Ms.Ashwina .N. Patil , Prof. S.S. Kanade , Ms. S.S. Bhakare / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue4, July-August 2012, pp.1486-1489

Fast Recovery For Dual-Link Failure Through Backup Path

Ms.Ashwina .N. Patil[*] , Prof. S.S. Kanade[**] , Ms. S.S. Bhakare[***]

[*] Department of CSE, College of Engineering. Osmanabad
[**] Head of E&TC Dept, College of Engineering , Osmanabad
[***] Department of CSE, Sinhgad College of Engineering. Pune.

ABSTRACT

The nodes in Mobile Ad Hoc Network (MANET) are mobile resulting in dynamic topology with high rate of link breakage and network partitions leading to interruptions in the ongoing communication. Because of node mobility and power limitations, the network topology changes frequently. Link failures or path failure are common in such type of network. Therefore the networks employ path/link protection to achieve fast recovery from dual failures. While the first link failure can be protected using link protection, but if second link is failed then we have the problem of recover that path so the purpose of our system is that recovery from second failure. One of the strategies to recover from dual-link failures is to employ link protection for the two failed links independently, which requires that two links may not use each other in their backup paths if they may fail simultaneously. Such a strategy is referred to as backup link mutual exclusion (BLME). This paper develops a solution to the BLME problem by using two approaches by: 1) integer linear program; 2) developing a polynomial time heuristic based on minimum cost path routing.

Keywords-MANET, BLME, FDLP, FILP.

1.INTRODUCTION

A Mobile Adhoc Network (MANET) is a network composed of mobile nodes mainly characterized by the absence of centralized coordination or fixed infrastructure, which makes any node in the network act as potential router. MANETs are also characterized by a dynamic, random and rapidly changing topology. In MANETs, communication link between mobile nodes always require over multi-hop paths. Since no infrastructure exists and node may cause frequent link failure.

In WDM network, the failure of a single fiber link may lead to tremendous data loss since a single fiber link can carry a huge amount of data (on the order of terabits per second).Therefore, network survivability is an important problem in network design and its real-time operation. In order to reduce the data loss, various protection and restoration mechanisms have been proposed and studied in the literature to recover traffic after a failure occurs and before the failure is physically repaired [1], [2], [3], [4], [5]. Although the WDM network and wireless ad-hoc settings are quite different in nature, they share a number of problems and challenges. One of them is failures of network components. If a link failure is detected on the primary path (through which actual data transmission is taking place), the source can switch to an alternate path instead of initiating a route discovery/recovery process. A new discovery takes place only when all precomputed paths break.

Since in a wireless ad-hoc network has no fixed infrastructure and there is no centralized control over the nodes ; no designated routers. So nodes serve as routers for each other, and data packets are forwarded from node to node in a multi-hop fashion. Protecting the circuits or connections established in such networks against single-link failures may be achieved in two ways: *path protection* or *link protection [6]*. Main focus of this paper is to protect end-to-end connections from dual-link failures using path protection and link protection.

2. TAXONOMY OF PROTECTION SCHEMES

Protection schemes proposed in the literature can be broadly classified as link protection and path protection.

2.1 **Link protection**

Link protection schemes route a connection around a failed link. Re-routing is performed by the node connected to the failed link to the neighboring node on the original path. Such a protection may be achieved in the network in a way that is transparent to the source node, except in cases where a link connected to the source or destination fails. Link protection, as shown in Fig. 1, reroutes all the connections on the failed link around it. When accepting a call request, the link protection scheme will reserve the network resource for the associated protection path. The protection path connects the two nodes adjacent to the failed link. When a link failure occurs, the node adjacent to and upstream of the failed link immediately redirects the traffic along the predetermined protection path to the node on the other end of the failed link to restores transmission.

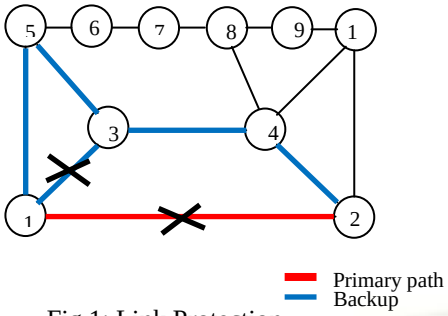

Fig 1: Link Protection

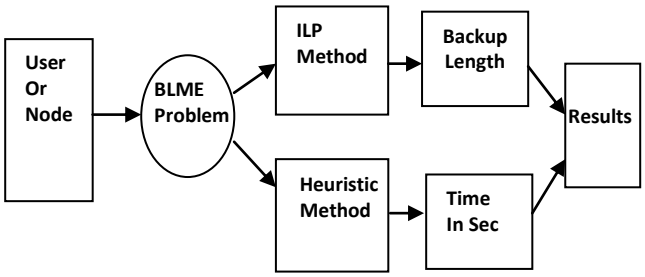

Fig 3 : System architecture

2.2 **Path protection**

Path protection schemes recover from a failure by re-routing the connections at the source. Path protection schemes may be classified into two categories based on their knowledge of the failure location. Assignment of a backup path that does not require precise knowledge of the link failure is referred to as *failure-independent path protection* (FIPP). Alternatively, if a connection may be assigned more than one backup path depending on the failure, then it is referred to as *failure-dependent path protection* (FDPP).Path protection, as illustrated in Fig. 2, reserves network resources for a single protection path in addition to the primary path. Since it is impossible to find which link on the primary path will fail, the system allocates a protection path, which is completely link-disjoint from the primary path. The primary path therefore shares no common link with its associated protection path. When a link fails, the source and destination nodes of a call on the failed link are informed of the failure, and the communication is switched to the protection path.

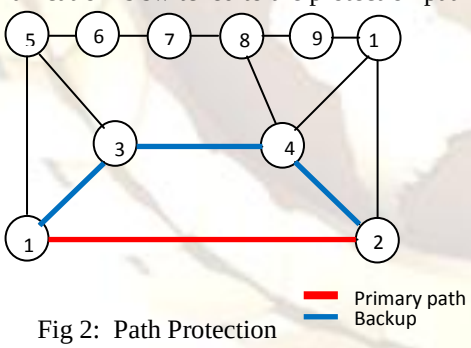

Fig 2: Path Protection

3.LINK FAILURE RECOVERY

Path protection schemes recover from a failure by re-routing the connections at the source. Path protection schemes may be classier into three categories based on their knowledge of the failure location. Assignment of a backup path that does not require precise knowledge of the link failure is referred to as failure independent path protection (FIPP). Alternatively, if a connection may be assigned more than one backup path depending on the failure, then it is referred to as failure-dependent path protection (FDPP). Link protection schemes route a connection around a failed link.

4. INTEGER LINEAR PROGRAMMING

Dual-link failure resiliency strategies are classified based on the nature in which the connections are recovered from first and second failures. The recovery from the first link failure is assumed to employ link protection strategy. Fig. 4 shows an example network where link 1-2 is protected by the backup path 1-3-4-2. The second protection strategy will refer to the manner in which the backup path of the first failed link is recovered.

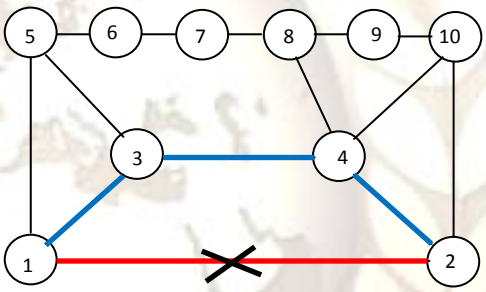

Fig 4: Back up link

4.1 **Failure Dependent Link Protection (FDLP)**

If the backup path is affected by the second failure, a backup path under dual-link failure is provided. This backup path is computed by eliminating the two failed links from the network and computing shortest path between the specific node pairs. Fig.4 shows the backup path assigned for link 1-2 under dual-link failures. It may be observed that the backup path assignment is different for different failures that affect the path. When a second link failure occurs, a failure notification must be sent to node 1, explicitly mentioning the failure location in the path 1-3-4-2. Every link is assigned one backup path for single link failure and multiple backup paths (depending on the number of links in the backup path for the single link failure) under dual-link failures. If the primary path and link 1-3 of backup path fails down , then this dual failed link is recovered by the path 1-5-3-4-2,similarly for link 3-4 and 4-5 fails, the recovery will be 1-5-6-7-8-4-2 and 1-3-4-10-2.

4.2 **Failure Independent Link Protection (FILP)**

One approach to dual-link failure resiliency using link protection is to compute two link-disjoint backup paths for every link. For any two adjacent

nodes, there exist two link-disjoint backup paths for the link connecting the two nodes. Let B_l and B'_l denote the two link-disjoint backups for link B_l. If any link in the backup path B_l fails, the backup path of will be reconfigured to B'_l. Hence, the nodes connected to link l must have the knowledge of the failure in its backup paths (not necessarily the location).If the link 1-2 fails, then under dual-link failure the backup path assigned by FILP will be 1-5-6-7-8-9-10-2. The backup path is identical under any second failure that affects the path 1-3-4-2. When the second failure occurs, a failure notification must be sent to nodes 1 and 2, although this notification need not explicitly mention which link failed in path 1-3-4-2.

5. HEURISTIC APPROACH

The heuristic solution is based on iterative computation of minimum cost routing. The network is treated as an undirected graph G. A set of auxiliary graphs corresponding to failure of a link $l \in G$ is created: $X_l = G(N, L-\{l\})$. In each auxiliary graph X_l the objective is to obtain a path between the nodes that were originally connected by link l . Let P_l denote the path selected in auxiliary graph X_l . If a link l' is a part of the path selected on graph X_l , then the path in graph X_l must avoid the use of link l .This is accomplished by imposing a cost on the links in the auxiliary graphs, and having the path selection approach select the minimum cost path. Let $W_{l\,l'}$ denote the cost of link l' on graph X_l such that it indicates that graph X_l contains link l and the two links l and l' may be unavailable simultaneously. Hence, the cost values are binary in nature. The cost of a path in an auxiliary graph is the sum of the cost of links in it. At any given instant during the computation, the total cost of all the paths (T) is the sum of the cost of the paths across all auxiliary graphs. It may be observed that the total cost must be an even number, as every link l' in a path P_l that has a cost of 1 implies that link l in path P_l would also have a cost of 1. For a given network, the minimum value of the total cost would then be two times the number of dual-link failure scenarios that would have the network disconnected. If τ denotes the number of dual-link failure scenarios that would disconnect the graph, then the termination condition for the heuristic is given by $T = 2^{\tau}$.

6. PERFORMANCE EVALUATION

6.1 Simulation setup

The setup of the simulation depicts an ad hoc network that consists of a varying number of Mobile Hosts (MHs) that move randomly in a square field free of obstacles. The setup is based on the OMNeT++ discrete simulator. The implementation of the proposed methods is based on the AODV routing protocol. We have fixed the area to a rectangular region of 350m x 350m. The transmission range of each node is fixed to 250 m. Nodes move around in the rectangular region according to the "random way-point" mobility model. All data packets are 512 bytes long. All traffic sessions are established at random times near the beginning of the simulation run and the sessions stay active until the end. Each simulation is run for 100 sec. We evaluate the performance by varying number of nodes for both the methods.

6.2 Performance Metrics

The performance of the ILP and heuristic algorithm developed in this paper are evaluated by using the given performance metrics .

- Packet delivery ratio (PDR):
- Path length
- Throughput

Packet delivery ratio is the ratio of the number of data packets received at the destinations and the number of data packets actually sent to the network. This measures the quality of the discovered path. The packet delivery ratio in IMCP and FDLP is shown in figure 5.As the number of nodes varies, the packet delivery ratio of both the methods increases. The packet delivery ratio of FDLP is higher than that of IMCP.

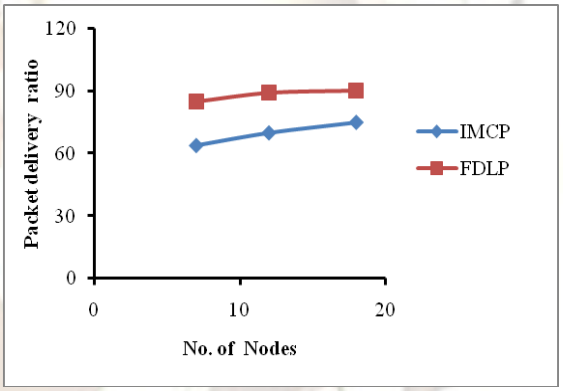

Fig 5 :Packet Delivery Ratio for IMCP and FDLP

The average hop length in IMCP and FDLP is shown in figure 6. The path length is calculated during the packet delivery. The alternative path may be longer than the main path.

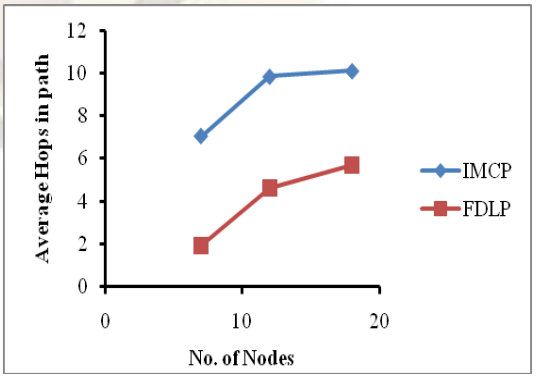

Fig 6 :Average hop length for IMCP and FDLP

Figure 7 shows the throughput comparison of IMCP and FDLP. The ratio of the total amount of data that

reaches a receiver from a sender to the time it takes for the receiver to get the last packet is referred to as throughput. It is expressed in bits per second or packets per second. Factors that affect throughput include frequent topology changes, unreliable communication, limited bandwidth and limited energy. Packet delivery capacity of the proposed method decreases as the network size increases. This is due to the route breaks as the number of size increases.

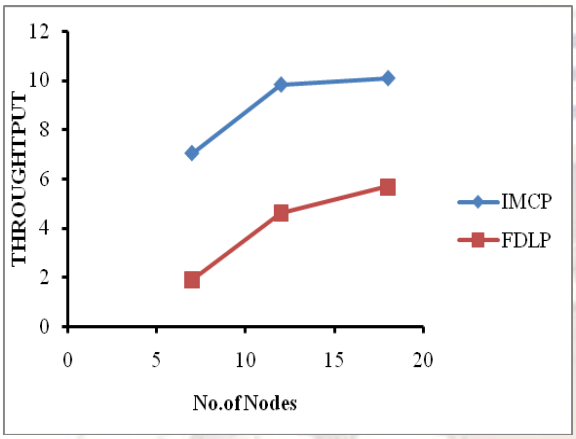

Fig 7: Variation of throughput with network size for IMCP and FDLP

7. CONCLUSION

This paper focuses on the approaches for providing dual-link failure resiliency. Recovery from a dual-link failure using an extension constraint, referred to as BLME constraint, whose satisfiability allows the network to recover from dual-link failures. In this paper, we motivated the need for considering double-link failures and presented some approaches for handling such failures. So here, we have proposed two schemes to solve BLME problem . The proposed scheme shows significant improvements in terms of packet delivery ratio, average hop length and throughput.

REFERENCES

[1] B. Mukherjee, "WDM optical networks: progress and challenges," IEEE J. Select. Areas Commun., vol. 18, pp. 1810–1824, (Oct. 2000).

[2] O. Gerstel and R. Ramaswami, "Optical layer survivability: a services perspective," IEEE Commun. Mag., vol. 38, pp. 104–113, (March 2000).

[3] G. Mohan, C. S. R. Murthy, and A. K. Somani, "Efficient algorithms for routing dependable connections in WDM optical networks," IEEE/ACM Trans. Networking, vol. 9, pp. 553–566, (Oct. 2001)

[4] M. Clouqueur and W. D. Grover, "Availability analysis of spanrestorable mesh networks," *IEEE J. Select. Areas* Commun., vol. 20,no. 4, pp. 810–821, (May 2002).

[5] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM mesh networks," *IEEE/OSA J.* Lightwave Technology, vol. 21,no. 4, pp. 870–883, (Apr. 2003).

[6] A. Chandak and S. Ramasubramanian, "Dual-link failure resiliency through backup link mutual exclusion," in Proc. IEEE Int. Conf. Broadband Networks, Boston, MA, (Oct. 2005), pp. 258–267.

[7] R. Ramamurthy, A. Akyamac, J.-F. Labourdette, and S. Chaudhuri, "Preemptive reprovisioning in mesh optical networks," in *Proc. OFC'(2003)*, pp. 785–787.

[8] H. Choi, S. Subramaniam, and H.-A. Choi, "On double-link failure recovery in WDM optical networks," in Proc. IEEE INFOCOM'(2002),vol. 2, pp. 808–816.

[9] S. Kim and S. Lumetta, "Evaluation of protection reconfiguration for multiple failures inWDM mesh networks," in Proc. OFC'(2003), pp. 210–211.

[10] D. Schupke and R. Prinz, "Performance of path protection and rerouting for WDM networks subject to dual failures," in Proc. OFC'(2003),pp. 209–210. [10] S. S. Lumetta

[11] Perkins C E., "Ad Hoc Network", Switzerland: Addsion-Wesley, (2000).

[12] S.J. Lee, E. Royer and C.E. Perkins, "Scalability study of the ad hoc on-demand distance vector routing protocol", International Journal of Network Management, Vol.13, (2003), pp. 97–114.

[13] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations", RFC. 2501, (1999).

[14] D.B Johnson, D.A Maltz and Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", In Ad Hoc Networking, edited by Charles E. Perkins, Chapter 5, pp. 132–172, Addison-Wesley, (2001).

[15] C.E. Perkins and E.M. Royer, "Ad-Hoc On Demand Distance Vector Routing," Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications *(WMCSA)*, New Orleans, LA, (February 1999), pp. 90-100