Institute of Advanced Engineering and Science

International Journal of Electrical and Computer Engineering (IJECE)
Vol. x, No. x, May 2015, pp. 1 – 11
ISSN: 2088-8708

Issues in Routing Mechanism for Packet Forwarding : A Survey

Rohit Nilkanth Devikar[*], Dipak V. Patil[**], and V. Chandraprakash[***]
[*]Departement of Computer Science and Engineering, K L University
[**]Departement of Computer Engineering, MET, Bhujbal Knowledge City, Savitribai Phule Pune University
[***]Departement of Computer Science and Engineering, K L University

Article Info

Article history:
Received June 13, 2015
Revised
Accepted

Keyword:
Routing protocols
Packet forwarding
Connectivity
Load balancing
Convergence
Congestion Control

ABSTRACT

Nowadays internet has become more popular to each and every one. It is very sensitive to nodes or links failure due to many known or unknown issues in the network connectivity. Routing is the important concept in wired and wireless network for packet transmission. During the packet transmission many times some of the problems occur, due to this packets are being lost or nodes not able to transmit the packets to the specific destination. This paper discusses various issues and approaches related to the routing mechanism. In this paper, we present a review and comparison of different routing algorithms and protocols proposed recently in order to address various issues. The main purpose of this study is to address issues for packet forwarding like network control management, load balancing, congestion control, convergence time and instability. We also focus on the impact of these issues on packet forwarding.

Corresponding Author:
Rohit Nilkanth Devikar
Research Scholar
Departement of Computer Science and Engineering
K L University, Vaddeshwaram, Guntur
+919028339491
Email: rohit.devikar89@gmail.com

1. INTRODUCTION

In the old era, routing is simply forwarding the packet from one node to another, but now it is the process of choosing the best optimal path for packets transmission to improve the network performance. Basically the telephone switching network provides the quality of service by establishing the connection between sender and receiver before transmission of data. In telephone switching network delays are introduced during connection establishment phase, connection release phase as well as in transmission of packets. The performance of data transmission in telephone network is good but it requires a bandwidth dedication between sender and receiver. Due to this the utilization of network links is poor, results in reducing the performance of the overall network.

Instead the packet switching offers a best effort delivery of the packets. Packet switched network does not require the connection establishment between sender and receiver. So, delay is only present at the time of data transmission. Best effort delivery provides the selection of optimal path and this would be done with many of the routing protocols and dynamic routing algorithm. The nodes (i.e. switches and routers) present in the network take a part in providing the best effort delivery of the packets. During the transmission of the packets in wired as well as in wireless networks many of the problems stand in front of us which will be discussed in the next section.

Some important approaches and issues considered in this paper regarding routing techniques are:

1. Control management related issues present in wired as well as in wireless network.
2. Different types of congestion controlling techniques for Traffic analysis.
3. Network load balancing mechanism in Traffic Engineering.
4. Problem occurring during scaling of network. Also the effect of scaling on routing table.
5. Choosing the better techniques to improve the network availability.
6. Instability of the network is the current issue in the routing mechanism which results in loss of packets due to

fluctuation of the network links called as route flapping.
7. Different algorithms on improving the convergence time, so that the network updates with minimum time duration.

We will discuss the above issues one by one:

2. ROUTING CONTROL MANAGEMENT

Over the years, wired and wireless network security has become a major issue. Network provides security with authentication, authorization, denial of services, IP security. One time password (OTP) is very effective security mechanism nowadays. The entire government sector makes the use of OTP for better security.

Madalina Baltatu et al [1] focused on todays internet, as it uses the TCP/IP for communication, even though problem may occur at the time of authentication. They describe the attacks using ICMP messages. The ICMP messages generally consist of Destination unreachable and Timeout exceeded messages. The Denial of service attack exploits one of these two messages. The author describes the security attacks using ICMP router discovery messages. They use the protocol called ICMP router discovery protocol (IRDP) [1]. The IRDP consists of messages: Route Advertisement and route solicitation. Router advertises its routing table to the neighboring connected routers. Due to this each router have the recent routing information. During the advertisement the IRDP might result in facing the following attacks: passive monitoring, man-in-the-middle, denial of service etc. The most secure protection for routing is the implementation of static route from source to destination. But it offers for only small network or in LAN, with no any special QoS requirements. But for dynamic traffic flow which requires QoS static routing fails. In this case there is a need to use suitable, reliable routing protocols which provides QoS and authentication mechanism is mandatory. RIP and OSPF are firstly taken into consideration for providing QoS and authentication. The RIPv2 provides the authentication facilities in autonomous system using key management. OSPF uses the MD5 authentication security mechanism [1]. Geoff Huston et al [6] provide the security related issues in BGP. Border Gateway Protocol (BGP) is used between the autonomous systems (AS). BGP consists of speaker node which contains the path information of ASs. For AS 100 speaker node is C and for AS 200 only single router acts as speaker node. BGP does not provide protection against replay, message insertion, message deletion, man-in-the-middle attack, message modification type of attacks. They are combined with TCP to provide protection against all of the above attacks. BGP is highly vulnerable due to lack of verifying the authorization and authenticity of BGP control traffic [6]. The secure BGP (S-BGP) addresses this vulnerability. S-BGP provides the three security mechanism [2]. First it uses Public Key Infrastructure (PKI) for authentication of ownership of IP address blocks. Second BGP path attribute is used to carry the digital signatures. Third, IPSec is used to provide the data and partial sequence integrity and to enable the BGP speaker nodes to authenticate each other [3].

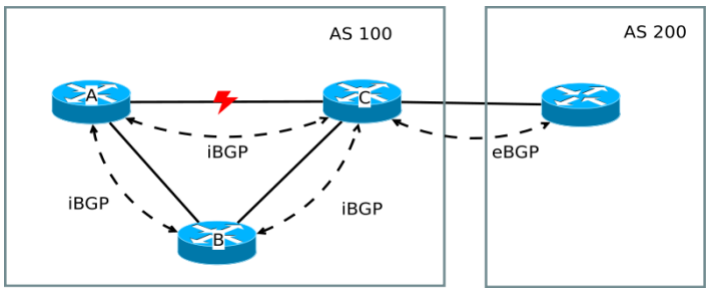

Figure 1. Communication between autonomous systems

Dan Wendlandt et al. [4], [2] use Availability Centric Routing (ACR) which enable end system to provide secure communication even if adversary controls the network infrastructure. ACR uses the four components:
1) It uses transit Autonomous system (AS) which provides multiple routes for each destination. Due to this adversary fails to track a valid communication path.
2) The destination can be identified by cryptographic algorithm by source ACR to conform whether destination is valid.
3) End systems securely monitors the communication to measure the performance, if performance is low then it chooses another path.
4) ACR end systems distribute traffics over more than one path.
The ACR provides end to end security with increasing the availability of the network [4].

Table 1. Security Related Techniques

Article	Technique for Secure Communication	Protocol/ Algorithm	Advantages
Madalina Baltatu et al [1]	Uses ICMP router Discovery messages	IRDP	It provides the route advertisement and route solicitation.
Glenn Jacobson [2]	Uses PKI, BGP Path Attributes, IPSec	S-BGP	It addresses the vulnerability of authentication and authorization.
Dan Wendlandt et al. [4]	Uses Transit AS, Cryptographic Algorithm, End system Monitors the communication,	ACR	Provides end to end security.
Chin-Fu Kuo et al [5]	Random packet delivery, Maintain External Routing Information	DDRA	Adding a field in routing table of RIP History Record for Packet Deliveries to the Destination Node
Mael Saleh and Liang Dong [7]	A single layer Module, Multilayer module.	Diff-EDF schedule with security enhancement services	Use for Real Time Application

Chin-Fu Kuo et al [5] proposes the dynamic routing algorithm that could select the path randomly for providing better security. The main goal is to propose the distance vector based algorithm to improve the data transmission for dynamic routing. The tradition routing table for distance vector routing uses the routing information protocol (RIP) consist of field (Next Hop, Destination Address, Metrics). The author uses the distributed dynamic routing algorithm (DDRA) which is the extended routing table version of distance vector routing algorithm. The table keeps the entries same as RIP with added field of History Record for Packet Deliveries to the Destination Node [5]. The DDRA consists of two parts:
1) Randomization process for packet delivery,
2) Maintaining external routing table information.

The algorithm proposed in [5] is easy to implement and is compatible with popular protocols like RIP and DSDV. The real time network application in traditional approach provides the better quality of service (QoS) with less essence of giving attention on security mechanism. Mael Saleh and Liang Dong [7] proposed a security enhancement in packet switched network for real time application. The use of adaptive security aware scheduling for packet switched networks has been done in [1] which is incorporated with security enhancement services. For scheduling they use the differentiated-earliest-deadline-first (Diff-EDF) and for security mechanisms they use security enhancement services [7]. The two modules are used to design a security service enhancement.
1) A single-layer Module,
2) Multilayer module.

The single layer design provides the enhancement for security services like confidentiality, integrity, or authentication. Whereas the multilayer module provides the enhancement for multilayer security services. At the destination the system measures the use of buffer and informs the source to change the security level of data packets adaptively. This scheme is effective for time and security related application.
Table 1 provides the comparison of different security related issues for controlling the network.

3. CONGESTION CONTROL TRAFFIC ANALYSIS

In data transmission and queuing theory, congestion occurs when the link carries more traffic than its capacity. The congestion in the network affects on packet transmission, data loss, as well as more queuing delay [8]. Let the capacity of the link from one node to another be suppose X, if the node transmit the packets with the capacity suppose Y, there would be two conditions:
1) $X > Y$, This case shows that packets are smoothly transmitted from one node to another without any congestion.
2) $X < Y$, The packets are lost due to congestion in the link.
In the new era, the internet users are growing very rapidly. Due to this many times congestion may occur during the packet transmission. The congestion is the main reason to degrade the performance and quality of service of the network. The following section describes the various issues and controlling techniques for congestion in the network:

Saverio Mascolo [8] proposed the control law and smith principle for managing the ABR (Available Bit Rate) flow in ATM network for congestion control. The Laplace transform technique is used to design the controller and for analyzing the performance of control system. For each flows from the switch the queue is maintained that stores the packet for transmission.

Ian F. Akyildiz et al. [9] discussed about the congestion control scheme for satellite network. Traditional TCP approach has the lower throughput mainly because of large propagation delays and high link error rate. The author introduces TCP-PEACH control scheme which provides end to end solution to improve the throughput performance. The TCP-PEACH control scheme has following algorithms:
1) Sudden start
2) Congestion Avoidance
3) Fast retransmission
4) Rapid recovery

The congestion avoidance and fast retransmission are the basic TCP-RENO and TCP-VEGO algorithms [9]. The sudden start and rapid recovery work on the principle of dummy segments. The dummy segments are the low priority segments generated at the sender. These dummy segments are used to avoid the congestion in the network. Generally the sender sends the dummy segments to examine the availability of the network resources. If the router in the path is congested then it discards the dummy segment and, if not then router replies to the sender with ACK message to inform the sender that i am ready to receive the packets.

Atilla Eryilmaz et al. [11] reduce one of the fair rate allocations of resources problems with the use of primary-dual congestion controlling (PDCC) mechanism incorporated with backpressure. The author proposes the mathematical model to improve fairness and stability.

VEHICULAR NETWORK

The Jianhua He et al. [12] proposed dedicated short range communication (DSRC) based collaborative safety application (CSA) scheme for congestion control. It contains two adaptive congestion control mechanism. 1) Detection of congested channel has been done at MAC layer. 2) After detection the congestion signal is transmitted to the application layer to control the traffic rate. In vehicular network the nodes are distributed unevenly. Due to this some nodes have many neighbors while others have less. For the fair generation of traffic and fair controlling of traffic it is necessary to have the cooperation among the nodes. Due to this, nodes having many neighbors are not congested unevenly; this can be handled with the help of MAC blocking and unblocking techniques.

Haitao Wu et al [13] propose the new technique called Incast congestion control for TCP (ICTCP). Actually what happens in traditional approach the multiple users send data to the single user or node or link, so there is a possibility of congestion at the receiver. Traditional approach concentrates on fast transmission only without knowing the receiver capacity. Unlike in ICTCP they focused on receiver based congestion control algorithm to reduce the packet losses. Due to this performance of the network is improved with reduction in congestion. The [13] [14] provide the congestion control in packet transmission, but they fail to reduce the detection of packet losses at required extent. The Shikhar Shukla et al. [15] proposed the PLATO TCP congestion control mechanism which detects the packet losses. PLATO concerns the packet labeling scheme for the solution to TCP Incast. TCP detects the loss after 200ms, because of loss cannot be avoided earlier. The PLATO detects the loss packets with the help of providing three duplicate acknowledgement mechanisms with labeling system rather than waiting for 200 ms delay. In that PLATO places a label to the TCP segment and transmits to the receiver. Receiver sends a label acknowledgement (ACK) for the receive label segment. Again sender sends the label segment to acknowledge the Label ACK [15]. Ferhat Dikbiyik et al. [16] proposed the problem in exploiting the excess capacity (EC) in optical WDM (Wavelength Division Multiplexing) in terms of bandwidth blocking. Optical network uses the two links: primary link and protected link (Backup link). The primary link is used to transmit regular traffic and when any failure or congestion occurs in primary link or in any node then there is a provision to use the protected link. They investigate the three techniques for the management of EC [16]:
1) Pre-provisioning: When network is lightly loaded, the resources are reserved by pre-provisioning technique, i.e. protected links are reserved to increase the availability.
2) Backup re-provisioning: High available links generally have more number of available resources. Connection in the proposed scheme switches to protection scheme having lower availability. If the traffic on the protected scheme is increased then it is necessary to re-provisioning the backup resources.
3) Hold light-path: In this technique they keep the pre-established resources for lightly loaded path to increase the availability of the link and reduce the connection setup time.

The authors more focus on hold light-path technique where the light paths are held, even if no any supported

Table 2. Controlling Congestion in the Network

Article	Network	Algorithm for Congestion Control	Description
Saverio Mascolo [8]	ATM	Control Flow and Smiths Principle	Use to control best effort traffic, algorithm guarantees stability of network queue also provides full link utilization.
Ian F. Akyildiz et al. [9]	Satellite	TCP-PEACH	Improves the fairness for sharing network resources and goodput performance.
Atilla Eryilmaz et al. [11]	Wireless	primary-dual congestion controlling (PDCC)	Provides fairness and stability in wireless network.
Jianhua He et al. [12]	Vehicular	Cross layer design approach and traffic rate control approach	These control schemes are used to adapt dynamic traffic load effectively.
Haitao Wu et al [13]	Data Centre	Incast congestion control for TCP (ICTCP)	Avoid Congestion by Achieving zero timeout and provides better goodput.
Shikhar Shukla et al. [15]	Data Centre	PLATO TCP	Use packet labeling technique for detection of loss packets.
Ferhat Dikbiyik et al. [16]	OpticalWDM	Preprovisioning, Backup reprovisioning, Hold-lightpath	Increases availability of connection and decreases connection setup time.

connection, until a backup re-provisioning event triggers [16].

Congestion controlling mechanism is very important part in traffic engineering, as it leads to the birth of load balancing. For congestion controlling it is necessary to divide the traffic across multiple paths or store it at the nodes (router or switch) queue. Table 2 provides different congestion control mechanism for packet forwarding.

4. NETWORK LOAD BALANCING

Load balancing is a technique used to distribute the workload over multiple paths or multiple processors. Load balancing term is generally evolved to utilize the network resources effectively and reduce the congestion in the network.

General Load balancing algorithms described in [18] are weighted balance, Priority, Overflow, Persistence, Least Used, Lowest Latency. Weighted load balancing algorithm assigns large traffic to faster link and less traffic to slower link. In priority based load balancing, priority is given to the paths. Traffic will be forwarded from high priority path and low priority is used when the high priority link or path fails. In Overflow load balancing technique, the node transmits the packet from the high priority link. If it exceeds the available bandwidth then overflow in the link may occur. So, if the overflow occurs in the link, the operator uses the low priority link for forwarding. Persistence algorithm is one in which the traffic type should be specified by the sender, and it would be sent from the same link until the connection failure has occurred. Least used algorithm is one in which traffic should be transmitted to those link having most available bandwidth. Lowest latency specifies the assignment of traffic to the link having minimum response time or minimum delay (Lower latency) [18].

The basic load balancing algorithm to improve the network availability is shown in figure 2. In the network for switching of traffic a primary paths as well as number of alternative paths are present. In traditional approach there is a use of primary path for the transmission of traffic and when the primary path is congested or fails, then and then only the secondary path is used. The alternate or backup route is utilized only when the primary link fails which shows inefficient utilization of bandwidth and network resources. The simple algorithm shown below describes how the network balances the load on the primary as well as on secondary paths.

Suppose P1 and P2 represent Path1 and Path 2 respectively. S is the source node and D is the destination node. The total number of routers between source and destination is R. The number of routers in path1 and path2 are assumed to be R1and R2 respectively. N is the total number of packets at the source at time T0.

Suppose source S has 90 packets at time T0, and then it will send 60 packets from path2 and 30 packets from path1.

Xiaohua Jia et al [19] analyses the shortest path tree (SPT) and Minimum spanning tree (MST) approach to reduce the delay and cost of the network respectively. Also the MST and SPT are used to provide the optimum

```
Then,
        R= (Σ R1) + (Σ R2);
        Z=N/R;
If (P1 Hops (S, D) >P2 Hops (S, D))
  Then P1 sends ( Z*ΣR2) number of packets.
Else
If (P2 hops (S, D) >P1 hops (S, D))
  Then P2 sends (Z*ΣR1) number of packets.
Else
  Both P1 and P2 send N/2 number of packets.
```

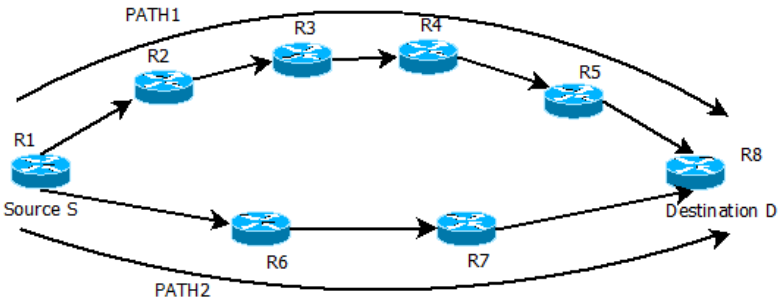

Figure 2. Algorithm and relative figure for Load balancing approach

solution for load balancing and wavelength assignment problem. Kartik Gopalan et al [20] proposed a Link criticality based routing (LCBR) algorithm used to select the primary route and primary backup route. In the network Dijikstra algorithm is used to select the shortest path from source to destination but it is not efficient in the presence of large delay also Dijikstra algorithms cannot solve the end to end delay partitioning problem. The route selection process in Primary LCBR can be carried out using both online and offline fashion. In offline technique performs once for entire network. Between each source and destination the k shortest paths are calculated and compute the expected load on each link. While in online technique the Primary LCBR calculates cost of each link between source and destination. It also checks the resources available for the route r satisfy the QoS. If resources are sufficient then PLCBR distributes end to end delay among the links of route r. After this PLCBR calculates the remaining link capacity R of route r and projected network cost cost(G). There are two conditions to reject the route setup request for primary path F.
1) If route does not have resources to fulfill the QoS,
2) The value of cost(G) for route r is greater than predefined cost.
For selection of Primary Backup LCBR (PBLCBR) the primary route elements is removed and same procedure like PLCBR is applied to obtain the Backup route [20]. Lu Ruan et al. [21] describe the load balancing in optical WDM network based on primary, backup and free channels. The primary link can be selected as a shortest path with more number of free channels. Suppose "δ" be some threshold value for free channel. Assign cost of 1 to every link having more than "δ" free channels and cost greater than one to a link having less than "δ" free channels. If the link does not have any free channel then cost of the link would be considered as ∞. After assigning the cost to each link, Dijkstras algorithm is applied to the topology to compute the primary path with having minimum number of cost. Backup route is used to reduce the load on primary route as well as the link having large number of sharable backup channels. Suppose ***cand(l)*** is the ***"l"*** backup channels, so the cost for backup route can be computed as: ***Cost(l)*** is considered to be for link having zero backup channel, otherwise cost for backup channel is $1/cand(l)^r$, where ***"r"*** depends on the difference between two link costs. After cost computation the backup route is calculated based on the link having high chance of sharable back up channels [21].

A. K. Mishra and A. Sahoo [22] proposed the S-OSPF algorithm for load balancing. Source node distributes the traffic to the neighbor node, after this traffic forwarded to the destination node using OSPF protocol. The S-OSPF works based on traffic demand which maintains the traffic matrix. But it requires more processing power and the fluctuation in the network will increase the problem of maintaining the traffic matrix. Jiayue He and Jennifer Rexford in [23] proposed the method for multipath routing mechanism for load balancing. They explain the congestion in control plane and data plane and splitting the traffic over multiple paths. The router in the data plane use to forward the packets on the alternate path based on encapsulation and explicit routing techniques. Marija Anti et al. [24] proposed linear programming approach for load balancing. They define the link load not only depends on node traffic load, traffic matrix element. When the routing packet enters in the network, intermediate routers are decided. Packets are then forwarded along the shortest path from source node to intermediate node and from intermediate node to final destination. Network assigns the different weights to the nodes, and split the network capacity to the different nodes depends upon their bandwidth requirements. The Sangsu Jung et al. in [25] propose the load balancing and congestion control approach in wireless mesh network. The traditional routing approach such as AODV and geographic routing such as GPSR are responsible for long delay and frequent packet losses if the hot spot is congested. The wireless mesh network provides the hub and spoke type routing policy in which firstly they reflect the traffic volume, secondly the finite element method is used to assign a potential value to each node, and finally proposed a novel Potential-Field Based Routing (PFBR) protocol for load balancing. The potential value reflects distance to destination as well as traffic volume at each node. In PFBR the congestion at far node can be avoided by only exchanging the local routing information with the neighbor which is just a one hop distance from the node. The mesh node can forward a packet to

the neighbor node which has lower potential value [25].

Marija Antic et al. [26] proposed the load balancing shortest path routing (LB-SPR) technique, which significantly reduce the reliable network cost. The LB-SPR provides:
1) It does not require the actual traffic pattern for routing optimization.
2) Require low cost for bandwidth reservation.
3) Every router in the network knows the maximum traffic load it is allowed to generate.
The LB-SPR algorithm improves the reliability of the network. If any node or link fails the LB-SPR with OSPF adjust the routing in such a way that traffic loads are forwarded. LB-SPR consists of two steps to send the traffic from source to destination. In this algorithm the source does not directly transmit the traffic to destination. It first sends the traffic to the intermediate node called load balancing router, after that from load balancing router to the destination [24], [26]. To reduce the problem of traffic demand [22], extended scheme of S-OSPF is used in [27], which works on hose model. In this scheme only the total amount of traffic the source sends into the network and the total amount of traffic it receives from the network is needed. Suppose the network consists of source *"p"* and destination *"q"*. The source *"p"* sends the traffic into the network (Outgoing traffic) is given by the following equation:

$$\sum_{q \in Q} d_(pq) \leq \alpha p \qquad p \in Q \tag{1}$$

Where, αp is the maximum traffic sent by source into the network.
While the total incoming traffic to the source node *"p"* is given by:

$$\sum_{p \in Q} d_(pq) \leq \beta q \qquad q \in Q \tag{2}$$

Where, βq is the maximum traffic received by node *"q"* from the network.

The Brice Augustin in [28] proposed the multipath routing in the network with three different load balancing algorithms: Per-flow, Per-Destination, and Per-Packet. They estimate the results using above three algorithms and observe that the per-packet load balancing are less effective. In per-packet load balancing the main problem is each packet follows different paths so it requires the reordering of the packets. While the per-flow and per-destination load balancing techniques are still widely used. Traffic engineering (TE) plays an important role in determining the reliability and performance of a network. George Athanasiou et al. [29] describe the Energy Aware Traffic engineering scheme. The main objective of TE is to minimize the maximum utilization of link. The author also focuses on minimizing the energy consumption by turning the unutilized and idle links into the sleeping mode. Load balancing can be achieved by splitting the traffic over multiple links with consideration of minimizing the maximum link utilization. Equal cost multiple paths forwarding (ECMP) is a very prominent technique for the network in which each link has equal cost. But this technique is inefficient for increasing path diversity in which each link is having different weights to optimize network resource usage. In [30] uses the PEFT (Panelized Exponential Flow spliTting) technique which transmits the packets over multiple unequal link cost paths, where as traffic splitting decision are made independently. The topology uses the OSPF protocol for computing the links weight. For implementation of link weight optimizer requires solving a convex optimization problem and Link weights computation. Traffic engineering is improved by fairer network load balancing, minimizing the maximum link utilization (MLU) and increasing network capacity. Shuo Fang et al. [31] proposed a software defined approach for load balancing by integrating dynamic load balancing multipath scheme (DLBMP) with congestion control (CC). The DLBMP+CC improve the network throughput by making the full utilization of bandwidth and congestion control used to prevent the excessive network traffic entering into the network. With the use of SDN in [31], the dynamic algorithm can react very quickly towards topology changes, congestion control, load imbalance, and any updates. Table 3. shows different scenarios for balancing the load over network.

5. INSTABILITY AND CONVERGENCE TIME

In the recent years internet instability and route fluctuation are important problems in the network. Instability in the network results in loss of packets, which in turn increases the latency and convergence time. Following section describes the research work done by different researchers to improve the convergence time and instability of the network.

Craig Labovitz et al. [33] describe some unpredicted trends in routing stability. The authors developed the taxonomy for routing information and identify the origin of pathological behavior. The routing information is

Table 3. Network Load Balancing

Article	Load Balancing Scheme	Description
Xiaohua Jia et al [19]	SPT, MST	SPT is used to minimize Delay and MST reduces the network Cost.
Kartik Gopalan et al [20]	LCBR	Provides higher resource utilization, also have primary as well as backup route for faster link failure recovery.
Lu Ruan et al. [21]	Routing with Load Balancing Heuristics (RLBH)	Assign link cost based on number of free channels available at link.
A. K. Mishra et al. [22]	Smart-OSPF (S-OSPF)	Provides better resources utilization for traffic engineering.
Jiayue He et al. [23]	Flexible Multipath Routing	Flexible splitting Distributes load over multiple paths based on traffic class.
Marija Anti et al. [24]	Linear Programming Approach	Assign traffic values to network nodes.
Sangsu Jung et al. in [25]	Potential-Field Based Routing (PFBR) protocol	Assign potential values to nodes based on numerical analysis. This potential value provides distance to destination as well as traffic volume.
Marija Antic et al. [26]	LB-SPR	Supports guaranteed traffic load and simplifies resource reservation.
Brice Augustin [28]	Per-flow, Per-Destination, and Per-Packet	Provides broad description of multipath routing in the internet.
George Athanasiou et al. [29]	Energy Aware Traffic engineering	Splitting the traffic over multiple links by minimizing the maximum link utilization.
Fung Po Tso et al. [30]	PEFT (Panelized Exponential Flow spliTting)	Use to transmit packets over unequal cost path.
Shuo Fang et al. [31]	DLBMP+CC	Only Path load attribute is monitor to track network traffic load.

classified into three classes: 1) Forwarding instability, 2) Policy Fluctuation, 3) Pathologic updates (redundant). This research observed redundant data during update of routing topology for nine months. Most of the data collected were redundant. Finally they explain the impact of this redundant data on network infrastructure. Aristotelis Tsirigos et al. [34] define a failure probability technique to improve the stability of the network. Each link has the failure probability Pi, and each path is independent of others, no any node or link is common for particular path in the network. In mobile network, the topology changes due to time unstable state of the network. As this scheme defines the probability of path failure for each link, it is used to develop the probability function Psucc (Probability that no more Mblocks is lost). From observation it was shown that the probability of successful communication increased between source and destination only when we increase the number of paths. This reduces the congestion and transmission delay. In the recent years OSPF and IS-IS are used to compute the shortest path tree (SPT) from router to router. As there are multiple SPT in the network, recovery from failure causes changes in existing SPT topology which results in routing instability. Paolo Narvez et al. [35] [36] proposed the new algorithm which improves the stability of network by making minimum changes in the existing SPT topology, when some link or router in the network fails. After failure, the discontinuity is encountered in link state advertisement and re-computation of routing table. For link state routing OSPF (optimal shortest path first) protocol is used. As failures is increasing the instability in the network increases. To improve the failure resiliency without affecting routing stability, Srihari Nelakuditi [37] proposed a failure insensitive routing (FIR) approach. This approach suppresses the link state advertisement. Using this approach, when at most one link failure notification is suppressed, a packet is guaranteed to be transmitted to its destination along loop free path. The experimental results show that FIR provides better routing stability and availability than OSPF in terms of network sizes, failure frequency, and convergence delays.

Yang Richard Yang et al. [38] reported the results on efficiency and stability to achieve the traffic engineering objectives in interdomain routing when interactions among routing to multiple destinations cause instability in routing even if each route to destination has unique solution. Route selection problem is stable only if the interaction among the ISPs follows the set of interdomain traffic engineering guidelines; otherwise instability occurs in route selection process. The accidental activities such as failure, misconfiguration, route flapping, induced several BGP instabilities

in the network lead to delays, loss of data and connectivity.

Todays internet routers are overcome by a number of BGP updates caused by events such as failure, session reset, and policy changes. Such events can delay routing convergence, which degrades the performance of networks in terms of jitter and delay sensitive application. Wei Sun et al. [39] propose the novel approach of differentiated processing in terms of BGP updates, which improve the routing convergence and reduces the routers load. Based on this approach the BGP updates are classified into two classes. Higher priority updates are processed sooner, while the lower priority updates are delayed to reduce router load and processing. The simulation result shown [39] reduces the convergence time by 80% and having 30% fewer BGP updates. Mean Route Advertisement interval (MRAI) performs an important role in BGP convergence time. In the case of normal load, adaptive MRAI timers perform better for BGP updates. As soon as load is increased there may be a problem of flooding at routers and adaptive MRAI timer is not efficient. Adaptive MRAI timer fails to scale if the BGP Updates in the network are increasing. Shivani deshpande et al. [40] proposed the BGP instability detection mechanism that can be executed by individual routers. The input data for detection of instability is BGP update messages received by routers from its neighbor. From this BGP update messages features (like AS path length, AS path edit distance) are extracted in every five minutes, this shows the change in topology. The GLR (Generalized Likelihood Ratio test), Segmentation boundary detection, Boundary position optimization algorithms are used to detect the changes. Geoff Huston et al. [41] proposed a Path Exploration Damping (PED) technique which reduces the volume of BGP update messages and decreases the average time required to restore reach-ability. They compare PED impact on convergence time with Mean route advertisement interval (MRAI), Route Flap Damping (RFD), and Withdrawal Rate Limiting (WRATE). From experimental results it was found that the total BGP announcement can decrease by up to 32%, and path exploration reduced by 77% compared with traditional MRAI approach. Mohammad Yanuar Hariyawan [10] compared different technoques like Fast Reroute one to one backs up, local rerouting, Haskin, 1+1 path protection recovery mechanism and PSL oriented path protection mechanism technique for fast rerouting after failure. The performance shows that 1+1 path protection recovery mechanism has minimum packet loss, but having more cost. Rajvir Gill et al. [42] proposed the FLD-MRAI (Flexible Load Dispersing MRAI) algorithm that disperses the load in the network, which results in reducing the routers overhead. The authors focused on routing policies and their effects on number of updates, convergence time. The FLD-MRAI algorithm works in case of both high and normal loads. When degree of preference (DoP) chooses the shortest path, then FLD-MRAI believe this situation as normal load, and when DoP chooses the longest path then FLD-MRAI believe this situation as high load. Below table compares the different approaches to improve the convergence time of a network. Table 4 provides different scenarios for improving the stability and reducing convegence time of network.

6. CONCLUSION

In this paper, we have presented a brief survey on different issues like control management, availability, congestion control, convergence time, instability, load balancing based on network routing. Most of the researchers are working on network load balancing and congestion control for traffic engineering (TE). From the existing work we have discussed the different problems and their respective solutions for packet forwarding by considering above issues. I hope this paper will be beneficial to readers for better understanding about the current issues that are occurring in the network for packet forwarding.

REFERENCES

[1] Madalina Baltatu, Antonio Lioy, Fabio Maino, Daniele Mazzocchi, Security Issues in Control, Management and Routing Protocols, Terena Networking Conference, May 22-25, 2000 pp. 1-12.
[2] Glenn Jacobson , Security Issues with Internet Routing Border Gateway Protocol (BGP), Global Information Assurance Certification Paper, SANS Institute 2003.
[3] Stephen T. Kent, Securing the Border Gateway Protocol: A Status Update, 7th IFIP-TC6 TC11 International Conference, CMS 2003, Torino, Italy, October 2-3, 2003, Proceedings, pp. 40-53.
[4] Dan Wendlandt, Ioannis Avramopoulos, David G. Andersen, Jennifer Rexford, Dont Secure Routing Protocols, Secure Data Delivery, In Proc. 5th ACM Workshop on Hot Topics in Networks (Hotnets-V), (Irvine, CA), Nov. 2006, pp. 1-6.
[5] Chin-Fu Kuo, Ai-Chun Pang, Sheng-Kun Chan Dynamic Routing with Security Considerations, IEEE Transactions on Parallel and Distributed Systems, Vol. 20, No. 1, January 2009 pp. 48-58.
[6] Geoff Huston, Mattia Rossi, and Grenville Armitage Securing BGP - A Literature Survey, IEEE Communications Surveys & Tutorials, Vol. 13, No. 2, Second Quarter 2011, pp. 199-222.

Table 4. Mechanism to Improve the Convergence Time

Article	Protocol	Description
Aristotelis Tsirigos et al. [34]	Multipath routing	In this technique, routing scheme that uses multiple paths by splitting the information over multiple paths to increase corrected data receive probability.
Paolo Narvez et al. [35] [36]	Dynamic SPT	Used to update only part of shortest path tree affected by changes. Due to this only minimum changes have been done to improve the stability.
Srihari Nelakuditi [37]	Failure Insensitive Routing (FIR)	FIR improves the availability and stability by suppressing the advertisement of failure paths and traverse traffic along the loop free path.
Yang Richard Yang et al. [38]	Rational Route Selection Algorithms	Analysis of set of guidelines for interdomain traffic engineering has been done. If AS follows this guidelines, it provides guaranteed stable route solution.
Shivani deshpande et al. [40]	Statistical Pattern Recognition Techniques	The method performs well under all kinds of instability. In this, features has been extracted from the BGP update messages for capturing the statistical changes.
Geoff Huston et al. [41]	Path Exploration Damping (PED)	PED Reduces the BGP update message announcement compare to traditional damping approach.
Rajvir Gill et al. [42]	FLD-MRAI (Flexible Load Dispersing MRAI)	Improves convergence time by Dispersing network loads over routers.
Chi Harold Liu. [32]	Generic Admission Control (GAC)	By controlling the admission for packet at ingress node the algorithm improves the QoS.

[7] Maen Saleh and Liang Dong, Real-Time Scheduling with Security Enhancement for Packet Switched Networks, IEEE Transactions on Network and Service Management, Vol. 10, No. 3, September 2013, pp.-271-285.
[8] Saverio Mascolo, Smith's Principle for Congestion Control in High-Speed Data Networks, IEEE Transactions on Automatic Control, Vol. 45, No. 2, February 2000, pp. 558-564.
[9] Ian F. Akyildiz, Giacomo Morabito, and Sergio Palazzo, TCP-Peach: A New Congestion Control Scheme for Satellite IP Networks, IEEE/ACM Transactions on Networking, Vol. 9, No. 3, June 2001, pp. 307-321.
[10] Mohammad Yanuar Hariyawan, Comparison Analysis of Recovery Mechanism at MPLS Network, International Journal of Electrical and Computer Engineering(IJECE), Vol.1,No.2, December 2011, ISSN:2088-8708, pp.151-160
[11] Atilla Eryilmaz, and R. Srikant, Joint Congestion Control, Routing, and MAC for Stability and Fairness in Wireless Networks, IEEE Journal on Selected Areas in Communications, Vol. 24, No. 8, August 2006, pp. 1514-1524.
[12] Jianhua He, Hsiao-Hwa Chen, Thomas M. Chen, and Wenqing Cheng, Adaptive Congestion Control for DSRC Vehicle Networks, IEEE Communications Letters, Vol. 14, No. 2, February 2010, pp. 127-129.
[13] Haitao Wu, Zhenqian Feng, Chuanxiong Guo, Yongguang Zhang, ICTCP: Incast Congestion Control for TCP in Data-Center Networks, IEEE/ACM Transactions on Networking, Vol. 21, No. 2, April 2013, pp. 345-358.
[14] Yan Zhang, Nirwan Ansari, On Architecture Design, Congestion Notication, TCP Incast and Power Consumption in Data Centers, IEEE Communications Surveys & Tutorials, Vol. 15, No. 1, First Quarter 2013, pp. 39-64.
[15] Shikhar Shukla, Shingau Chan, Adrian S.-W. Tam, Abhishek Gupta, Yang Xu, and H. Jonathan Chao, TCP PLATO: Packet Labelling to Alleviate Time-Out, IEEE Journal on Selected Areas in Communications, Vol. 32, No. 1, January 2014, pp. 65-76.
[16] Ferhat Dikbiyik, Massimo Tornatore, and Biswanath Mukherjee Exploiting Excess Capacity for Survivable Traffic Grooming in Optical Backbone Networks, Journal of Optical Communication Network Vol. 6, NO. 2/FEBRUARY 2014, pp. 127-137.
[17] Eitan Zahavi, Isaac Keslassy, and Avinoam Kolodny, Distributed Adaptive Routing Convergence to Non-Blocking DCN Routing Assignments, IEEE Journal on Selected Areas in Communications, Vol. 32, No. 1, January 2014, pp. 88-101.
[18] http://www.peplink.com/technology/load/balancing - algorithms/.
[19] Xiaohua Jia, Xiao-Dong Hu, Lu Ruan,and Jianhua Sun Multicast Routing, Load Balancing, and Wavelength

Assignment on Tree of Rings, IEEE Communications Letters, Vol. 6, No. 2, February 2002, pp. 79-81.
[20] Kartik Gopalan, Tzi-cker Chiueh, Yow-JianLin, Load Balancing Routing with Bandwidth-Delay Guarantees, QoS in IP and Wireless Network, IEEE Communication Magazine June 2004, pp. 108-113.
[21] Lu Ruan, Haibo Luo, and Chang Liu, A Dynamic Routing Algorithm With Load Balancing Heuristics for Restorable Connections in WDM Networks, IEEE Journal on Selected Areas in Communications, Vol. 22, No. 9, November 2004, pp. 1823-1829.
[22] A. K. Mishra and A. Sahoo, S-OSPF: a trafc engineering solution for OSPF based on best effort networks, in Proc. IEEE Globecom 2007, pp. 1845-1849.
[23] Jiayue He and Jennifer Rexford, Toward Internet-Wide Multipath Routing, IEEE Network, March/April 2008, pp. 16-21.
[24] Marija Antic, Aleksandra Smiljanic, Routing with Load Balancing: Increasing the Guaranteed Node Trafcs, IEEE Communications Letters, Vol. 13, No. 6, June 2009, pp 450-452.
[25] Sangsu Jung, Malaz Kserawi, Dujeong Lee, and June-Koo Kevin Rhee, Distributed Potential Field Based Routing and Autonomous Load Balancing for Wireless Mesh Networks, IEEE Communications Letters, Vol. 13, No. 6, June 2009, pp. 429-431.
[26] Marija Antic, and Aleksandra Smiljanic, Cost Reduction of Reliable Networks Using Load Balanced Routing, IEEE Communications Letters, Vol. 14, No. 3, March 2010, pp. 263-265.
[27] Eiji Oki and Ayako Iwaki, Load-Balanced IP Routing Scheme Based on Shortest Paths in Hose Model, IEEE Transactions on Communications, Vol. 58, No. 7, July 2010, pp. 2088-2096.
[28] Brice Augustin, Timur Friedman, and Renata Teixeira, Measuring Multipath Routing in the Internet, IEEE/ACM Transactions on Networking, Vol. 19, No. 3, June 2011, pp. 830-840.
[29] George Athanasiou, Kostas Tsagkaris, Panagiotis Vlacheas, Dimitrios Karvounas, and Panagiotis Demestichas, Multi-Objective Trafc Engineering for Future Networks, IEEE Communications Letters, Vol. 16, No. 1, January 2012, pp. 101-103.
[30] Fung Po Tso and Dimitrios P. Pezaros, Improving Data Center Network Utilization Using Near-Optimal Traffic Engineering, IEEE Transaction on Parallel and Distributed System, Vol. 24, No. 6, June 2013, pp. 1139-1147.
[31] Shuo Fang, Yang Yu, Chuan Heng Foh, and Khin Mi Mi Aung, A Loss-Free Multipathing Solution for Data Center Network Using Software-Defined Networking Approach, IEEE Transaction on Magnetics, Vol. 49, No. 6, June 2013, pp. 2723-2729.
[32] Chi Harold Liu, Kin K. Leung, and Athanasios Gkelias, A Generic Admission-Control Methodology for Packet Networks, IEEE Transactions on Wireless Communications, Vol. 13, No. 2, February 2014, pp. 604-617.
[33] Craig Labovitz, G. Robert Malan, and Farnam Jahanian, Internet Routing Instability, IEEE/ACM Transactions on Networking, Vol. 6, No. 5, October 1998, pp. 515-528.
[34] Aristotelis Tsirigos and Zygmunt J. Haas, Multipath Routing in the Presence of Frequent Topological Changes, IEEE Communications Magazine, November 2001, pp. 132-138.
[35] Paolo Narvez, Kai-Yeung Siu, and Hong-Yi Tzeng, New Dynamic Algorithms for Shortest Path Tree Computation, IEEE/ACM Transactions on Networking, Vol. 8, No. 6, December 2000, pp. 734-746.
[36] Paolo Narvez, Kai-Yeung Siu, and Hong-Yi Tzeng, New Dynamic SPT Algorithm Based on a Ball-and-String Model, IEEE/ACM Transactions on Networking, Vol. 9, No. 6, December 2001, pp. 706-718.
[37] Srihari Nelakuditi, Sanghwan Lee, Yinzhe Yu, Zhi-Li Zhang, and Chen-Nee Chuah, Fast Local Rerouting for Handling Transient Link Failures, IEEE/ACM Transactions on Networking, Vol. 15, No. 2, April 2007, pp. 359-372.
[38] Yang Richard Yang, Haiyong Xie, Hao Wang, Avi Silberschatz, Arvind Krishnamurthy, Yanbin Liu, Li Erran Li, On Route Selection for Interdomain Traffic Engineering, IEEE Network, November/December 2005, pp. 20-27.
[39] Wei Sun, Zhuoqing Morley Mao, Kang G. Shin, Differentiated BGP Update Processing for Improved Routing Convergence, IEEE Conference Publication, ICNP Network Protocol, 12-15 November 2006.
[40] Shivani Deshpande, Marina Thottan, TinKamHo, and Biplab Sikdar, An Online Mechanism for BGP Instability Detection and Analysis, IEEE Transactions on Computers, Vol. 58, No. 11, November 2009, pp. 1470-1484.
[41] Geoff Huston, Mattia Rossi, and Grenville Armitage, A Technique for Reducing BGP Update Announcements through Path Exploration Damping, IEEE Journal on Selected Areas in Communications, Vol. 28, No. 8, October 2010, pp. 1271-1286.
[42] Rajvir Gill, Ravinder Paul, and Ljiljana Trajkovic, Effect of MRAI Timers and Routing Policies on BGP Convergence Times, in proc. IPCCC, IEEE 31st International Conference, 1-3 December 2012.