ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Enhancing the Security in Cross Layer Method which reduces the Link Failure in Networks using CP-ABE

D. Ramyaa[1], P. Sabarinathan[2]

P.G Student, Department of CSE, Pavendar Bharathidasan College of Engg and Tech, Trichy, Tamilnadu, India[1]

Assistant Professor, Department of CSE, Pavendar Bharathidasan College of Engg and Tech, Trichy, Tamilnadu, India [2]

ABSTRACT: The *n*etworking is the process of linking two or more computing devices together for sharing the data using a routing path. Link failures are common in such networks and the disconnection of link for several seconds creates major data loss. 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 path 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 the Cipher Text Attribute Base Encryption (CP-ABE) 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.

KEYWORDS: routing; link failure; probabilistic correlated failure; layer mapping; IP networks; CP-ABE.

I. INTRODUCTION

IP link failures are very common in internet which is due to several reasons. Millions of packets are dropped if such links are disconnected in a high speed network for several seconds [1]. Overcoming such failures for improving reliability and availability is very essential. In recent years Internet Service Providers (ISP) use backup path based protection [2, 3] for safeguarding their respective domains where the backup paths are precomputed, configured and stored in the routers. The time to identify the failure is less than 50 ms in this backup path based protection method and if any link failure is detected then the traffic is rerouted to its corresponding backup path. However selection of a backup path is complicated in this method. Most of the systems mainly aim on selecting a reliable backup path and the main drawback here is that, it does not explain about the correlation between the failure models which makes the selected path unreliable. Also it may consider the backup selection as a problem of connectivity and does not consider the traffic load and the bandwidth capacity. Hence in the existing system IP-over-WDM networks is used. This network is built on the wavelength division multiplexing (WDM) infrastructure [4] which has embedded IP layer topology on the optical layer topology and this is generally represented as two undirected graphs [5], [6] and [7]. Each IP link in the physical layer topology is mapped to a light path (connecting nodes in the logical topology) in the optical layer topology. As a result each IP link contains multiple fiber links which in turn may be shared by multiple IP links. When a single fiber link fails, the simultaneously all the logical links which is embedded on it fails.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

An example of IP-Over-WDN network is shown in Fig 1.1 and Fig 1.1a is the logical topology which is embedded on physical topology of Fig 1.1b where v_5, v_6 and v_7 are nodes in the physical topology which is absent in logical topology [8]. In Fig 1.1c the logical links are mapped to light paths.

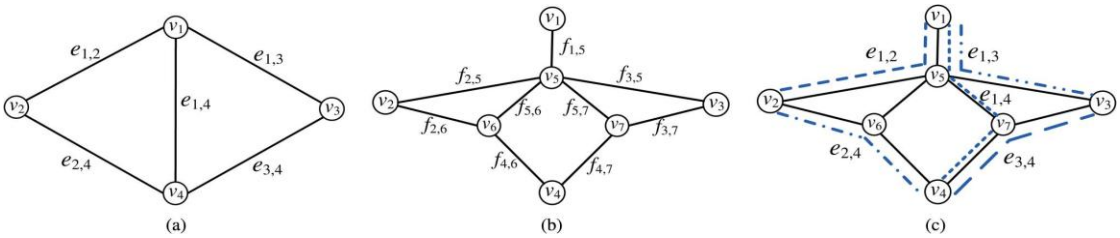

Fig 1.1 Mapping between Logical and Physical Topologies in IP-Over-WDM Networks
(a) Logical topology. (b) Physical topology. (c) Mapping between the logical and fibre links.

Say for example, let's consider the logical link $e_{1,4}$ which shares fiber link $f_{1,5}$ with the logical link $e_{1,3}$ and shares the fiber link $f_{4,7}$ with the logical link $e_{3,4}$ respectively. Sharing the fiber links does not mean that all the corresponding correlated logical links in the same SRLG must also fail. For example, let's look at the Fig 1.1c where the logical links $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ belongs to the same SRLG. If the logical link $e_{1,4}$ is failed due to the fiber link failure $f_{4,7}$ then it does not mean that the other links $e_{1,2}$ and $e_{1,3}$ must also fail which is an independent event. Also there is some probability where both $e_{1,2}$ and $e_{1,3}$ may also fail that becomes a correlated failure. Hence the failure of $e_{1,2}$, $e_{1,3}$ and $e_{1,4}$ are probabilistically correlated.

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 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.

An algorithm is used in this model for choosing 'N' reliable backup paths for each IP link which also calculates the rerouted traffic load and the usable bandwidth for each backup path to avoid link overload even when multiple link fails simultaneously. But the multiple reliable backup path information which is stored in the existing method is not secure and any unauthorized user and adversary can easily attack the stored information. In several systems user can able to access the information if he is provided with certain set of credentials. This is achieved by applying certain policies such as storing the data in a trusted server and medicate access control and if any server with the data is compromised the data confidentiality is also compromised [9].

Hence in the proposed system security mechanism is provided in the storage space where unauthorized adversary node should not alter or delete the stored information. For this purpose Cyphertext Policy – Attribute Based Encryption (CP–ABE) algorithm is used, where all the routing information (plaintext) in each router is encrypted and converted into cyphertext using public key encryption method. This encrypted information is stored in the hash table instead of the original plaintext. By this method the encrypted data is kept confidential even if the storage server is untrusted and also secure against collusion attack. The Attribute-based encryption (ABE) offers this desired ability to encrypt without exact knowledge of the receiver set. Decryption is enabled if and only if the ciphertext and secret key attribute sets overlap by at least a fixed threshold value [10].

A real ISP network with both optical and IP layer topologies are taken for the evaluation and concluded that it requires at least two backup paths to improve reliability, which in turn reduces the percentage of path disruption to some extent.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

II. RELATED WORK

In [1] the authors used Reactive Two-phase Rerouting (RTR) for intra domain routing with shortest path recovery. This protocol is used to recover networks from large scale failures by using two phases. In first phase the RTR forwards the packets towards the neighbor to gather the failure information and store it in the packet header. In the second phase it finds a new shortest path and bypasses the failure region which is independent of shape and location. This method achieves good performance with 98.6% reliability with minimum network resources. In [8] the authors used multiple backup paths which is predefined and stored in the hash table. Probabilistically Correlated Failure (PCF) model with a layer mapping approach is used which minimizes and quantifies the IP link failure and provides reliable backup paths too. If an IP link fails, its traffic is split into multiple backup paths such that the rerouted traffic should not exceed the usable bandwidth. The authors used ISP networks with both optical and IP layer topologies. A minimum of two backup paths are selected to provide reliability up to 18% and the routing disruption is reduced to about 22%. Hence the interface between rerouted traffic and normal traffic is avoided in this case. In [9] the authors used CP-ABE algorithm meant for realizing complex access control on encrypted data. By this technique the encrypted data can be kept confidential even if the storage server is untrusted; moreover, this method is secure against collusion attacks. In this method the attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.

III. EXISTING SYSTEM

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.

A. Disadvantages

1. The selection of the backup path consists of many interconnecting elements and thus it is very intricate in backup path-based protection method.
2. This methodology consumes some time for selecting multiple backup paths.
3. Many systems contemplate the evaluation of backup path as a connectivity problem and disregard the traffic load and the bandwidth capacity of the IP links for rerouting the traffic if any miscarriage occurs.
4. It took some delay to choose another reliable backup path if the existing backup path fails.
5. The backup path information which stored in the hash table can be easily attacked by the hackers or can be easily prone to adversary attack.
6. By changing the original routing information by the adversary there exist a major chance in data loss or the data may reach a wrong destination.

IV. PROPOSED SYSTEM

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

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.

An example of the basic architecture of CP–ABE algorithm is shown in Fig 4.1. All the backup path information is first encrypted using a public key before it is stored in the hash table and now the hash table contains the encrypted information. If any of the authorized users needs the data then the user has to request for an authorization to the node which encrypts the data. If the user is an authorized person then the corresponding node has to response the user with credentials. Then the user can send the request to the hash table to access the data and gets the encrypted data as response. Now the user can decrypt the data using the same public key. If the user is an unauthorized person then the corresponding node while receiving the request will not allow the user to access the data from the hash table.

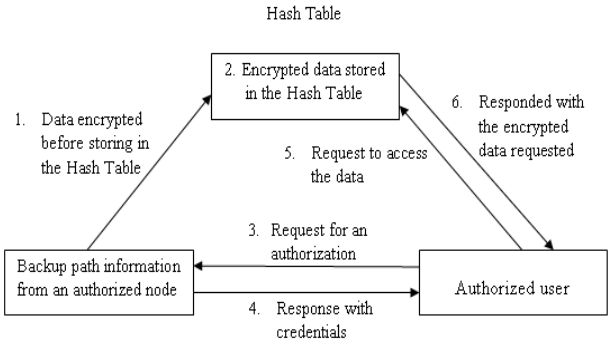

Fig 4.1 Basic Architecture of CP–ABE

A. 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 ciphertext and secret key attribute sets overlap by at least a fixed threshold value.

V. SYSTEM ARCHITECTURE

The architecture diagram for the proposed system is shown in Fig 5.1. All the nodes which need to involve in the communication are first created. All the nodes must then initialize themselves by registration before entering into the network. After registration in the network if the user is valid they can enter into the existing network topology. Path creation for the new node is then taken place in the hash table which includes both the primary path and multiple backup paths. This new node then sends default packets to all the nodes and the router to identify path failures. If there is no link failure along the selected primary path then packets are transmitted along the primary path. Suppose any link failure is detected then that particular link is removed from the network topology and the new details are then updated in the hash tables. Hence a reliable backup path among multiple backup paths is selected from the hash table using

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

DSDV protocol and this selected path is set as the primary path and packet transmission is taken place along this path. Unauthorized nodes can easily attack the routing information in the hash table. Hence to provide security to the routing information the hash table values are encrypted using CP–ABE algorithm with public key and this cyphertext is stored in the table. Hence the routing information is secured from adversary attack.

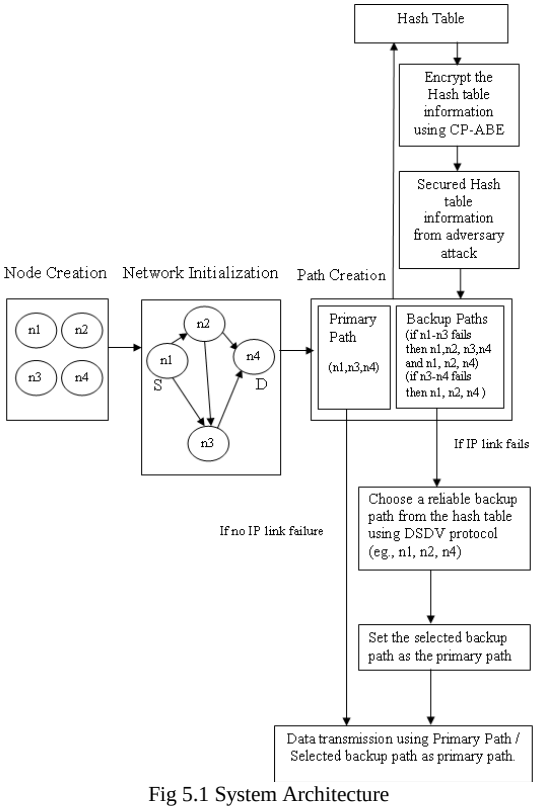

Fig 5.1 System Architecture

VI. 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.

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

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 cyphertext. 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 cyphertext that prevents the routing information from the adversary attack in network.

VII.RESULTS

The proposed system is implemented using NS2. Because of the lack of security in the existing system hash table and the ease of adversary attack, the packet drop is higher since the adversary can modify the information. A graph is plotted between time and packet size to study the packet drop in the existing system and is shown in Fig 7.1. The interpretation of result shows that the variation of packet size with respect to the time is Non linear and the packet size was found to be a maximum of 1.000 mbps at 13.000 ms minutes and is found to be a minimum of approximately 0.8000 mbps when the time is 16.000 ms. A graph is plotted between time and packet size to study the packet delivery ratio in the existing system and is shown in Fig 7.2. The interpretation of result shows that there is a linear decrement in delivered packet size with respect to its delivery time because of the lack of security. A graph is plotted between time and packet size to study the throughput of the proposed system and is shown in Fig 7.3. Here the packet size distribution starts increasing and it reaches a peak value of 280.000 mbps when the time is 1.000 ms and starts decreasing after that. At time 3.000 and above the packet size suddenly comes down to 0.000. The packet delivery ratio is improved since security is enhanced in the proposed scheme. A graph is plotted between time and packet size to study the packet delivery ration in the proposed system and is shown in Fig 7.4. The result interpretation shows that the delivered packet size increases linearly with respect to time. A graph is plotted between time and packet size to study the delay in the proposed system and is shown in Fig 7.5. Here the packet size distribution starts increasing and it reaches a peak value of 100.000 mbps when the time is 2.000 ms and starts decreasing after that. At time 4.000 ms the packet size suddenly comes down to 0.000 mbps and then the packet size remains zero till 20.000 ms.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

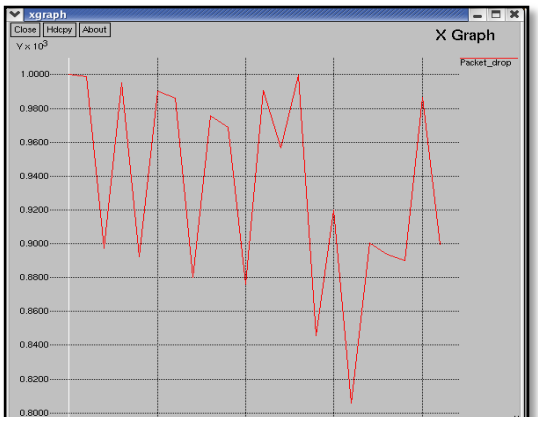

Fig 7.1 Packet Drop in the Existing System

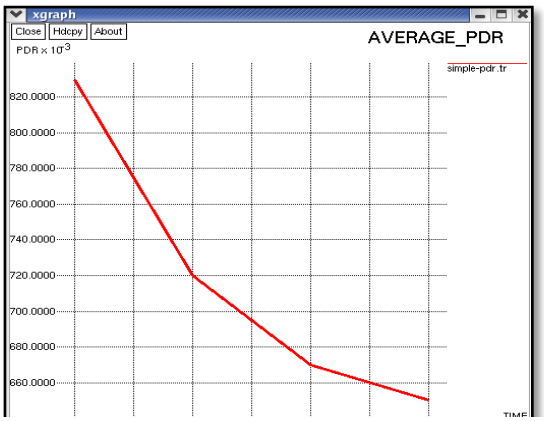

Fig 7.2 Packet Delivery Ratio in Existing System

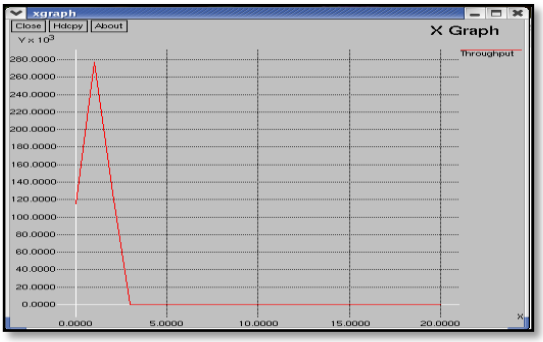

Fig 7.3 Throughput in Proposed System

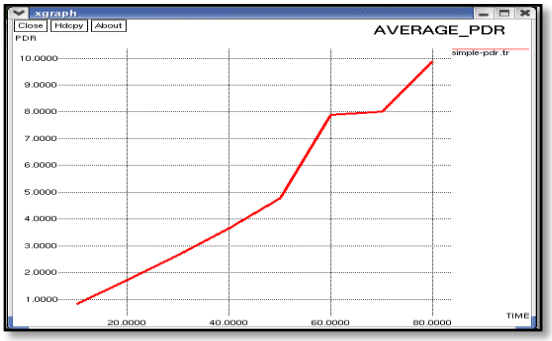

Fig 7.4 Packet Delivery Ratio in Proposed System

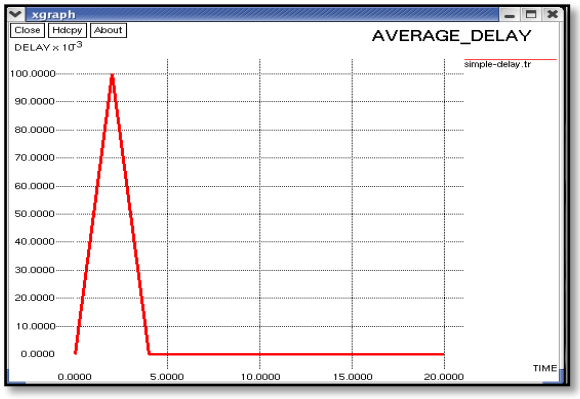

Fig 7.5 Delay in the proposed system

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

VIII. CONCLUSION

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.

REFERENCES

[1]Q. Zheng, G. Cao, T.L. Porta and A. Swami (2012), 'Optimal Recovery from Large-Scale Failures in IP Networks' in Proc. IEEE ICDCS, pp. 295-304.
[2]Bremler Barr, Y. Afek, H. Kaplan, E. Cohen and M. Merritt (2001), 'Restoration by Path Concatenation: Fast Recovery of MPLs Paths' in Proc. ACM PODC, pp. 43-52.
[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]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.
[6]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.
[7]K. Lee and E. Modiano (2009), 'Cross-Layer Survivability in WDM Based Networks' in Proc. IEEE INFOCOM, pp. 1017-1025.
[8]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.
[9]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.