RESEARCH ARTICLE OPEN ACCESS

IP Failure Handling Using Localized On-Demand Link State Routing

Prof. S.M.Sangve, Sushil Warkar, Amit Shirke,
Kunal Solanke, Pratap Patil,
Department of Computer Science and Engineering,
ZES's Dnyanganga College of Engineering and Research
Pune- 411041
Maharashtra- India

ABSTRACT
IP network is mostly associated with a number of failures and these failures can make our system degraded i.e. makes our system weaker and the packet forwarding becomes a crucial issue at such times. Now here we use an implementation of different algorithm in such a way that we can minimize the chances of failure within such a network and thus making it convenient and reliable. The system is made enough powerful to handle these failures within a network at their own level. We have suggested a powerful schema which enables our system to overcome its initial drawback and making it flexible. We hereby offer a corresponding system working on Greedy Forwarding and Blacklist Based Algorithm. We have integrated our system along with the LOLs i.e. localized on demand link state routing for greater efficiency. The main aim of our system is to handle failures by using both the algorithms simultaneously i.e. on one hand check for the blacklist based algorithm and on the other hand check for the greedy forwarding algorithm. The Greedy forwarding includes weight based distribution of the packets. On the other hand blacklist checks the blacklist table which maintains record of degraded links within network. Now here we have a powerful mechanism to re-route [6] the packet although the network goes into the state of failure.

Keywords: - Packet Forwarding, Greedy Forwarding, Blacklist Based Forwarding, Rerouting.

I. INTRODUCTION

We now a day's use of internet on large scale but during such a usage we frequently observer failure during our access. Sometimes it may be network not found or many a times it may be time expired or may be network not responding. These all are common problem and which generally occur due to IP Failure. Our mechanism is to minimize such a conditions which occur into the network .We have made source to destination packet forwarding easy and reliable by using greedy forwarding and blacklist based algorithm. We have integrated our system along with the LOLs [1] i.e. localize on demand link state routing to achieve maximum efficiency into our system. There are many ways to handle failure in IP Network but we have chosen the efficient and convenient method of handling these commonly occurring failures.

Greedy Forwarding forwards the packets and Blacklist maintains a blacklist table during the transfer of the packets from the source to the destination. We also have used a mechanism of current topology and advertised topology to ensure the packet forwarding. We also check and ensure the packet forwarding by rerouting during case of link or node failure. These mechanisms are strong enough to handle the failure within the IP Network.

II. GREEDY BASED FORWARDING ALGORITHM

We have used Greedy forwarding algorithm [2] which makes us to detect the failure into a node it checks for sink node and sensor node. The sink node which is more convenient and reliable is being used and the data is sent to the sensor node thus both of them work into progression and by this they show efficient and convenient data

transfer the sink node check out for next sink node and by using sensor node transfer and manipulate the link or the node failure.

The greedy checks for all the connected nodes and transfer the packet to each and every node then the most efficient path is being elected which can forward the data into the packet and thus render a good throughput at every condition of packet forwarding and data transfer. The purpose to send it to other sensor node and thus it can be used to recover from the failure which may occur into an IP network due to noisy channel or other network problem it uses wireless transmission scheme for such a purpose. So here greedy forwarding checks for weight at each node or link and accordingly check for its appropriate minimal set of path for forwarding packet. Here in that case we have used bandwidth as a part of the weight into our system and thus we only check out for the bandwidth and its weight at this condition of greedy forwarding algorithm.

BLACKLIST BASED ALGORITHM

The blacklist based algorithm is made with an effort to forward the packets based onto their efficient path in such a way that each path is reliable and convenient to transfer data in an network [2].We find the most efficient path with the help of the routing table and render that we transfer the data from one node to the another node in an efficient and reliable way.

By using the Blacklist Aided Forwarding [3] we can check out for the link which has maximum chances of failure and avoid transfer of the packet using such a link. Thus minimize the chances of node or the link failure by using Blacklist forwarding algorithm. The blacklisted link is avoided and the probability of the link failure is obtained in this algorithm and thus we can find out whether the link is good enough to forward the packet at the given condition and thus we can ensure the node and link failure doesn't occur at those particular stages or the phases. Thus Blacklist Aided Forwarding along with Greedy Forwarding both together work parallel in order to make a complete detection and recovery of link failure and thus make our system more convenient and much more scalable as well as make it good and worthy enough for faster rerouting[5][8] in order to avoid time constraint. The time required to reroute and recover the link is reduced a result of use of the Blacklist Aided Forwarding and Greedy Forwarding Algorithm and hence we can say it leads to achievement in faster rerouting and easy packet forwarding in case of link failure.

ADVERTISED TOPOLOGY

The advertised topology is the proposed topology. These suggest the possible network formation during packet forwarding and also ensure how the packet can reach from source to destination along various paths. The current topology uses the advertised topology during it formation.

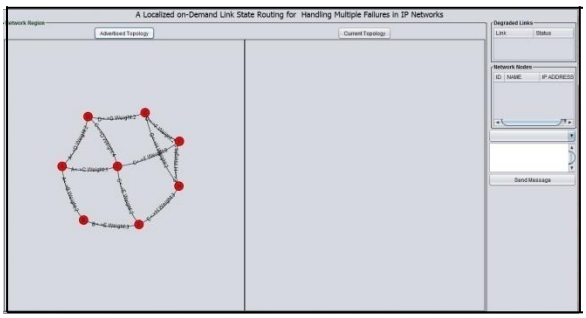

Fig. Advertised Topology

CURRENT TOPOLOGY

The current topology is the working topology into our system, it shows the various degraded links. These link are not functional and are shown dotted and we also have the current topology showing a clear description about the various network formation during the current working.

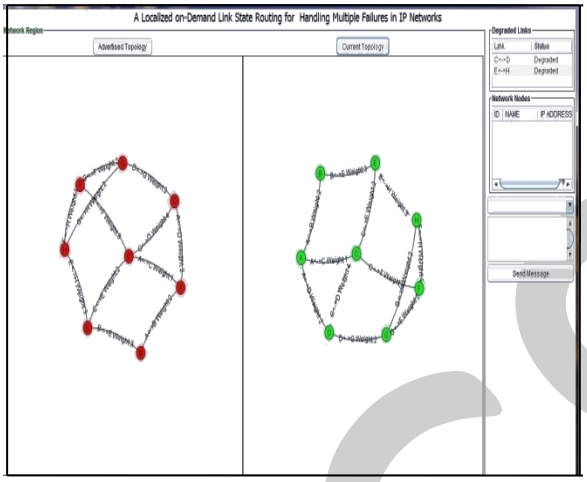

Fig. Current Topology

Geographic Position based Routing

It is same as greedy mode. When the *dead-end* is occur i.e., when the destination is closer to forwarding node than adjacent nodes, then the forwarding is changed to *face* mode. The packet is again switched to greedy mode when it reaches to the destination.

LOCALIZED LINK STATE UPDATES

The limited dissemination dependent schemes have been proposed to make link state routing more scalable for mobile ad-hoc networks. Fisheye state routing [10] (FSR) schemes upgrades the given nearby nodes at a larger frequency than the remote nodes which lie outside a certain scope. Localized On demand Link State [13] can be considered a form of limited dissemination based routing scheme that check out for loop-free forwarding while giving an notification only a small subset of nodes in the chance of a failure.

III. WIRELESS NETWORK IMPLEMENTATION

Our system can also be implemented onto the wireless network. We accept the IP address and then we find out within a wireless network [11] which node is not functional. The degraded link are find out and by this way we can know about which node is not efficient to pass packet from source to destination. We assign a host node and all other nodes are linked with the host node to check this we fire a Net View command on host node and find out which nodes are connected to host node. This is a simple way and this is also represented on our system display which nodes are functional in network.

In this Wi-Fi network node to be connected and identified the IP addresses are given to each and every node in network [12].

IV. SYSTEM IMPLEMENTATION

We have node to node transfer of the packet from the host to the next hop and this transmission is fast and reliable due to multiple rerouting [4, 6] during packet forwarding.

The degraded nodes are found out and then we choose another path to transmit the packet from host node to the destination or required node. From that node if our next hop is found we pass the message to that hop else we show a message that "**no next hop found**" as shown in figure below. This show the path in which forwarding is done from source to the destination.

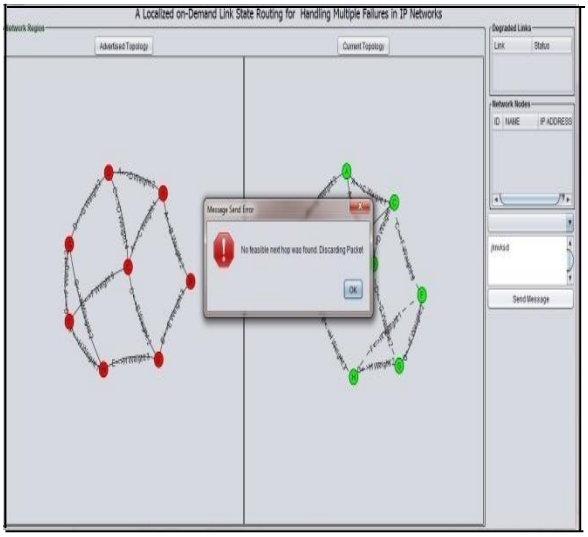

Fig. System Implementation

Tables are maintained for degraded links and for total number of nodes in network. And message box is taken as packet to be forwarded.

Packet is forwarded using greedy method that it finds out all the efficient paths with less cost from source to destination through all the possible ways or adjacent nodes to choose the next hop. This method is repeated until we get a destination node. There are so many methods of packet routing [9]. But we have used the Localized on demand link state routing which is efficient than other methods.

V. CONCLUSION

We have checked efficiency of both the algorithms and it is observed that blacklist based algorithm is much stronger in the comparison to the greedy forwarding algorithm because it does not allow the packet to drop but the blacklist algorithm show convenient path for packet forwarding from the source to the destination. If we see the scenario for the Greedy Based Forwarding Algorithm the packet loss is seen in such a condition. The packet which is sent from source gets drop till it reaches the destination thus there is loss of packet and loss of data at each level.

The degraded nodes are found out and then we choose another path to transmit the packet from host node to the destination or required node. Packet is forwarded using greedy method that it finds out all the efficient paths with less cost from source to destination through all the possible ways or adjacent nodes to choose the next hop. So we can conclude that Blacklist based algorithm is good as compared to that of Greedy Forwarding and hence we integrate both of them to improve our system efficiency.

REFERENCES

[1] A. Gonzalez and B. Helvik, "Analysis of failures characteristics in the uninett IP backbone network," in *Proc. 2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications*, pp. 198–203.

[2] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proc. 2000 ACM Mobicom*, pp. 243–254. Available: citeseer.ist.psu.edu/karp00gpsr.html

[3] S. N. et al, "Blacklist-aided forwarding in static multihop wireless networks," in *2005 SECON*.

[4] G. Robertson, J. Bedenbaugh, and S. Nelakuditi, "Fast convergence with fast reroute in IP networks," in *2010 IEEE HPSR*.

[5] S. Bryant, M. Shand, and S. Previdi, "IP fast reroute using not-via addresses," Internet Draft (work in progress), July 2007,

draft-ietf-rtgwgipfrr- notvia-addresses-01.txt.

[6] A. Li, X. Yang, and D. Wetherall, "SafeGuard: safe forwarding during routing changes," in *2009 CoNEXT*.

[7] M. Gerla, X. Hong, and G. Pei, "Fisheye state routing protocol for ad hoc networks," IETF Internet Draft, June 2002, draft-ietf-manet-fsr-03.txt.

[8] M. Shand and S. Bryant, "IP fast reroute framework," RFC 5714, January 2010.

[9] S. Nelakuditi et al., "Failure insensitive routing for ensuring service availability," in IWQoS'03 Lecture Notes in Computer Science 2707,Jun. 2003.

[10] M. Gerla, X. Hong, and G. Pei, "Fisheye state routing protocol for ad hoc networks," IETF Internet Draft, June 2002, draft-ietf-manet-fsr-03.txt.

[11] H. A. B. F. Oliveira, A. Boukerche, E. F. Nakamura, and A. A. Loureiro, "Localization in time and space for wireless sensor networks: An efficient and lightweight algorithm." *Performance Evaluation*, vol. 66, no. 3-5, pp. 209–222, 2009.

[12] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," vol. 43, no. 4. New York, NY, USA: Elsevier North-Holland, Inc., 2003, pp. 499–518.

[13] C. Santivanez, R. Ramanathan, and I. Stavrakakis, "Making link-state routing scale for ad hoc networks," in *Proc. 2001 ACM MobiHOC*.