International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Encrypt the Routing Data for Providing Security in Cross Layer Method

Phoebe Gade
M.Tech Computer Science &Engineering,
E-mail: phoebe.gade@gmail.com
Pampati Nagaraju
Asst. Professor, Department of CSE, Talla Padmavathi College of Engineering, Warangal, Telangana, India.
E-mail: nagaraju.pampati@gmail.com

Abstract:
A single link cut in the network may leads to insignificant loss of data flow. Hence backup paths are the most used techniques in IP networks in order to safe guard IP link from failures. The existing system chooses multiple reliable backup paths to eliminate the problem of IP link failures and minimizing routing disruption only when IP link fails. This is done by maintaining all the routing information in a hash table. Probabilistically Correlation Failure (PCF) model with a layer mapping approach is used to quantify the IP link failure. DSDV protocol is used to detect the IP link failure in the network and to deploy the hash table to manage all the routing information for data exchange between nodes in a network. But the drawback of this process is that all the routing information stored in the hash table is not secure. Hence the multipath routing information can be easily modified by the adversary in network. Hence in the proposed system algorithm is deployed to encrypt the routing information before it is stored in the hash table. Hence only the authorized user can modify the multipath routing information in the hash table.

Index Terms: IP networks; Link failure; Backup path; Failure recovery; Cross-layer

1. INTRODUCTION

In network communication the communication takes place between sources to destination through the media. The communication can be wired or wireless. In the wired communication there are actual links between the nodes of the topology. The flow of data passes through that links until these are intact. If there is the breakage of single link from the topology the flow is interrupted and hence communication network. Due to this disruption of the IP network there is the loss of the data which is flowing currently through the link.

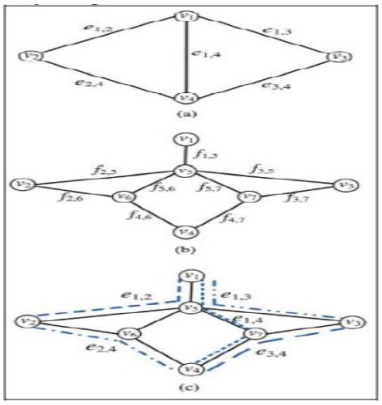

Fig. 1 Topology mapping of IP network (a) Logical Topology, (b) Physical Topology, (c) Mapping between the Logical and Physical Topology.

To avoid all these losses by the link failure we have to find the alternative way for the recommencing of the flow. The link can be repaired, but for high bandwidth links the speed of flow is so high that the loss of data is so large. For the real time application such losses are dangerous. There should be high reliability and the high availability. So, another alternative is to provide the backup path for each link by which the flow can be switched to that path. Currently in

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

the IP network the whole connections done as per the wavelength division multiplexing (WDM) layered structure. So there are logical links in the network which are connected directly to the communicating nodes which are in between source to destination. IP network having layered IP topology in which logical links are implanted on the physical links.

Logical links are nothing but the IP links and the physical links are nothing but the fiber links. As shown in Fig. 1(a) the nodes in the communication are mapped by the logical topology. It shows ei,j as a logical link between node vi and vj. While mapping the actual communication between the nodes physical topology is used as shown in Fig. 1(b). It shows fi,j as a fiber link between node vi and vj. In the physical mapping there can be addition of nodes to divide the long links into the light-paths. These additional nodes are nothing but the physical devices induced into the network. Link state routing is the method of routing in which each node of the network forms the map of its connectivity for communication with other nodes in the network. Every node calculates the best path for the destination from it in logical topology independently. All these best paths form the graph which is the combination of all best paths and forms the routing tables of each node.

2. RELATED WORK

As discussed above, in the recent world of internet it is become necessary that service should be with high availability, reliability and robustness. There is a large impact of unavailability off the network communication all the time due to failure of links. To achieve goal of recovering the flow of the network should be resumed as quickly as possible.

When there is the exposure of failure at some link the flow of data is instantaneously directed through the alternate output link. This technique is suitable for single link failure affairs for both link and nodes with the single mechanism instead of knowing the reason of failure. It is a connectionless technique and works on hop-by-hop forwarding. MRC forms network configuration for the backup with small set by using network mapping graph and links associated with it. By overall observations of simulations, MRC approaches performance of re-convergence of global OSPF.

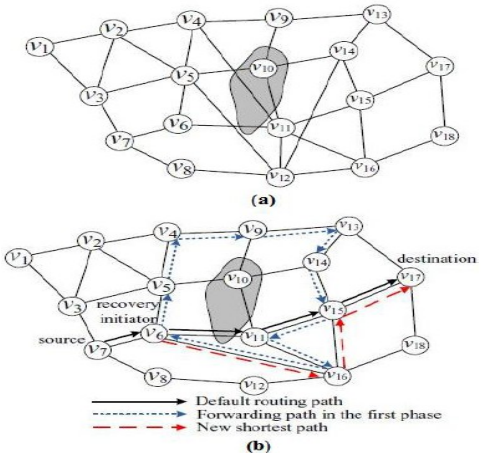

Fig. 2 a) Network with Failure(shaded region). b) Failure Handling with RTR

The technique name suggests two phases, quick recovery from failures and finding the shortest recovery paths. Initial stage contains the collection of failure details by forwarding the packets in failed network. Second stage contains the finding out shortest path for the destination from the current source and packets are forwarded through that path. Network of any mapping can be handled by this technique for the recovering and finding shortest path up to destination. Simulation of this technique on the ISP topology shows that about 98.6% of failure paths are recovered with shortest path in the recovered network. As compared to previous techniques, network resources used for the irrecoverable paths of failed network is very less along with the better performance for recovering failed network.

Most of the systems consider the selection of the backup path as a connectivity problem and ignore about the traffic load and the bandwidth capacity of the IP links for rerouting the traffic if any failure occurs. As a result, in some IP links the rerouted traffic may exceed its band width

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

capacity and hence overloaded traffic occurs in such links. So it is very important to choose a reliable backup path. To overcome all the cross mapping strategy for reducing the disruption due to IP link failure is used. It mainly focuses on the correlation between the IP links failures and provides multiple reliable backup paths for each IP link. To select a reliable backup path this system uses the Probabilistically Correlated Failure (PCF) model which is based on the topology mapping and the probability of failure of both fiber and logical links.

Normally back up path is used to protect IP network when the IP link is failed**.** Most of the backup path-based production method mainly aims at selecting the reliable backup paths to overcome the path obstruction due to IP link failure. Back up path based protection method is deployed by Internet service providers appreciably for fortifying their analogous domains. The independent model and Shared Risk Link Group (SRLG) model works on the principle of having a single backup path in their corresponding routers. But this system will create some delay if the existing backup path fails. Hence the existing system uses cross mapping strategy with multiple backup paths. This system selects multiple reliable backup paths for each IP link to safeguard and enhance the backup path-based protection method. If an IP link fails, then its corresponding backup path is selected immediately. The reliability of backup path should be calculated under the condition when the IP link fails. To achieve this, Probabilistically Correlated Failure (PCF) model is used in the existing system. When an IP link failure occurs, PCF immediately calculates the probability of failure for fiber link, IP link and backup path which results in identifying the reliable backup path.

3. IMPLEMENTATION

In high speed IP networks like the Internet backbone, disconnection of a link for several seconds can lead to millions of packets being dropped. Therefore, quickly recovering from IP link failures is important for enhancing Internet reliability and availability, and has received much attention in recent years. Also the stored information in the router for the above existing system is not secure and can be easily affected by the adversary attack. Hence in the cross mapping strategy security is enhanced to protect from adversary attack. An ISP network with both optical and IP layer topology is used to evaluate the proposed approach. This proposed scheme used CP–ABE algorithm to provide security for the stored information. This algorithm will encrypt the routing information in the hash table using public key encryption method and store the cipher text instead of the original plain text. Hence the unauthorized hacker or the adversary cannot be able to attack or alter the information. Only the authorized user with the corresponding public key can access those secured routing information.

Advantages:

1. Even if more number of IP link fails at a time, its multiple backup path topology will improve its reliability.
2. This multiple backup path will reduce the rerouted traffic load without exceeding its usable bandwidth for each link.
3. This system is more secure as the routing information is encrypted using CP–ABE algorithm.
4. The encryption can be done without exact knowledge of the receiver set.
5. Decryption is enabled if and only if the cipher text and secret key attribute sets overlap by at least a fixed threshold value.

4. MODULES DESCRIPTION

The four modules for multipath backup based protection are:

A. Node creation in network
B. Hash table compromise by adversary
C. Deploying CP-ABE algorithm
D. Detect the attack and prevent the routing information in hash table.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

A. Node creation in network

This module is secured completely so that only the authorized user can enter into the network. The users must register themselves before entering into the network and hence that person is considered as an authorized user. The network formed by number of nodes are connected and created. The participated nodes are having a separate login credential to ensure their authentication of network and exchange the data between them using the selected routing path. In this module the number of nodes connected into the network can also be identified and all the routing path information is managing by hash table.

B. Hash table compromise by adversary

This module is to configure the hash table. The hash table here is located in a centralized manner and contains all the routing information. It also contains the details about the status of the IP link. Each router in the network sends default packets to its neighbors. If the packet is received by the neighbor and acknowledges the router then there is no link failure and this path is updated in the hash table. If the packet is not received by the neighbor (Acknowledgement is not received by the router) then there is a link failure and this failure information is also updated in the hash table. But the routing information in the hash table is not secure and can be easily compromised by the adversary which can modify or attack the routing information.

C. Deploying CP-ABE algorithm

All the available backup paths are located in a centralized manner (stored in the hash table). The previous work only to avoid the IP link failure and minimize overhead of link and improve performance. But not focus on the security of the hash table. The multi path routing information in the hash table can be compromised by the adversary which can easily modify the hash table routing information. So this module protects the routing information by deploying Cipher Text Attribute Base Encryption (CP-ABE) algorithm on the hash table.

D. Detect the attack and prevent the routing information in hash table.

The Cipher Text Attribute Base Encryption (CP-ABE) is used to avoid the adversary attack of the hash table routing information. This encryption method uses the public key encryption method to convert the plaintext routing information into the corresponding cipher text. Hence the node with the correct public key only can access the encrypted information. After encryption the routing information is stored to the hash table as cipher text that prevents the routing information from the adversary attack in network.

5. CONCLUSION

Overlay networks over valuable services needed by end-systems and help overcome functionality limitations of the Internet. However, as shown in our thesis, they lead to complex cross-layer interaction with potentially detrimental effects. The existing layer mapping strategy will improve the reliability of backup paths by introduced a probabilistic correlated failure (PCF) model which protects the IP link failure by choosing multiple backup paths. Even if multiple logical paths fail simultaneously this scheme will reroute the traffic without any buffer overloading. But the routing information stored in the hash table is not secure and any unauthorized or adversary node can easily attack those information. Hence the packet drop and the delivery ratio may be higher or the packet may not reach the correct destination. The proposed scheme will provide security to the hash table routing information using CP-ABE algorithm. The algorithm reduces the delay and the packet delivery ratio to some extent.

6. REFERENCES

[1] V. Sharma and F. Hellstrand, Framework for MPLS-Based Recovery, RFC 3469, 2003.

[2] M. Shand and S. Bryant, IP Fast Reroute Framework, RFC5714, Jan. 2010.

[3]V. Sharma and F. Hellstrand (2003), 'Framework for MPLS-Based Recovery' RFC 3469.

[4]F. Giroire, A. Nucci, N. Taft and C. Diot (2003), 'Increasing the Robustness of IP Backbones in the Absence of Optical Level Protection' in Proc. IEEE INFOCOM, pp. 1-11.

[5] \Peer-to-Peer in 2005." Cachelogic White Paper, http://www.cachelogic.com/ home/pages/research/p2p2005.php.

[6] Calvert, K., Doar, M., and Zegura, E., \Modeling Internet Topology," IEEE Communications Magazine, June 1997.

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

[8] 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.

[9] A. Kvalbein, A. F. Hansen, T. Cicic, S. Gjessing,

[10]E. Modiano and A. Narula-Tam (2002), 'Survivable Lightpath Routing: A New Approach to the Design of WDM-Based Networks' IEEE J. Sel. Areas Commun., vol. 20, no. 4, pp. 800-809.

[11]A. Todimala and B. Ramamurthy (2007), 'A Scalable Approach for Survivable Virtual Topology Routing in Optical WDM Networks' IEEE J. Sel. Areas Commun., vol. 25, no. 6, pp. 63-69.

[12]K. Lee and E. Modiano (2009), 'Cross-Layer Survivability in WDM Based Networks' in Proc. IEEE INFOCOM, pp. 1017-1025.

[13]Qiang Zheng, Guohong Cao and A. Swami (2014), 'Cross-Layer Approach for Minimizing Routing Disruption in IP Networks' in Proc. IEEE PADS, vol. 25, no. 7, pp. 1659-1669.

[14]John Bethencourt, Amit Sahai and Brent Waters (2007), 'Ciphertext-Policy Attribute-Based Encryption' in Proc. IEEE/ACM SAP, pp. 321-334.

[10]Ling Cheung and Calvin Newport (2007), 'Provably Secure Ciphertext Policy ABE' IEEE/ACM CACS, pp. 456-465.