J. Basic. Appl. Sci. Res., 4(6)57-67, 2014

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

A Review Study of Interior and Exterior Gateway Protocols

Muhammad Umar Aftab[1], Amna Nisar[2], Dr. Muhammad Asif Habib[3], Adeel Ashraf[4], Muhammad Burhan[5]

[1]Research Associate Department of Computer Science, National Textile University Faisalabad
[2,4,5]Department of Computer Science, National Textile University Faisalabad
[3]Assistant Professor Department of Computer Science, National Textile University Faisalabad

Received: January 23, 2014
Accepted: April 27, 2014

ABSTRACT

In networks selecting the shortest path and sending data over that path is called routing. The path selection can be done either manually or through some routing protocol. There are many protocols that are used for routing like Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and Border Gateway Protocol (BGP). RIP, OSPF, and EIGRP which are used for routing within an autonomous system. BGP is used for routing between two or more autonomous systems. This paper describes the working and current issues of routing protocols. This paper describes protocols working, scenarios that describe the efficiency or inefficiency of protocols, and the protocol's best selection for a particular networking environment. The study shows the flaws in these protocols which can be minimized with the help of some new algorithms and techniques.
KEYWORDS: Routing Protocols, RIP, OSPF, EIGRP, BGP, Overview of Routing Protocols.

I. INTRODUCTION

In Computer Networks, the data sent from source to destination needs a specific path. There are number of paths in a computer network for communication between the nodes, and the selection of a shortest path from those paths is one of the key issues. The appropriate path selection can be done by applying routing protocols. Routing is an umbrella term for the set of protocols that determine shortest path for sending the data over the network. Routing selects the shortest path from source to destination and then send data on that shortest path. Data is routed from source to destination and between multiple networks through a series of routers.

The Routing protocols enable routers to build up a routing table that associates the final destinations with next hop addresses. Routing can be done through two ways: first is static routing and second is dynamic routing. The router sends data on the shortest path defined in its routing table. The manual selection of path in a router is called static routing and if the path selection is done on the basis of a routing protocol (for example RIP, OSPF and EIGRP etc) then this type of routing is called dynamic routing. Dynamic routing is efficient than static routing because it automatically adopts the topological changes happened in the network. An usual objection against static routing is that it is hard to administer. This objection is valid for medium to large scale networks but it is not valid for small networks with few or no alternative routes. The dynamic routing is done through protocols called routing protocols. The dynamic routing have two types of protocols, first is Interior Gateway Protocol (IGP) and second is Exterior Gateway Protocol (EGP). The protocols that run within an autonomous system are called Interior Gateway Protocols (IGP) and the protocols that run among two or more autonomous systems are called Exterior Gateway Protocols (EGP). In context of routing, an autonomous system has a single routing policy. In dynamic routing, we have three IGP routing protocols that are RIP, OSPF, and EIGRP. On the other hand, we have one EGP protocol named as BGP.

This paper describes the working of routing protocols. Rresearchers have worked a lot by using these protocols like improvement in efficiency, security, and efficient path selection etc. It also describes the positive and negative aspects of routing protocols, and issues with possible solutions given in various papers.

Corresponding Author: Muhammad Umar Aftab, Research Associate Department of Computer Science, National Textile University Faisalabad. Email: ms.umaraftab@yahoo.com

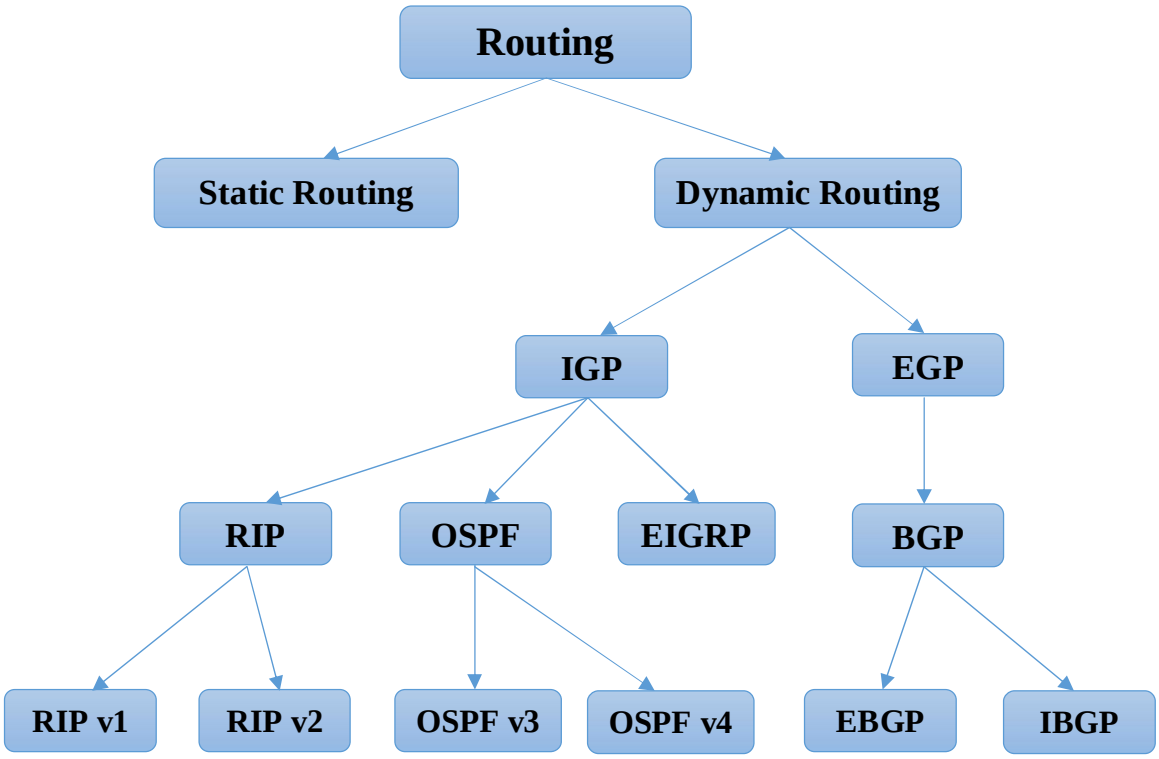

Figure 1: Routing Protocols Tree

II. INTERIOR GATEWAY PROTOCOL (IGP)

It was discussed earlier that IGP protocols are used within an autonomous system (AS). There are four IGP protocols that are discussed in this section.

A. Routing Information Protocol (RIP)

RIP belongs to the family of IGP (Interior Gateway Protocol) that shares routing information within an AS. RIP is based on the algorithm known as “distance vector (Bellman-Ford) algorithm ".
First time this algorithm was described by Ford and Fulkerson [1]. That is why this is also called as Ford-Fulkerson algorithm. Formulation of this algorithm depends upon the Bellman’s equation. This equation shows that this algorithm is based on the dynamic programming [2].

RIP is used in IP based internet. The internet is a collection of networks which are connected with each other by gateways. The types of networks may be as simple as point-to-point or complex as Ethernet and ARPANET. IP datagram has been used to show gateways and hosts. Routing is a technique by which gateways decide the location of destination for transmission of datagram. If the sender and receiver are directly connected with the router then they can send data directly and when they are not directly connected then the router use routing table, for checking that which path is closer to destination to send the datagram. In other words we can say that working of routing protocols is that it provides the information which is required for routing.

A routing protocol that based on distance vector (Bellman-Ford) algorithm is used for routing computation in networks from the time of early days of ARPANET. The testing packet format and protocol described is based on the program "routed” that integrated with Berkeley sharing of UNIX. It becomes de-facto customary to swap routing information amongst gateways as well as hosts. This is helpful as an “IGP". According to countrywide network, it is not possible that is the same protocol will be used for the entire network. The network will ordered as a group of "autonomous systems (AS)". In general, an AS will be administered by a distinct entity; every AS holds its own routing technology. It will vary AS to AS. “IGP” will be referred by the protocol used within an AS [3].

There are two Versions of RIP, RIPv1 and RIPv2 [4]. RIPv1 supports the class full addressing but it does not support subnetting for IP addressing. RIPv1 does not include the (VLSMs) "variable length subnet masks".
RIPv1 shares updates by broadcasting packets to an address 255.255.255.255. RIPv2 supports the classless addressing and so it supports the subnet mask in its routing table updates. RIPV2 includes the VLSMs completely. Thus this allows discontinuous networks and accommodates varying subnet masks.
Some other features included in Version 2 are: send the routing updates by using the multicast address 224.0.0.9 which is used by it for multicasting between RIP version 2 routers [2]. All Cisco routers by default are configured to RIPv1. So, if they are to be configured for RIPv2 then this information will be updated into the routers manually.
RIPv1 has some limitations because it might not be suitable for each routing problem.
Some of the limitations are described below as:

- This protocol is not suitable for large networks; because it supports networks maximum up to 15 number of hops.
- This protocol is not suitable for situation that focused on "counting to infinity".
- This protocol uses fixed metrics to calculate the routes [5].

The working mechanism of RIP is as follows. Router creates the list of directly connected network nodes. This information is advertised on all enabled interfaces of the router. Any router that is connected to interface of advertising router receives this table and copies this information into its own routing table and forwards this information to next. This process makes sure that all routers become aware of each other. In case the router doesn't continue sending its advertisement, eventually there will be "time out" and will stop sending packets [6].
Router has a property called metric (distance). After receiving advertisement, router increments metric. Metric is also called hop count. A router may have more than one route between two network nodes & in case of more than one route the router will prefer shortest path for the transmission purpose [7].

In case of selecting shortest path, the router selects the path with lowest metric (hop count). Maximum value of metric can be 16 towards destination. The destination will be unreachable if router has more than 15 nodes between source and destination. In case of any change in its routing table the router immediately updates its neighbors. This process of advertisements will be executed again and again. In case the router finds any node unreadable it immediately updates its neighbors to optimize the performance of network [7, 8].

The recent developments in Ad-Hoc networks have led to extensive research in routing protocols which include Reactive routing protocols and Proactive routing protocols. The routing protocols define the scheme to forward data (packets) from source node to destination node. These protocols vary from each other on the basis of examining, maintaining and retrieving the routes or path. One of the major concerns in Ad-Hoc networks is how to conclude which of the routing protocol is optimal and fulfills the requirements of an application regarding some criteria. RIP represents the proactive routing protocols and reactive routing protocols were represented by Dynamic Source Routing (DSR). Performance metrics were energy consumption, jitters, end-to-end delay and throughput. Evaluation based study on QualNet simulation showed that RIP performed better than the DSR [9]. The security of the routing protocols can be increased by applying access control. There are different access control models that secure the organization in an efficient manner. Researchers suggest different theories for the secure access in an organization, enterprise and institutions etc. Role Based Access Control (RBAC) is the most popular access control model that enforce the policies with the help of roles [10]. RBAC provides the efficient management of permissions with the help of roles and users in an organization can also be managed with the help of organizational unit (OU) [11]. So, the merger of access control models with routing protocols can give a secure environment for fast and secure packet sending.

One of the major issues in Wireless Sensor Networks (WSNs) is the consumption of energy. WSNs should provide optimal performance and consume less energy. Researchers investigated and analyzed the effect of receiving energy on nodes and remaining energy in the wireless sensor networks. Examination and simulation results showed that varying the receiving energy had significant impact on the life time of network. A new approach was proposed for optimizing energy consumption in wireless sensor networks that assures the maximum life time of nodes while transferring a data packet from the source to host. It could be deployed by avoiding or excluding nodes which have a minimum remaining battery power. This approach was implemented by introducing a threshold value on every node and transmitting the same length data packet on the route. The threshold value indicated whether the node should be involved in making routing choices for a data packet and the length of the packet should be considered for equal energy consumption. Broad simulation results were conferred to confirm the effectiveness of the proposed approach. The behavior of three routing protocols in wireless sensor network (WSNs) was studied. Wide-ranging simulations were done on OLSR, RIP and Fisheye in determining the network lifetime

at different network load and at different node mobility. Simulation outputs suggested that OLSR is the most efficient protocol in terms of energy as compared to other protocols [12].

B. Open Shortest Path First (OSPF)

OSPF is a link state protocol. It is commonly used in IP networking. It is one of the best suited protocols for large networks under IGP. Its metric is link costs (bandwidth), for the determination of best path. The RIP is suitable only for small network because it has some limitation like limit of hop count is 15 and it does not support sub netting. On the other hand, the EIGRP have number of new features but the main drawback of EIGRP is that it is cisco proprietary and suitable only for cisco devices or routers. But OSPF does not work on hop count, it works on the cost of link as well as it supports sub netting. First word 'Open' in OSPF shows that it is open for every vendor like Cisco, Juniper, and Motorola etc. So, it shows that it is not a cisco proprietary like EIGRP. OSPF have major benefits over the distance vector protocols, like RIP and on other protocols, which are listed as below:

- It works with the use of areas that reduces the effect on CPU and memory.
- Fully supported classless behavior
- Uses multiple paths efficiently by equal-cost load balancing.

The main theme of OSPF is the division of autonomous system (AS) in multiple areas for better resource utilization, easy administration, and traffic optimization. The size of area depends on the discretion of administrator. If administrator designs the areas in such a way that there will be no backbone for areas then routing loops will be generated. For the avoidance of loops, a backbone area is used in OSPF through which every non-backbone area sends its information to other non-backbone area. If the information is only for the router that already exists in its own area then the information will not be sent to the backbone area. So, this type of information sending will reduce the traffic on the link and obviously, it will be a step towards bandwidth utilization in an efficient manner. The non-backbone area is called regular area. The combination of backbone and regular areas will create an organized network.

OSPF works on the state of link and calculates the cost. The cost calculation is done with Dijkstra algorithm or shortest path first (SPF). The main theme behind the cost calculation of OSPF is: bandwidth that is inversely proportional to the cost. So, more bandwidth will give us less cost. A path that has less cost will be selected as best or shortest path.

Every router in OSPF has the idea about the cost of the path between two directly connected neighbors. After calculating the cost the router transmits that information to all other routers in its area so that every router of every area has the complete shortest path information about its area. The central and major area in OSPF is area 0 which is also called backbone area. All the routers communicate through area 0. The area 0 routers have the information of their area and other areas. All these routers make a complete network in which they have shortest path information for moving towards any router or node. When the routing tables of all the routers are completely filled in a network then that network will be called fully converged network in which we have shortest path for every router [8]. OSPF works on incremental or trigger updates. If a new path is added for another router, then the OSPF has to send that information to other routers or areas as well. It will only send the updated route for the specific router (that is added) instead of sending full routing table again. This decreases the load on the bandwidth unlike some other protocols.

OSPF that uses ipv4 is called OSPFv2 and that uses ipv6 is called as OSPFv3. OSPFv3 has an advantage over OSPFv2. The processing of protocol in OSPFv3 is done on link instead of per subnet. It also supports multiple instances per link. In wireless networks we have ipv6 addressing in its network for communication and the network gets the maximum efficiency by using the ipv6 addressing scheme. OSPFv3 is the best option for the small workspace in a congested environment. It works in an efficient manner for congested environment with fewer costs [13].

Traffic engineering concept is most widely used now a day. In traffic engineering we utilize the link capacity of the network in a good manner and share the load of the link. Usually traffic engineering is done with Multi-Protocol Label Switching (MPLS) but the challenge is to do the work like MPLS in an OSPF network, through OSPF. The researchers introduced the concept of smart-OSPF. According to this concept, the packet is sent from source to destination by keeping in mind the link utilization and load balancing concept. The source node sends packets to all its neighbors except its ancestor for avoiding loops. The division of packets will be performed on the source node and all other nodes will forward the packets according to OSPF shortest path criteria. As the OSPF does not support flexible routing of packets. So the S-OSPF provides the load division between various links and all links are properly utilized by using Linear programming Formulation (LPF). Basically LPF is an algorithm used for proper link utilization. The major constraints that will apply in that algorithm are the constraint on all

intermediate nodes to route the packets according to OSPF shortest path criteria and routing of packets to ancestor node for the avoidance of loops [14].

Most of the Interior Gateway Protocols (IGP) use dynamic cost like bandwidth, utilization rate, and time delays. As the OSPF uses bandwidth as a cost and transmit its packets on the shortest path having less cost. It does not bother that either the path is congested or not. It just transmits its packet on the path having low cost. That is obviously a drawback. A solution for this is the use of HELLO algorithm. In this algorithm, the cost of link is calculated dynamically but this algorithm was instable. The routers count time delay as metric for cost. Heavy traffic is transmitted over such a path that has less delay. The drawback in this algorithm is the oscillation of traffic that leads to a big delay as compared with the normal OSPF. The suggested OSPF algorithm, reviewed under the study, counts the cost as a static cost. It selects paths for the transmission that leads to decreased delay and traffic on the network is also balanced through it. Also no extra memory is required for this algorithm. It does not send extra packets for doing this job [15].

The routers that enable OSPF for routing within an autonomous system send "Hello" packets after a specific interval. The "Hello" packet tells other routers that "I am alive". Every router sends Hello packets to other that are in its area or adjacent to it. These types of packets increase the load over the CPU and utilize the bandwidth in a big amount just for these packets except the transformation of original information. A new concept is introduced named type of service (TOS), for increasing the efficiency of OSPF. In this concept link state advertisement (LSA) flooding is controlled on parallel links. In OSPF packets are sent on the shortest path but TOS sends packets on the path that have less load instead of shortest path. This technique decreases the load of CPU and utilizes the bandwidth of all links. Also OSPF-Traffic Engineering (OSPF-TE) is introduced that works on virtual trunks. A virtual trunk is created by the criteria set by the administrator that can include initial bandwidth, type and class of traffic. Virtual trunk shows the best link. This approach is another success towards proper resource utilization and load sharing [16].

A highly available OSPF (HA-OSPF) router consists of two OSPF router units that have been dedicated for supporting and maintaining high availability networks. A few services incorporated into the high availability management (HAM) middleware that are interface monitor, checkpoint, fault handler, Availability management framework (AMF) and OSPF fault manager. These are intended to support and capture state information trade, health check and takeover system in HA-OSPF router. The experimental outcomes have proved that HAM middleware is extremely helpful in system recovery and failure detection. HA-OSPF modules have also been implemented on the Advanced Telecom Computing Architecture (ATCA) control cards. The ATCA offers an industrialized standard modular architecture for a flexible, reliable and proficient router design. The average takeover delay of the ATCA HA-OSPF router is calculated as about 131 ms for a software failure and in case of hardware failure, it is 331 ms [17].

A comprehensive study of stability issues regarding OSPF routing has been carried out under secure and stable conditions. Three stability indicators are described, that includes routing load on processors, network convergence time, and the number of route flaps. All the experiments have used a model tool support by a realistic OSPF implementation and a complete processor model from an available vendor router. A statistical study on three different scenarios was also performed to enhance the working visibility. The network topology used matches with slight adjustments to an actual ISP network having 765 links and 292 nodes. Insertion of Traffic Engineering (TE) extensions to OSPF protocol does not significantly modify the OSPF stability [18].

Routing protocols are devised considering that in network; each node ought to be able to reach i.e. send or forward packets to every other node. This routing protocol faces some challenges like Denial of Service (DoS) attacks and spam launching. The "blocking option" in routing protocols is being proposed which permits a node to block a particular set of nodes and stop each of the nodes from reaching that node. If a node blocks a large number of nodes, subsequently it may end up obstructing other nodes too. These unintentionally blocked nodes are referred as blind to that particular node. Thus, a node will not be able to communicate with the blind nodes in usual way. The routing protocol has been extended to allow this aspect by an additional intermediate node i.e. joint node. This node will not be blocked by any of the nodes. An algorithm has been demonstrated to find the best and most suitable joint node. After simulating the algorithm, it has been concluded that the chances of a joint node being blind is fairly small, ranging from 10^{-3} and average number of blind nodes is almost zero when the average number of blocked nodes is < 20 [19].

There are many Ad-hoc routing protocols that are used for Mobile Ad-hoc Networks (MANET) like Dynamic Source Routing (DSR), Ad-hoc On Demand Distance Vector (AODV) and OSPF-v3 etc [20]. Researchers simulate the results and analyze all the routing protocols of MANET and present the performance analysis to describe the protocol's working for various environment and scenarios. OSPF is implemented on large scale all-over the world for various types of networks like wide area networks and MANET etc. In MANET, an issue is always there about the selection of a particular routing path because the selection of routing path is easy but that

path must not be congested. The load balancing during routing is an important task, so that data packets should reach the destination more quickly or without any delay. Load balancing mechanism can facilitate the distribution of network traffic among different appropriate paths [21].

C. Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is built by enhancing IGP. EIGRP uses same technology of distance vector as it is implemented in IGRP without changing the distance information. The point where EIGRP differs from IGRP is its convergence property and the working efficiency of the protocol. The improvement in convergence property of EIGRP is because of the Diffusing Update Algorithm (DUAL) which the research work is done by SRI (Stanford Research Institute) International. It is DUAL that provides the loop free environment at every level during path calculation [22]. DUAL is also responsible to synchronize all routers in real time whenever a topology change occurs. EIGRP achieves maximum efficiency level by avoiding useless operations such as involving only those routers in computation which can be affected by the change of topology. DUAL provides the best convergence time among all existing protocols.

There are four building blocks of EIGRP that includes Neighbor Discovery or Recovery, Reliable Transport Protocol, DUAL Finite State Machine, and Protocol Dependent Modules. With Neighbor Discovery or Recovery, the routers process and store the information about other routers that are directly attached with them. The routers keep track of information that includes the time when neighbor routers are out of access, link failure, and when neighbor routers are working efficiently. This information tracking is done with the help of special packets called "Hello" packets which are multicasted by routers in a periodic manner. For acknowledgment (Ack) the same "Hello" packet with no data is sent out. It is important to know that Acks are always unicasted. Now as far as a router is receiving "Hello" packets, it comes to know that the neighbor is active. When it does not receive "Hello" packets from its neighbor routers it assumes that neighbor is unavailable. In EIGRP, the routers exchange their routing information after creating all neighbor links [22].

For the computations of all routers DUAL automaton exemplifies the decision process. DUAL monitor all routers which are advertised via the neighbor routers. Almost all other distance routing protocols have a metric, in the same way EIGRP also have metric named as distance information, which is used by DUAL to compute the paths without any loop [23]. The selection of routers to be inserted in to routing table is done by DUAL on the basis of the feasible successors. The routing table of EIGRP maintains some parameters to compute the metric i.e., bandwidth, delay, load and reliability. Feasible successors are such type of neighboring routers that can forward packets to a destination at minimum route cost with a guarantee that it is not a part of any routing loop [24]. If no feasible successor is found and neighboring routers are advertising the destination then there will be re-computation. During this process the new successor comes into existence. The time for re-computation affects the convergence time of EIGRP. To avoid re-computation and making EIGRP efficient, the DUAL selects any of the feasible successors when topology change occurs and more than one feasible successors will be available. Protocol dependent modules handle the requirements that are protocol specific like IP or IPX.

There are five types of packets that are used in EIGRP i.e., Hello/ Ack, Updates, Queries, Replies and Requests. We have discussed Hello /Ack earlier in neighbor discovery and neighbor discovery process. The update packet conveys the information about reachability up to destination. Update packets are communicated whenever a new neighbor is found creating the topology table of router. It is important to note that update packets are unicasted topology tables are created. But in another situation whenever link cost changes, these packets are multicasted. When a destination router enters into active mode the Queries and replies are sent. When queries/replies communicate as a response to a query/reply, it is unicasted but in all other cases it is always multicasted. Replies tell the query sender that it has feasible successors so do not go into active state. When a router needs some specific information from the neighbors then they send request packets. Request packets are sent in both multicasting and unicasting ways [25].

In EIGRP every router has the information about the state of neighboring routers. In the result of addition of a new neighbor, the routers record the address and interface information of that new neighbor. All this information is noted in the neighboring tables. Every protocol dependent module has one neighboring table. After sending a hello packet, every router waits for acknowledgements up to a specific time which is usually three times greater than the sending time of hello packets. This time is called as "Hold Time" or we can say that this is the time interval when the router considers neighbors as available and operational. A topology change is informed to the DUAL on the expiry of Hold Time. Information required for the reliable transport process is also provided by the neighboring tables. To detect order packets, sequence numbers are assigned with data packets and matched with acknowledgments as last sequence number is stored.

It has been observed that by implementing the EIGRP on top of the Maude infrastructure the casual description in the previous model was formalized. Researchers presented specifications in executable by using a rewriting

logic in Maude which allowed them to associate many operational instances of the protocol and with the execution of existing applications on the top. They also used EIGRP in Instantaneous Maude, which allowed them to analyze their protocol in several ways. Size of the messages is less in EIGRP as compared to other routing protocols. They concluded that the performance of Maude type applications is inversely proportional to the fact that messages to be sent are required to be interpreted into strings and return the messages when received. Furthermore in order to make user free from providing actual translation functions each operator deteriorates this act. They found the simplification with the use of reflective aptitudes of Maude. They noticed that to convey the overall terms, the actuality in Maude of a sent operator at the socket level resolved this problem [26].

The VoIP provide too much assistance to service providers but the implementation of VoIP based application on an enterprise network is still challenging. Routing is necessary to provide instantaneous data delivery that is demanded from VoIP. An enterprise scale network with OPNET Modeler established to analyze the three basic protocols IGRP i.e., RIP, OSPF and EIGRP. In order to measure the performance of various protocols, various standardized simulators were developed. The results showed that RIP performed very badly in a bottleneck data communication pattern because RIP ignores the bandwidth. On the other hand EIGRP and OSPF performed greatly because they are dedicated to calculate the route in a fastest way. Some results showed that for VOIP applications, EIGRP and OSPF both calculated almost the same paths when the network specifications are same. In both OSPF and EIGRP the failure of links affected the performance. In auto recovery process OSPF showed consistency but EIGRP was totally messed up during this process but it retains the actual level of performance after recovery process. To recalculate the new path, OSPF updated the routing table with the network failure, and did not change the operational route as far as some problem occurred in it. The results described that the OSPF based networks are fruitful for VoIP based applications as OSPF showed constant behavior during failure. When there is no feasible successor for DUAL, the OSPF performed well in that condition. The final conclusion describes that for enterprise network with OSPF is effective to support VoIP characteristics [27].

The researchers analyzed the suitable environments for RIPv1, RIPv2, OSPF and EIGRP protocols as well as they also compared their main characteristics [24]. They actually studied the traffic behavior during the implementation of these protocols. The environment that they established is consisted of three computers attached to each other. The personal computer PC A was the starting node, PC B was the destination node and the PC C was in between both A and B. They used same network strategy for all protocols to make the process standardized. They found that in the sense of convergence the EIGRP was at top, OSPF was first runner up and RIPv1 performed worst. So they suggested that if we have critical network, EIGRP must be applied as its convergence was best among all. About OSPF they found that it is routing protocol that gives minimum downlink and uplink bandwidth feeding and on contrary protocol with average downlink and uplink bandwidth usage was RIPv1. So it is being recommended that OSPF must have to be applied when constraints exist on bandwidths of links. When peaks of packets per seconds is not our desire then it is suggested that one of the protocol from OSPF or PIRv1 is to be used as both give lowest mean numbers of packets per second. On the other hand the EIGRP has great average of number of packets per second. They found through their research work that RIP should not be used when there is a limitation of bandwidth as RIP is highly unstable routing protocol in sense of the number of bytes per second [28].

In theoretical and practical Analysis of EIGRP and OSPF, the theoretical study found that in spoke topology and hub, EIGRP scales quite efficient than OSPF. To verify theoretical results they performed it on simulation which confirmed the results. Mostly in EIGRP hubs or networks, on a low bandwidth a pair of hub router connects more than 300 remote sites. But the OSPF connects 200 remote sites with higher bandwidth. So the final analysis describes many advantages of EIGRP over OSPF in the hub and spoke network such as efficient convergence, increased scalability, and proper usage of CPU and router memory, and intelligent bandwidth control. They observed while calculating the rate at which it transmits updates, the EIGRP takes the available bandwidth into consideration. To use maximum amount of bandwidth, even while calculating routing topology, interfaces can also be configured and a specific area of the link capacity remains available for data transmission [29].

OSPF proceeds bandwidth concern while computing the cost of routing path on which data will be transmitted. EIGRP can be configured for computing optimal route, the usage of proper bandwidth, load, reliability and delay. Timing issues are greatly tackled by EIGRPv4. EIGRP is not difficult in case of configuration and administration[30].

III. EXTERIOR GATEWAY PROTOCOL (EGP)

EGP is used for the communication between two or more ASs. It consists of only one protocol that is BGP.

A. Border Gateway Protocol (BGP)

Autonomous Systems need to distribute their routes information. They used a protocol name BGP for this purpose. Each AS (Autonomous System) has border routers i.e. ASBR (Autonomous System Border Router) to

exchange data i.e. data enter and leaves an AS through these routers. Also each AS has a router namely "BGP speaker" which communicates with other AS's BGP speakers via BGP. An AS can serve as transit service for other ASs, if it has BGP speakers.

Border routers learn a lot of information from outside networks and then they have to distribute this information to inside routers. Thus, distribution complicates the network design and makes difficult for these routers to calculate the best path to anywhere outside router. Border routers have to speak BGP for inter-domain communication but it would also be unwise to speak BGP to internal routers who work conventionally on direction-vector protocols or link state protocols. For an effective intra-domain route information distribution, border routers make BGP sessions termed "iBGP" (interior Border Gateway Protocol) sessions with inside routers. Interior routers then use this information to calculate "best" paths. An iBGP neighbor in an AS should have: the same AS number and a defined route and reachability. While, there are few BGP attributes that are used. The MED known as Multi Exit Discriminator, is an indicator to preferred path. It tells a router which entry point is preferred. If there are two or more options for a routing path then the path with minimum value will selects for sending packets. Another attribute is LOCAL_PREF which tells iBGP peers the best way to get out to a different AS. From BGP's perspective this mechanism is used to prefer one equal path over the other.

The AS path provided in BGP is inefficient in detecting routing loops that occur during iBGP sessions within that AS. Thus, an iBGP peer will not advertise a route it has learned from another iBGP peer to any other iBGP peer. To prevent looping, all iBGP peers are fully meshed. Logically this means that every iBGP router must have a peer with every other iBGP router which is also not a good strategy. In this strategy, n^2 peering mesh requirement directs to one of the most important routing scaling issues with ASs and BGP. Thus, BGP peering sessions of this mesh may go beyond the capacities of the routers. As soon as the iBGP mesh becomes huge, then alternative structures should be implemented. Some modifications can be brought into the configuration of iBGP. When networks get adequately large enough, then adding a new BGP speaker (router) means it has to be connected to every other router. This is another issue of iBGP. To solve this issue, route reflectors or confederations are usually used.

In confederation an AS is broken down into small parts internally, known as sub-autonomous systems, which are then tied together with the external BGP. It is a lot of hassle, configuring confederations. Route reflectors are more effective than using these. Route reflectors are iBGP routers which re-advertise routes to other iBGP routers. Clusters of iBGP routers are created and connected with a reflector. Moreover, a reflector sends the best paths to its peers rather than sending every route.

Routing oscillations within an AS have been detected over the past few years. These oscillations bring in redundant routing updates, causing workload on routers and thus degrading the network performance. IBGP is configured by a single network operator using simple rules. Two refinements, have been presented to prevent iBGP oscillations, which are proved algebraically. First one, "minimum iBGP hop-count" is implemented in decision process of iBGP. A minor change has been done to the step which is used to select best paths or routes. This change has been done on route reflectors, not on the network and it might defy the semantics of the attribute MED. While, second modification to iBGP, is related to distribution (propagation) of additional routes from each router. Mathematical approach has been used for this modification to determine additional routes while maintaining the routing stability and routing flexibility [31].

Configuration languages of BGP permit AS border routers to alter the iBGP attributes that are related to the route selection process. Possibilities of altering iBGP attributes have been investigated. Then advantages of altering these attributes have also been discussed while a famous model related to iBGP stability has been extended to maintain the attributes changing within a network provider. A statically implementation of a tool to check the configuration of iBGP stability consequently, detecting the routing oscillations. It has also been analyzed that altering iBGP attributes let oscillations arise that might not occur otherwise. Instructions to configure iBGP attributes in a beneficial way have also been proposed [32].

Distributed approach is used for routing in IP networks. A new approach has been proposed that isolates the procedures (routing table and traffic forwarding) into two planes i.e. two remote hardware. The routing information issues regarding diversity and visibility have also been tried to solve. Separation of these tow processes reduces the routers overhead of the (BGP) routing process. In comparison to the recent BGP routing, this proposed design helps in issues related to parallel calculation of routes while undertaking the scalability problems [33].

A reliance graph model has been offered to check the dependency of route selection among routers. IGP distances and iBGP topology are used as inputs in the model. The model helps in calculating, the set of routes selected by all routers efficiently, regardless the configuration of iBGP. This model also works even when incomplete routing information is offered. Effectiveness of the model has been demonstrated by implementing it to a Tier-2 having more than 220,000 network prefixes. Using this method a proper and constant solution was

given even with the 15% routing information in some cases. The graph model has not effect on it by IGP distance or iBGP configuration. These features are supposed to permit this method to work [34].

May be it appears too complex and even routing protocol designers are not well aware about defects that cause iBGP routing anomalies. These defects have been described and analyzed to support in protocol designing to verify the consistency and revealing the possible problems that may occur. Five core defects have been described on the basis of inconsistent routing, cost-sub-optimal routing, and robustness routing problems. Route reflection and Full-mesh were illustrated by exemplifying while verifying the proper behavior and liability to an inconsistency [35].

Often it has been observed that table transfers in routing are slower and ultimately this transformation of routing tables affects the network performance. A comprehensive study and an organized experiment has been performed to explain delays in transfer by merging the BGP messages collected from a VPN backbone and three different router models. Results have illustrated that there are gaps in table transfers, in both controlled experiments and VPN. Gaps mean no (BGP) routes are exchanged; sending router and receiving router both remain idle in this situation. Also these delays are caused by exploiting time-driven implementations in sending of BGP messages. Event-driven implementations may help in speeding up table transfers. Though, for quicker table transfers or in favor of more organized router load, it all depends on aspects like the network design and nature, the number of BGP neighbors, the number of routes, or the capacities of routers [36].

Numerous anomalies are caused by faulty propagation of iBGP routes. Several unanticipated side-effects like traffic black-holes and forwarding loops are present in iBGP. Propagation precision property is defined, simulating the routers capabilities to learn single route to each destination network, in any situation. By differentiating, propagation correctness and already offered accuracy properties, counter examples invalidate a few results in the literature. Moreover, making a decision on whether configuration of iBGP is computationally difficult and not traceable. Yet it is more difficult, to conclude and calculate whether adding up a single iBGP session is capable of badly affecting the propagation precision of an iBGP design. Lastly, adequate provisions that guarantee precision of propagation have been provided [37].

Neighbor-specific BGP (NS-BGP) is being presented as an addition to the BGP enabling a variety of local guidelines regardless of global routing stability. Where an existing BGP speaker (BGP router) chooses a single "best" route, Neighbor-specific BGP permits a router in customizing the route choice on behalf of every router who is its neighbor. It's proven that flexibility of NS-BGP is certain to be consistent if there are fewer limitations on ranking the candidate routers. How Neighbor-specific BGP can be implemented by individual Autonomous Systems separately with no alterations to the format of BGP message or neighboring AS's collaboration [38].

Inter-domain routing protocol BGP's convergence time can proceed to almost 30 minutes. But still, routing performance during convergence of BGP route is inadequately implied. During convergence of BGP route, there can be reachability loss in a continuous Internet route. This loss is referred as "transient routing failure". These can cause packet/data losses, and extended packet loss disintegration can make the applications performance inappropriate. How these failures can occur has been discussed using a proper model which checks these failures of BGP, and several conditions have been derived in which these failures can crop up. To improve the stability and performance of their network this analysis can be applied by network administrators [39].

Interior Border Gateway Protocol (iBGP) nodes are not able to reflect echo routes. Thus, these nodes must have iBGP sessions with all AS Border Routers. Router reflectors were extensively implemented to avoid full-mesh, a key to lessen the number of iBGP sessions required and in order to increase the scalability of an AS. The PC-iBGP i.e. Partial Complete iBGP is being proposed as another option to the conventionally used approach route reflection. In Partial Complete iBGP, nodes are able to reflect nodes. It helps in reducing the clustering and sets up iBGP sessions only amongst neighbors which are at single hop distance. It's been proven that Partial Complete iBGP has satisfactory accuracy provisions in addition to this it is good against oscillations and failures [40].

IV. CONCLUSION

We conclude from various articles that routing protocols work efficiently in various circumstances by applying various techniques but they also have some flaws. These flaws can be covered by applying little changes in the old routing techniques. OSPF for example has some deficiencies for load sharing and proper utilization of bandwidth of all links and these deficiencies can be covered by applying traffic engineering and MPLS. The notion of this research paper is to review routing protocols and contributing with the concept of traffic engineering and load sharing for the proper utilization of resources on OSPF.

REFERENCES

[1] R. Braden and J. Postel, *Requirements for Internet gateways*: ISI, USC Information Sciences Institute, 1987.

[2] C. L. Hedrick, "Routing information protocol," 1988.

[3] G. Malkin, "Routing Information Protocol Version 2," RFC 2453, SRI Network Information Center1998.

[4] L. Ford and D. R. Fulkerson, *Flows in networks* vol. 3: Princeton Princeton University Press, 1962.

[5] G. Malkin and F. Baker, "RIP version 2 MIB extension," 1994.

[6] D. P. Bertsekas, R. G. Gallager, and P. Humblet, *Data networks* vol. 2: Prentice-Hall International, 1992.

[7] J. Doyle and J. Carroll, "Routing TCP/IP, vol. 1 of CCIE Professional Development," ed: Indianapolis, IN, USA: Cisco Press, 2006.

[8] L. L. Peterson and B. S. Davie, *Computer networks: a systems approach*: Elsevier, 2007.

[9] Z. G. Al-Mekhlafi and R. Hassan, "Evaluation study on routing information protocol and dynamic source routing in Ad-Hoc network," in *Information Technology in Asia (CITA 11), 2011 7th International Conference on*, 2011, pp. 1-4.

[10] M. A. Habib and Q. Abbas, "Mutually exclusive permissions in RBAC," *International Journal of Internet Technology and Secured Transactions*, vol. 4, pp. 207-220, 2012.

[11] M. U. Aftab, A. Nisar, M. Asif, A. Ashraf, and B. Gill, "RBAC Architectural Design Issues in Institutions Collaborative Environment," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, 2013.

[12] D. Vir, S. Agarwal, and S. Imam, "A Dynamic Approach to Optimize Energy in RIP, OLSR and Fisheye Routing Protocols using Simulator," *Energy*, vol. 2, 2013.

[13] G. Merlin Sheeba, A. Nachiappan, and P. Gokulnath, "Improving link quality using OSPF routing protocol in a stable Wi-Fi mesh network," in *Communications and Signal Processing (ICCSP), 2012 International Conference on*, 2012, pp. 23-26.

[14] A. K. Mishra and A. Sahoo, "S-OSPF: A traffic engineering solution for OSPF based best effort networks," in *Global Telecommunications Conference, 2007. GLOBECOM'07. IEEE*, 2007, pp. 1845-1849.

[15] P. Liu, R. Sun, and Z. Yan, "Dynamic OSPF protocol," in *Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on*, 2011, pp. 51-55.

[16] K. Shuaib and F. Sallabi, "Extending OSPF for large scale MPLS networks," in *Advances in Wired and Wireless Communication, 2005 IEEE/Sarnoff Symposium on*, 2005, pp. 13-16.

[17] C.-T. Tsai, R.-H. Jan, C. Chen, and C.-Y. Huang, "Implementation of highly available OSPF router on ATCA," in *Dependable Computing, 2007. PRDC 2007. 13th Pacific Rim International Symposium on*, 2007, pp. 147-154.

[18] A. Basu and J. Riecke, "Stability issues in OSPF routing," in *ACM SIGCOMM Computer Communication Review*, 2001, pp. 225-236.

[19] Y. Li and M. G. Gouda, "The blocking option in routing protocols," in *Reliable Distributed Systems, 2009. SRDS'09. 28th IEEE International Symposium on*, 2009, pp. 227-235.

[20] S. Naseer, S. Hussain, I. Raza, S. Chaudry, J. Mirza, and M. Raza, "Mobile Ad-hoc Network Routing Protocols: A Simulation and Performance Analysis Using Multimedia Traffic," *Journal of Basic and Applied Scientific Research*, vol. 2, pp. 9925-9930, 2012.

[21] B. Mahdavi, B. Najafpour, H. Mojez, H. Masoomi, and F. Babazadeh, "An Overview of Traffic-Oriented load Balancing Routing Protocols Based on the Multiple Metrics in Mobile Ad Hoc Networks," 2013.

[22] V. Trujillo, J. Expósito, and E. Gamess, "An alternative way of teaching the advanced concepts of the diffusing update algorithm for EIGRP," in *The 2010 International Conference on Computer Science and Applications (ICCSA'10). San Francisco, California, USA*, 2010.

[23] D. Xu and L. Trajkovic, "Performance Analysis of RIP, EIGRP, and OSPF Using OPNET," 2011.

[24] H. Mahini, R. Berangi, and A. Mahini, "MLET: A POWER EFFICIENT APPROACH FOR TCAM BASED, IP LOOKUP ENGINES IN INTERNET," *International Journal of Computer Networks & Communications*, vol. 2, 2010.

[25] G. S. Kalyan and D. V. V. Prasad, "Optimal selection of Dynamic Routing protocol with real time case studies," in *Recent Advances in Computing and Software Systems (RACSS), 2012 International Conference on*, 2012, pp. 219-223.

[26] A. Riesco and A. Verdejo, "Implementing and analyzing in Maude the enhanced interior gateway routing protocol," *Electronic notes in theoretical computer science*, vol. 238, pp. 249-266, 2009.

[27] X. Che and L. J. Cobley, "VoIP Performance over Different Interior Gateway Protocols," *International Journal of Communication Networks & Information Security*, vol. 1, 2009.

[28] S. Sendra, P. A. Fernández, M. A. Quilez, and J. Lloret, "Study and Performance of Interior Gateway IP Routing Protocols," *Network Protocols & Algorithms*, vol. 2, 2010.

[29] N. Poprzen and N. Gospic, "Scaling and Convergence speed of EIGRPv4 and OSPFv2 dynamic routing protocols in hub and spoke network," in *Telecommunication in Modern Satellite, Cable, and Broadcasting Services, 2009. TELSIKS'09. 9th International Conference on*, 2009, pp. 491-494.

[30] D. Perić, M. Perić, and G. Petrović, "Redundant topology in computer network realized with millimeter wave radio links," *14th IST Mobile and Wireless Summit*, 2005.

[31] A. Flavel and M. Roughan, "Stable and flexible iBGP," in *ACM SIGCOMM Computer Communication Review*, 2009, pp. 183-194.

[32] L. Cittadini, S. Vissicchio, and G. Di Battista, "Doing don'ts: Modifying BGP attributes within an autonomous system," in *Network Operations and Management Symposium (NOMS), 2010 IEEE*, 2010, pp. 293-300.

[33] I. M. Oprescu, M. Meulle, S. Uhlig, C. Pelsser, O. Maennel, and P. Owezarski, "Rethinking iBGP routing," in *ACM SIGCOMM Computer Communication Review*, 2010, pp. 411-412.

[34] A. Flavel, J. McMahon, A. Shaikh, M. Roughan, and N. Bean, "Humpty dumpty: putting iBGP back together again," in *NETWORKING 2009*, ed: Springer, 2009, pp. 52-65.

[35] U. Bornhauser, P. Martini, and M. Horneffer, "Root causes for iBGP routing anomalies," in *Local Computer Networks (LCN), 2010 IEEE 35th Conference on*, 2010, pp. 480-487.

[36] Z. Ben Houidi, M. Meulle, and R. Teixeira, "Understanding slow BGP routing table transfers," in *Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, 2009, pp. 350-355.

[37] S. Vissicchio, L. Cittadini, L. Vanbever, and O. Bonaventure, "iBGP deceptions: More sessions, fewer routes," in *INFOCOM, 2012 Proceedings IEEE*, 2012, pp. 2122-2130.

[38] Y. Wang, M. Schapira, and J. Rexford, "Neighbor-specific BGP: more flexible routing policies while improving global stability," in *Proceedings of the eleventh international joint conference on Measurement and modeling of computer systems*, 2009, pp. 217-228.

[39] F. Wang, J. Qiu, L. Gao, and J. Wang, "On understanding transient interdomain routing failures," *IEEE/ACM Transactions on Networking (TON)*, vol. 17, pp. 740-751, 2009.

[40] B. Sarakbi and S. Maag, "Partial complete ibgp," in *Communications (ICC), 2010 IEEE International Conference on*, 2010, pp. 1-5.