International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 02 | Feb 2019 www.irjet.net p-ISSN: 2395-0072

IMPROVE REROUTING SCHEME TO MULTILINK FAILURE USING INTERFACE SPECIFIC ROUTING

A. MICHAEL[1], K. KALAI SELVI[2]

[1]PG Scholar, Dept. of Communication Systems, Govt. College of Engineering, Tirunelveli.
[2]Assistant Professor, Dept. of Electronics and Communication Engineering, Govt. College of Engineering, Tirunelveli

---

Abstract - *Link failures occur almost everyday in the internet. Due to both planned maintenance and unplanned events Such as cable cuts, optical layer faults, and other hardware/ Software bugs. Routing in the case of failures has became a hot topic in both academia and industry during the past Decade. Advanced fast rerouting approaches are developed to protect the routing against link failures. Instead of waiting for the routing protocol to converge, a fast rerouting approach can switch traffic to backup next hops or backup paths quickly. The existing system used a label based approach for multi link failure. This approach uses information that are carried by IP packets after failures occur. This means that modification to data packets are needed, such that extra information (labels) can be carried to indicate the existence of failures. However, fast rerouting faces the problem of efficiency, which has not been well addressed and the overhead is high, and topology constraints need to be met for the approaches to achieve a complete protection. In this project interface specific routing based on tunneling on demand (TOD) approach is proposed. This approach covers most failures with ISR and activates tunneling only when failures cannot be detoured around by ISR. In addition to this elliptic curve based diffie helman key exchange algorithm used to protect the data.*

Key Words: Multi-link failure, Fast rerouting, ISR, TOD, Diffie helman key.

1. INTRODUCTION

A wireless network is a computer network that uses wireless data connections between network nodes. Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building or as a connection between various equipment locations. Wireless telecommunication networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure. Examples of wirless networks include cell phonenetworks, wirelesslocalareanetworks (WLANs), wireless sensor networks, satellite communication networks, and terrestrial microwave networks. A wireless sensor network (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to monitor physical or environmental conditions. A WSN system incorporates a gateway that provides wireless connectivity back to the wired world and distributed nodes. The wireless protocols you select depends on your application requirements. Some of the available standards include 2.4GHz radios based on either IEEE802.15.4 or IEEE 802.11(Wi-Fi) standards or proprietary radios, which are usually 900MHz.

1.1 Wireless Link

Computers are very often connected to networks using wireless links, e.g. WLANs. Terrestrial microwave- Terrestrial microwave communication uses EARTH Based transmitters and receivers resembling satellite dishes. terrestrial microwave is in the low gigahertz range, which limits all communications to line-of-sight. Relay stations are spaced approximately 48km(30mi)apart.satelitescommunicate via microwave radio waves, which are not deflected by the Earth's atmosphere. The satellites are stationed in space, typically in geosynchronous orbit 35,400 km (22,000 ml) above the equator. These Earth—orbiting systems are capable of receiving and relaying voice, data, and tv signals. cellular and pcs systems use several radio communications technologies-wireless local area networks use a high-frequency radio technology similar to digital cellular and a low -frequency radio technology. wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area.

1.2 Wireless LAN

A wireless local area network (WLAN)links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for internet cassette use of spread-spectrum or OFDM technologies may allow users to move around within a local coverage area, and still remain connected to the network. WLAN standards are marketed under the wifi brand name. Fixed wireless technology implements point-to-point links between computers or networks at two locations, often using dedicated microwave or modulated laser light beams over line of sight paths.it is often used in cities to connect networks in two or more buildings without installing a wired link.

1.3 Wireless Ad hoc Network

A Wireless ad hoc network, also known as a wireless mesh network or mobile ad hoc network (MANET), is

awireless network made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes and each node performs routing. Ad hoc networks can "self-heal", automatically re-routing around a node that has lost power. Various network layer protocols are needed to realize ad hoc mobile networks, such as distance sequenced distance vector routing, Associativity-Based Routing, Adhoc on-demand Distance vector routing ,and Dynamic source routing.

1.4 Wireless MAN

Wireless metropolitan area networks are a type of wireless network that connects several wireless LANsWiMAX is a type of wireless MAN and is described by the IEEE 802.16 standard.

1.5 Wireless WAN

Wireless wide area networks are wireless networks that typically cover large areas, such as neighbouring towns and cities ,or city and suburb. These networks can be used to connect branch offices of business or as a public INTERNET access system. The wireless connections between access points are usually point to point microwave links using parabolic dishes on the 2.4GHz band, rather than omnidirectional antennas used with smaller networks.

1.6 Tunneling

In tunneling, the data are broken into smaller pieces called packets as they move along the tunnel for transport. As the packets move through the tunnel, they are encrypted and another process called encapsulation occurs. The private network data and the protocol information that goes with it are encapsulated in public network transmission units for sending. The units look like public data, allowing them to be transmitted across the Internet. Encapsulation allows the packets to arrive at their proper destination. At the final destination, de-capsulation and decryption occur. Tunneling is a way for communication to be conducted over a private network but tunneled through a public network. This is particularly useful in a corporate setting and also offers security features such as encryption options.

2.PROPOSED SYSTEM

In this section, we present our model for ISR,which label-free Fast routing approach.as discussed above, to achieve efficient fast rerouting, we first need to find out whether a label-free approach is adequate to provide a complete protection.ISR can be seen as a general label-free approach, since ISR makes full use of available label-free information known in current stage. We model the ISR rules, and model a valid routing as a set of ISR paths. Then we study how ISR rules and ISR paths change when failures occur. We reveal the conditions of complete protection and routing loops, and finally, we show the ISR is inadequate to provide full protection against arbitrary multi link failures in any network.

2.1 ISR RULES

For a packet with a certain destination address, each router should forward the packet to a certain next hop based on the ingress interface. Such a behavior can be modeled as an ISR rule. Formally, for a destination node $d \_ V$, *ISR rule r* is modeled as triple (*vi, vj, vk*), which means that, on receiving a packet destined to node *d* from link (*vi, vj*) $\_ E$, node *vj* will forward the packet along link (*vj, vk*) $\_ E$. We call link (*vi, vj*) the *ingress link* of ISR rule *r*, denoted by *lin*(*r*), and link (*vj, vk*) the *egress link* of *r*, denoted by *lout*(*r*).

A routing for a certain destination node *d* consists of all related ISR rules. Thus, we can model a routing by a set of ISR rules. However, not each ISR rule set is corresponding to a routing. We have:

Definition 1: ISR rules *r*1 and *r*2 are *conflicting* if *r*1 = (*vi, vj, vk*1), *r*2 = (*vi, vj, vk*2), and *vk*1 not equal *vk*2.
Definition 2: ISR rule set *Rd* is a *routing* if and only if 1) for each link (*vi, vj*) $\_ E$ and *vj* $\_ = d$, there is some ISR rule *r* $\_ Rd$ such that *lin*(*r*) = (*vi, vj*); and 2) for any *r*1 and *r*2 in *Rd*, *r*1 and *r*2 are not conflicting.

We focus on a specific destination node *d* when we discuss an ISR, because the routings to different destinations do not disturb each other. Definition 2 means that 1) each link (except the one whose end node is *d*) is an ingress link of some ISR rule, which implies that there must be a next hop for the ingress link; and 2) the ISR rules are not conflicting, which implies that an ingress link has only one next hop. Note that we did not model the situation that a packet is originated by a node, i.e., there is no ingress link. Such a packet can choose any available next hop, e.g., the next hop belonging to the shortest path.

2.2. ISR PATHS

Definition 2 does not require that destination node d is reachable. We propose ISR paths to model a valid routing. For two ISR rules r1 and r2, if the ingress link of r1 equals the egress link of r2, then a packet that is forwarded by applying r2 will next be forwarded by applying r1. As such, a sequence of ISR rules forms a path, along which a packet will be forwarded.

For example, in Fig. 3(a), the destination node is 5 and there are four ISR paths. (5, 4, 2, 1, 3, 5) is an ISR path, standing for four ISR rules (5, 4, 2), (4, 2, 1), (2, 1, 3), and (1, 3, 5). In some cases, ISR rules may form a loop. However, the loop is not an ISR path, because the destination node cannot be reached by the loop. However, the destination node may still be reachable through other ISR paths, even if there is a routing loop. We define valid routings.

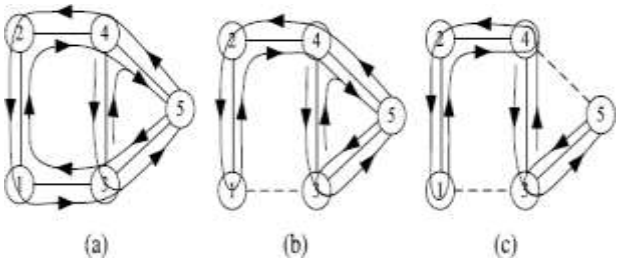

FIG 1:Example Of ISR PATHS, Node 5 is the destination. (a) w/o failures.(b) link (1; 3) failed. (c) link (4; 5) failed.

2.3.Adjusting Routing For Link Protection

A packet is forwarded to a backup next hop when the premier one fails. There can be different strategies to select the backup next hop,i.e.,the backup egress link. When there are multiple candidates. We propose the reverse rule forwarding (RRF)strategy. We choose RRF because any other strategy can be reduced to RRF in certain situations. After that will show how ISR paths change when a link fails. With RRF,a packet whose egress link is failed will be forwarded as if it is received from the reverse link of that egrees link.formally,assume a packet is received by node vi from node vh,and there is ISR rule (vh,vi,vj).if think (vi,vj)is failed,we will find ISR rule (vj,vi,vk) to deal with the packet.as such, the two ISR rules(vh,vi,vj)and (vj,vi,vk)are combined to a new ISR rule,i.e.,(vh,vi,vk).

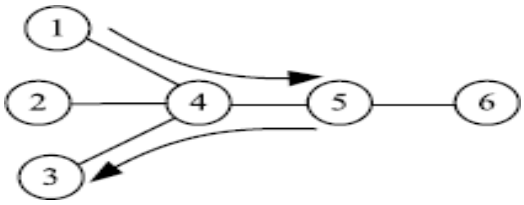

Fig -2: **An example of ingress &egress link selection strategy.**

Which shows a part of a network and node 5has degree 2. When link (5, 6) fails, node 5 has only one nexthop to use, i.e. node 4. And then, node 4 will forward a packet to node 3 according to ISR rule (5, 4, 3). Because node 4 is not aware of the failure, any egress link selection strategy in node 4 will not be triggered, so node 1 or node 2 will not be selected as the next hop.

2.4. Protection Effectiveness Limit of ISR

Now we show the limit of ISR-based protection. The result is negative: there exist some networks in which no ISR can be constructed to protect the routing against all *k*-link failures (*k* _ 2). Formally, we have the following theorem. *Theorem 1:* There exists network *G* such that, for any ISR *Rd* for *G*, at least one of the following holds: 1) *Rd* is not a valid routing; or 2) there exist at least one multi-link failure under which the resulting network is connected but the resulting routing is not a valid routing.

Proof: We prove the theorem by showing one such network that meets the conditions. The network topology is shown in Fig. 5(a), where node 1 is the destination node. We consider all possible cases when two links in set *{*(6, 7), (8, 9), (10, 11), (12, 13), (14, 15), (16, 17), (18, 19)*}* are failed simultaneously. Note that only the failure of links (6, 7) and (8, 9) will make the network unconnected. First, for all nodes except node 1, the ingress link of an ISR rule cannot be the egress link, or else a routing loop will be Second, the node degree of nodes 2 to 5 is 3. For each of these nodes, if there is an ISR rule (*vi, vj, vk*), then (*vk, vj, vi*) cannot be used, or else a routing loop will be induced when link failure occurs, according to Theorem 9. Thus, there exist only two possible cases of ISR rules in a node with degree 3, as shown in Fig. 5(b). Since there are 4 nodes with degree 3 in our network, there are only 24 = 16 possible ISRs in total. We can then check the routing validness one by one, and check the potential routing loops under failures following For instance, one possible ISR is shown in Fig. 5(c). We can see that there are two routing loops, and destination node 1 cannot be reached from nodes 18 and 19, so the ISR is not a valid routing. By checking all 16 possible ISRs, we find that either the ISR is not a valid routing; or there exist at least one multilink failure (except the failure of links (6, 7) and (8, 9)) that cannot be protected. This ends our proof.

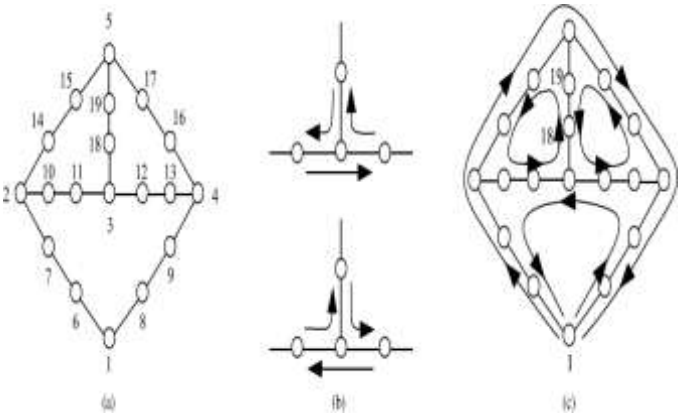

Fig. 3: Network used in the proof of Theorem1.(a) The network topology. (b) Two possible ISR-rule cases for a node with degree 3 in the network. (c) One of all possible ISRs where node 1 is the destination.

2.5 TUNNELING ON DEMAND APPROACH

We discuss the considering two broad categories of fast rerouting separately, namely *label-free approaches* and *label-based approaches*. Label-free approaches use information that can be obtained within tradition IP packet forwarding to select a backup next hop. Such information include destination address, local failures, next hop and backup next hops computed in advance [3], and the interface from which a packet arrives [4]. The overhead of label-free approaches is

little because packets are not required to be labeled, but the protection performance is in turn limited. For instance, the Loop-Free Alternates approach can protect the routing against any single-link failure only if the network topology meets certain conditions [5]. For multi-link failures, we have not seen any label-free approach that can provide a complete protection even against dual-link failures. On the other hand, label-based approaches use information that are carried by IP packets after failures occur. This means that modification to data packets are needed, such that extra information (labels) can be carried to indicate the existence of failures. The labels can have different forms such as special flags [2] or extra (tunneling) headers [6], [7], but they all introduce extra processing overhead and delay the packet forwarding. Since label-free routing (ISR) cannot provide a full protection against multi-link failures for any network according to Theorem 1, it is natural to take a label-based approach, while minimizing the labeling overhead. The tunneling on demand (TOD) approach in this section. TOD uses ISR to protect the routing against most (or all if possible) multi-link failures, and uses tunneling only for the cases that cannot be covered, and our goal is to use as few tunnels as possible. To realize the idea, we first need a proper ISR that can cover most multi-link failures. If not all multi-link failures can be covered by the ISR, we need to find out which multi-link failures can induce routing loops, so we can establish protection tunnels for them.

2.6 ELLIPTIC CURVE DIFFIE HELLMAN KEY

The Elliptic Curve Diffie-Hellman (ECDH), is an anonymous key agreement protocol that allows two parties, each having elliptic-curve public-private key pair, that have no prior knowledge of each other to establish a shared secret key over an in-secure channel. This shared secret may be directly used as a key, it can then be used to encrypt subsequent communications using a symmetric-key ciper.[1] It is a variant of the Diffie-hellman protocol using elliptic-curve cryptography. In a shared secret is a piece of data, known only to the parties involved, in a secure communication. The shared secret can be a password, a passphrase, a big number or an array of randomly chosen bytes. In contrast to a secure channel, an insecure channel is unencrypted and may be subject to eavesdropping. Secure communications are possible over an insecure channel if the content to be communicated is encrypted prior to transmission. As such, it is used by several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSec). SSL (Security Sockets Layer) is the predeces-sor to TLS (Transport Layer Security) and they are both referred to as `SSL'. SSL is the standard security technology developed to establish an encrypted link between a web server and a browser. The link should ensure privacy and integrity of all data passed between the web server and the browser. Before a client and server can begin to exchange information protected by SSL they must exchange or agree upon an encryption key and a cipher to use when encrypting data. The key and chiper must both have high security. EllipticCurve Diffie-Hellman is one of the secure methods used for the key exchange.in this report, and we try to benefit from this scheme by use the key (which exchange it) as a secret key. (That is, we know now the one of the advantages of the Diffie–Hellman key exchange system) and we are using Elliptic curve cryptography for encryption, in the method, because the sender compute the exponentiation function between the coordinates of the key in the encryption algorithm (use fast exponentiation method), and the receiver compute the inverse of the exponentiation function between the coordinates of the key in the decryption algorithm.

3.REQUIREMENTS

Hardware

1.Processor :Intel P4500 Processor

2.Clock Speed :1.8 GHz

3.RAM :4 GB

4.Hard Disk :500 GB

5.CD Drive :52x Reader

6.Keyboard :101 Standard key-board

Software

1.Language :C++,TCL

2.operating system :Ubuntu 14.0

3.Tools :NS2.35

4.Network :Wireless

4. RESULT AND DISCUSSION

The results are obtained by performing various simulations in NS-2 software. Moreover some important parameters such as area, number of nodes, placements of nodes and mobility are discussed.

FIG 4: ECDH ENCRYPTION

THROUGHPUT: Throughput is the measure of how fast we can actually send packets through network. The number of packets delivered to the receiver provides the throughput of the network. The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time it takes for receiver to get the last packet. An important quality of communication networks is the throughput. It is defined as the total useful data received per unit of time. In this metric, the throughput of the protocol in terms of number of messages delivered per. It is defined as the total useful data received per unit of time. In this metric, the throughput of the protocol in terms of number of messages delivered per one second (Mbps) analyzed.

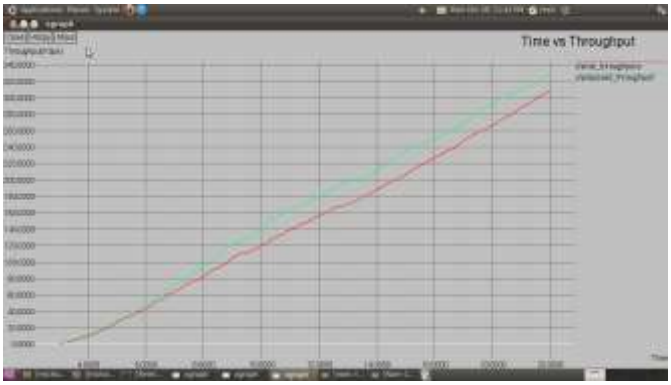

FIG 5: TIME Vs THROUGHPUT

DELAY: Delay indicates how long it took for a packet to travel from the source to the application layer of the destination. i.e. the total time taken by each packet to reach the destination. Average delay of data packets includes all possible delays caused by buffering during route discovery, queuing delay at the interface, retransmission delays at the MAC, propagation and transfer times.

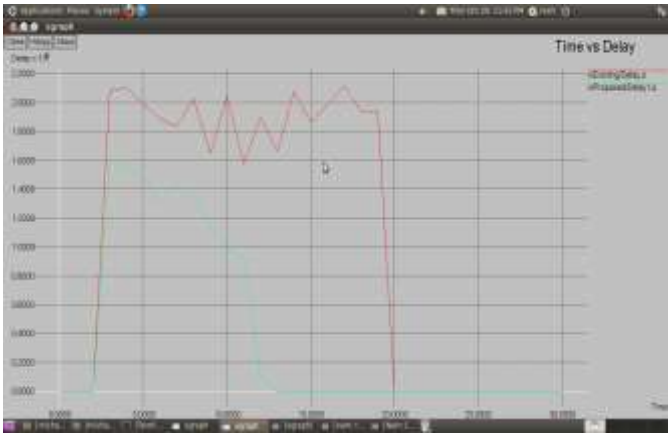

FIG 6: TIME Vs DELAY

PACKETLOSS: It is the number of data packets that are not successfully sent to the destination. When the number of nodes increases, the number of packets dropped also increases which means that number of packets not successfully reaching the destination is high.

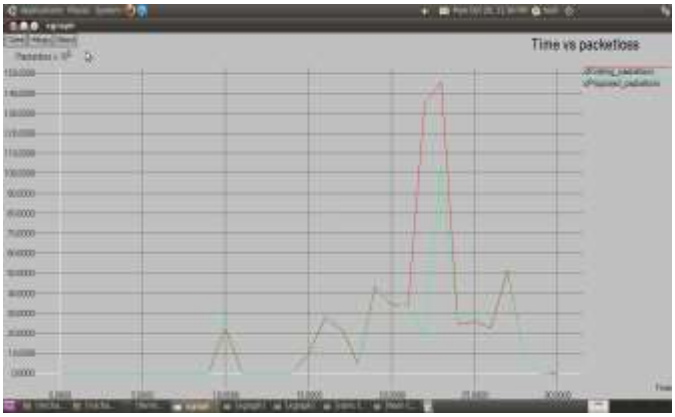

FIG 7: TIME Vs PACKETLOSS

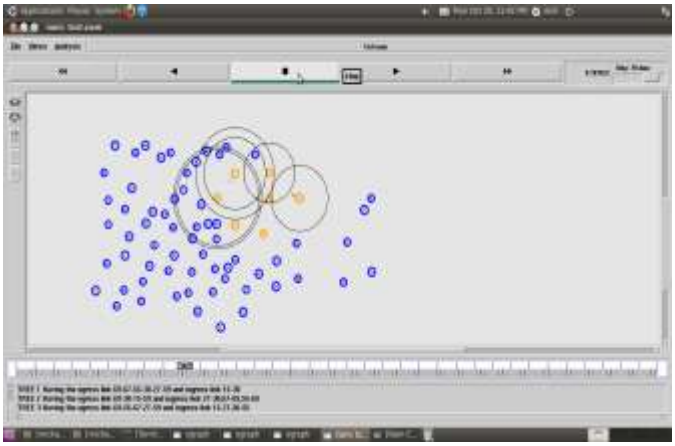

FIG 8: ISR PATH

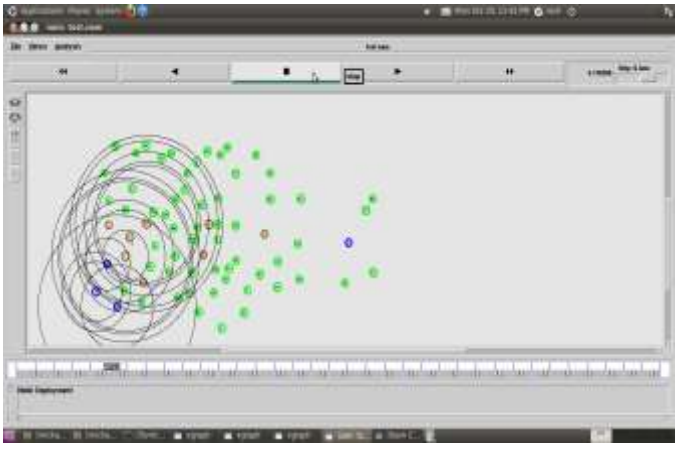

FIG 9: NEIGHBOUR INFORMATION TRANSMISSION

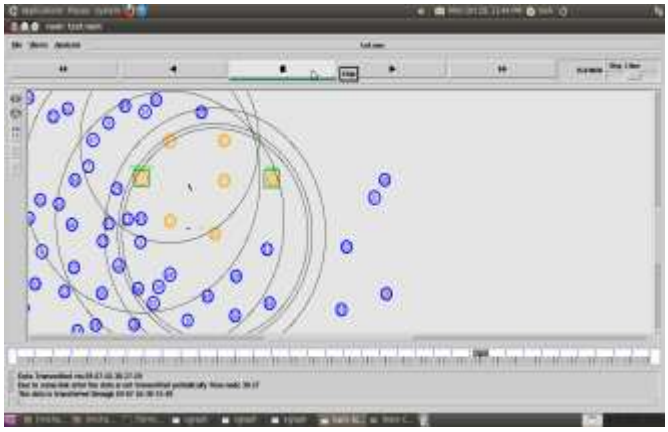

FIG 10: DATA TRANSMISSION USING ISR

5. CONCLUSION

We studied IP fast rerouting for multilink failures in networks without topology constraints. We proposed the ISR path model and found that a multi-link failure will induce routing loops when the ISR paths overlap in certain ways. We further proved that label-free approaches cannot provide a full protection against multi-link failures in some networks. Based on the findings, we proposed TOD, a light weight IP fast rerouting approach that uses tunneling only when needed. We developed algorithms for TOD, which can protect the routing against arbitrary single-link failure and dual-link failures. The results showed that TOD can achieve a higher protection ratio than the state-of-the-art label-based approaches with small tunneling overhead.

REFERENCES

[1]Yufang Huang, "Algorihtm for elliptic curve diffie-Hellman key exchange based on DNA title self assembly In Proceedings of 46th IEEE Theories and Applications,pp.31-36, 2008.

[2]K.Lakshminarayanan et al., "Achieving convergence-free routing using failure-carrying packets," in Proc. ACM SIGCOMM, 2007, pp. 241–252.

[3] A. Atlas and A. Zinin, Basic Specification for IP Fast Reroute:Loop-Free Alternates, document RFC5286, IETF, Fremont, CA, USA, Sep. 2008.

[4] S. Nelakuditi, S. Lee, Y. Yu, and Z.-L. Zhang, "Failure insensitive routing for ensuring service availability," in Proc. IWQoS, 2003, pp. 287–304.

[5] G. Rétvári, J. Tapolcai, G. Enyedi, and A. Császár, "IP fast ReRoute: Loop free alternates revisited," in Proc. IEEE INFOCOM, Apr. 2011, pp. 2948–2956.

[6] T. Elhourani, A. Gopalan, and S. Ramasubramanian, "IP fast rerouting for multi-link failures," in Proc. IEEE INFOCOM, Apr./May 2014,pp. 2148–2156.

[7] T. Elhourani, A. Gopalan, and S. Ramasubramanian, "IP fast rerouting for multi-link failures," IEEE/ACM Trans. Netw., vol. 24, no. 5, pp. 3014–3025, Oct. 2016

AUTHORS:

1) A.MICHAEL, PG Scholar, Department of Communication Systems, Government College of Engineering, Tirunelveli.

2) K.Kalai Selvi, Assistant Professor, Department of Electronics and Communication Engineering, Tirunelveli.