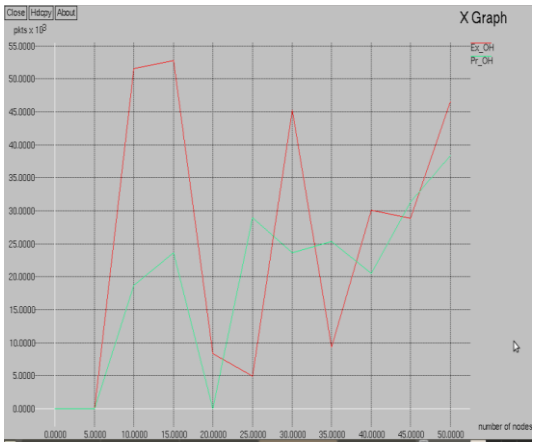


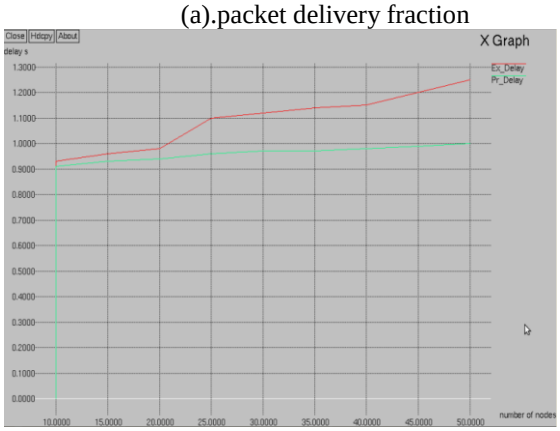
Fig 4.6 node chooses another path to reach destination



(a).packet delivery fraction



(b). packet overhead



(c). packet Delay

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

TABLE 1:- Simulation Scenarios

S.NO	PARAMETERS	VALUES
1.	Routing Overhead	39.0000 pkt
2.	Packet delivery fraction	330.0000 %
3.	Packet delay	1.0000 s

IV. CONCLUSION

Efficient node approach for reducing congestion by using Traffic aware routing protocol in IP networks then develop a probabilistically correlated failure (PCF) model to measure the impact of IP link failure on the dependability of backup paths. With this model, Propose a new traffic aware dynamic routing protocol called TAR to relieve congestion in MANET. With new improved TAR we have minimize delay and traffic and increase throughput while maintaining file sharing.TAR avoid congestion by detecting Hot Spot and reducing traffic. so make this work better we implement a technique of self knowledge, this method helps nodes and sink to find location of all the nodes in the network, which will make the node to find traffic areas and transfer the file through high efficient nodes, which will improve system performance.

REFERENCES

Qiang Zheng, Guohong Cao, F.Thomas ,La Porta, and Ananthram "Cross-Layer Approach for Minimizing Routing Disruption in IP Networks" vol. 25, no. 7, july 2014.

S.Priyadharshini, V.Govindaraj, "Multiple Backup path approach for link failure in IP networks" in proc.IJERT, vol.3, no.11, nov 2014.

V.Govindaraj, "Design of Low Power Dual Edge Triggered Flip Flop Based On Signal Feed throughScheme" in proc.IJAREEIE,vol.3,no.11,nov 2014.

V.Govindaraj," Removal of moiré pattern noise in images using median and Gaussian noise" in proc.IJSETR,vol.2,no.2,feb 2013.

V.Govindaraj, "Survey of image denoising using different filters" in proc.IJSETR,vol.2,no,2, feb 2013.

Q.Zheng, G.Cao, T.L. Porta, and A. Swami, ''Optimal Recovery from Large-Scale Failures in IP Networks,'' in Proc. IEEE ICDCS, 2012, pp. 295-304.

S. Kini, S. Ramasubramanian, A. Kvalbein, and A.F. Hansen, ''Fast Recovery from Dual Link Failures in IP Networks,'' in Proc. IEEE INFOCOM, 2009, pp. 1368-1376.

E. Oki, N. Matsuura, K. Shiomoto, and N. Yamanaka, ''A Disjoint Path Selection Scheme with Shared Risk Link Groups in GMPLS Networks,'' IEEE Commun. Lett., vol. 6, no. 9, pp. 406-408, Sept. 2002.

Q. Zheng, J. Zhao, and G. Cao, ''A cross-Layer Approach for IP Network Protection,'' in Proc. IEEE/IFIP DSN, 2012, pp. 1-12.

A. Kvalbein, A.F. Hansen, T. Cicic, S. Gjessing, and O. Lysne, ''Fast IP Network Recovery Using Multiple Routing Configurations,'' in Proc. IEEE INFOCOM, 2006, pp. 1-11.

A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot, ''Characterization of Failures in an Operational IP Backbone Network,'' IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 749-762, Aug. 2008.

[12]H.-W. Lee and E. Modiano, ''Diverse Routing in Networks with Probabilistic Failures,'' in Proc. IEEE INFOCOM, 2009, pp. 1035-1043.