International Journal of Data Science and Advanced Analytics (ISSN: 2563-4429)

A Review and Comparative Analysis of Routing Protocols in Network

Daniel Mago Vistro[1], Ishtiaque Mahmood[2], Attique Ur Rehman[3] and Farwa Javed[4]
[1]Asia Pacific University, Malaysia
[2, 4] Lahore Garrison University, Lahore, Pakistan
[3]University of Management and Technology, Lahore, Pakistan
[1]daniel.mago@staffemail.apu.edu.my, [2]ishtiaque.cs@lgu.edu.pk, [3]F2019288002@umt.edu.pk, [4] farwajaved@lgu.edu.pk

***Abstract*— In network correspondence, directing is the way toward moving information across network between various end gadgets. In the network of Local and Wide Area communication is an important aspect. Routings is considered as a significant interaction in network correspondence Router works with routing protocols. Different router used different routing protocols that is used for data communication. Various conventions have various qualities that makes them fit to accomplish efficient communication. According to this different routing protocol is used. The information gets across various organization geographies and various conventions working inside and outside a self-sufficient framework handles this information. Different types of protocols are used in routing procedure. The paper purpose is the give a comprehensive analysis on different types of routing protocols. In this paper, OSPF, RIP, BGP are concerned to be discussed.**

Keywords—Analysis, BGP, RIP, Routing, Protocols, Network, Communication, OSPF

I. Introduction

As we know that communication across network takes place by forwarding messages in form of packets from source to destination. A packet can be defined as single unit of data which is transmitted between two nodes. Transmission control protocol divides the messages into small packets and transfer them across network. A switch is a gadget that joins various network and characterizes the best way to send bundle from source to objective. Routing table is produced inside a router which contains the way data. It uses certain algorithms to find the best path for packet to travel inside the network.

There are numerous paths between two communicating nodes in a network. And selecting the shortest or most appropriate path for packet is a major issue. This task can be achieved by using routing protocols [1]. The terms routing means determining the path and sending packet across that path. Routing protocol is considered as a language router uses or speaks to communicate with other routers. The communication may involve network reachability and status [2]. Between source and destination point a shortest path is selected and packet is forwarded on that path. Data passes through various routers and reach its destination. Router uses routing protocols to generate a routing table [1]. Routing protocol uses various algorithms to work. Further, certain metrics is used to find the best route use different algorithm of router. [3].

Routing tables can be generated using two methods. These methods are as follows.

- Static Routing
- Dynamic Routing

Manual configuration is also used for the creation of routing table that is known as Static routing. In this process creation and maintenance is done by the network administrator [4]. For the establishment of full connectivity, each router must be configuring with the static route to all networks. Static routing does not tolerate any fault.

The following Fig. 1. give a graphical view of routing protocols.

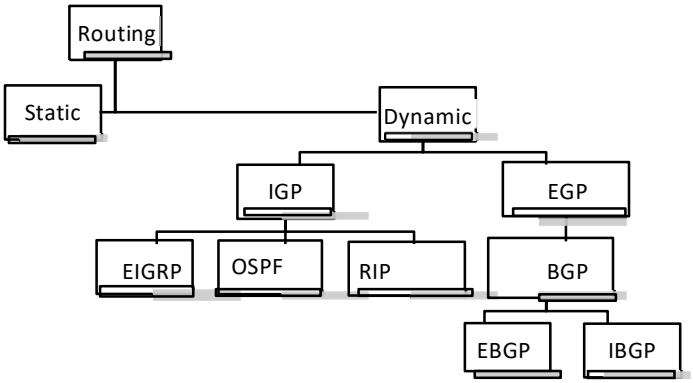

Fig. 1. Network Routing Protocols

In dynamic routing, routing table is updated by using routing protocols. Routing tables are not configuring manually [4]. As dynamic routing automatically adopts the network changes, they are more efficient than static routing [1].

II. Comparative Analysis of Routing Protocols

As per Fig. 1. We have discussed some routing protocols and its comparative analysis with the help o diagrams and literature.

A. Interior Gateway Protocol (IGP)

The protocol is classified as dynamic routing protocol. Different autonomous systems are the union that is possible by internet. An autonomous system is defined as a network which is governed by a single administration. When routing is done within single autonomous system IGP is used. Sender address to receiver address is the path for sending the data across the internet and that information is kept with the help of these protocols.

These are classified as link state routing protocol and distance vector routing protocols. Some examples of IGP includes RIP, OSPF, Extended Interior Gateway Protocol (EIGRP) and Intermediate System to Intermediate System (IS-IS) [5].

B. Extended Interior Gateway Protocol (EIGRP)

It is an improved form of IGP. It works by using distance vector technology. In distance vector routing protocol distance is calculated by using BF algorithm and FF algorithm. The path is chosen by calculating distance and vector direction of next router based on the information provided by the neighboring routers. If a change occurs in topology of network the path is updated by router [2]. The property of convergence and efficiency of protocol makes it different from IGRP. Stanford research institute proposed Diffusing update algorithm (DUAL) which improves the convergence of EIGRP [1].

DUAL is a routing protocol which will compute and generate tables to check whether the route is looped or loop free. Using this algorithm, the router running EIGRP will find alternate path without being updated by other router.

There are four basic parts of EIGRP. These are as follows:

- Neighbor discovery/ recovery
- Reliable transport protocol
- DUAL finite state machine
- Protocol dependent modules

The information about other routers that are connected directly connected with them are processed and stored [1]. Routers will also discover the unreachability and incompatibility of other routers in this phase. Router will send hello message to connected routers and will receive the hello packets from neighbors which will help the router identify that its neighbor is functioning and is alive.

Once the reachability is achieved the routers can exchange the information. The reliable transport protocol will ensure that packets are transferred to neighbor routers. Next the DUAL finite state machine will select the efficient loop free path for transmission of packets. Last the protocol dependent module will handle protocol specific requirements [1].

The Fig. 2. below shows the message format of EIGRP:

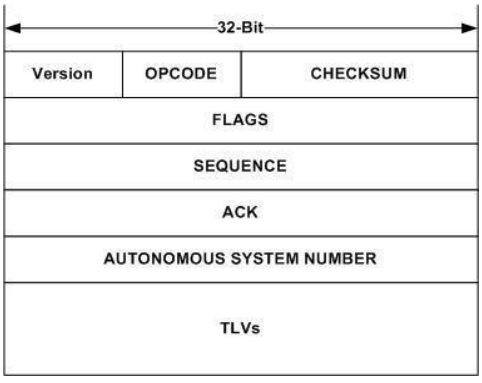

Fig. 2. Message Header of EIGRP Routing Protocols

Where the version is a 4-bit block which is used to indicate the version of protocol. Opcode is a bit of 4 field which will specify conversion type of EIGRP. Checksum is a 24-bit field which runs check on EIGRP packet. Flag is a 32-bit field. Sequence is also 32-bit field that contains the sequence number which in turn is used by Reliable Transport Protocol (RTP). It will ensure the ordered transfer of packets. Acknowledgement is a 32-bit field it contains the sequence number of the neighbor to which message is being transferred. Autonomous number system will identify EIGRP domain number. It is a 32-bit field. TLV stand for type, length, value, it contains route entries and gives EIGRP DUAL information.

EIGRP have following types of messages:

- Hello packet: The purpose of these messages is to identify the neighbors. Once the neighbors are identified these messages are used to check whether the neighbors are active and reachable or not.
- Acknowledgement: It is a message that have no data. It is referred as hello packet. These packets ensure the reliable transfer of EIGRP packets.
- Update Packet: It is used to ensure the reachability of destination and contains routing updates. Update packets are sent when a new neighbor is found.
- Query Packet: Quires are sent when router is in active mode.
- Reply Packet: These packets are sent in response of query packet.
- Request Packet: When some specific information is needed from neighbors a request packet is transmitted.

Every router in EIGRP has information about every neighboring router's states. When a new neighbor is added, the router will save the required information about that neighbor [1]. Two routers which are connected directly will become neighbors if and only if they are in same autonomous system [5].

C. Open Shortest Path First (OSPF)

As we know that, networks are collection of routers which are connected using IP's and OSPF is a routing protocol which is basically used to select the best path for transfer of packet. It was developed by IETF group in mid of 1980. OSPF supports both Internet Protocol Version 4 and Internet Protocol Version6. It is a dynamic routing protocol used in modern communication. It is a link state routing protocol [P6]. In link state routing, routers will exchange information that will help each router to learn topology of network. Each router will than create its own routing table by using shortest path algorithms. OSPF can detect change in topology and to select another route which is loop free within no time. Using available link state routing information, OSPF creates a topology and routing table is created [P1]. All routers that are connected will gain updates about changes through link state advertisements (LSA) [4].

When OSPF is configured, it will collect information about all neighbors and for all available paths a topology map is generated. This information is stored in Link state database. From this information shortest path to reach required network is calculated using shortest path first algorithm developed by Dijkstra in 1956. There are many variations of Dijkstra algorithm. Originally this algorithm finds the shortest path between 2 nodes but now one node is considered and fixed as source node. After fixing source node shortest path is computed between all nodes [P6]. Therefore, generating a

tree. Three tables are generated which will store the following information.

Neighbor Table: It will store all discovered neighbors with which the information is to be shared.

Topology Table: As its name implies it will store the network topology map. Best and alternate paths are also computed.

Routing Table: It contains the currently active path which will be used to deliver packets between nodes.

Similar Link State Database is maintained between all routers of the network. Communication is done by making adjacencies. Adjacency is a state where the routers are ready for exchanging link state advertisements. Initially, the routers are in down state. To form adjacency first a hello packet is transferred between routers to become neighbors. Decision to establish neighborhood relationship depends on these packets. After that the routers will add each other in their database if they decided to become neighbors. After that designated router and backup designated router elections will occur. After elections, the router will enter in Exstart state. In this state the routers and their DR and BDR creates a master slave relationship. The router with high router id will become master and link state databases are established by using database description packets (DBD). Routes are discovered by exchanging DBD. This process is known as Exchange. After that, a link state acknowledgement is sent. Information received is compared by slave and if the information is new, it will send an update request. In response to this request a n update is sent which contains the required LSAs. On successful receiving of updates an acknowledgement is again sent and adjacency is formed.

D. Routing Information Protocol (RIP)

Protocol is a router of distance vector. It uses the method of hop count to find the efficient route to destination. Jump check is alludes to the quantity of center gadgets through which information makes a trip from source to objective. Maximum number of hops that are included in RIP is 15. If the number of hops exceeds 15 the path is inconvenient. Initially, RIP sends an update message after every 30 seconds.

There are four basic timers in RIP. Update timer will tell after how long the router will send updates of routing table. By default, update timer time is 30 seconds. Invalid Timer will define the time after which route is invalid. By default, route will be considered invalid after 180 seconds. Third type of timer is hold down timer. It will define the time after which the route will receive an update message. Last is flush timer. When no updates are being received by the route flush timer will define after how long the route will be flushed out [2].

Routers will develop the list of network devices that are connected directly. The information then is released on all routers interface. The router which is attached with the advertising router will store the data in routing table and forward it to next router. In this way all the routers will have each other's information [1].

RIP messages are used for communication between routers. User Datagram Protocol (UDP) port 520 is used for sending these messages. There are two types of messages. First one is known as RIP request in which the router sends a request to other router requesting it to share its routing table. Second type of message is RIP Response in which the requested information is sent to router [6].

There are three versions of Routing information protocol. These are as follows:

RIPv1: The real identification of RIP, explained in RFC 1058, was produced in 1988 and utilize class- full routing. The regular routing upgrades do not convey subnet facts, unavailable maintenance for variable length subnet masks (VLSM). This restriction builds it unbearable to have distinct-sized subnets inner of the similar network class. Routers are not verified which will make RIP vulnerable to attacks.

RIPv2: Because of the shortfall of the first RIP acknowledgment, RIP form 2 (RIPv2) was continuing in 1993 and last coordinated in 1998. It covers the capacity to contain subnet subtleties, accordingly, keeping up Classless Inter-Domain Routing (CIDR). To help in reverse similarity, the bounce check cutoff of 15 persevered. RIPv2 has answers for totally pragmatic with the earlier distinguishing proof if all Must Be Zero convention fields in the RIPv1 correspondences are suitably recognized. In adding up to, a similarity switch trademark allows fine-grained interoperability convenience. While trying to avoid undesirable load on has that don't occupied with steering, RIPv2 multicasts the total directing table to all close by switches at the location 224.0.0.9, as against to RIPv1 which uses broadcast. Unicast tending to is as yet approved for applications.

RIPng: RIPng (RIP next generation), explained in RFC 2080, is an addition of RIPv2 for maintenance of IPv6, the afterward generation Internet Protocol. The core differences between RIPv2 and RIPng are:

- Maintenance of IPv6 networking.
- While RIPv2 cares RIPv1 updates validation, RIPng does not. IPv6 routers stayed, at the time, thought to use IPsec for verification.
- RIPv2 encodes the upcoming-hop into each path admission, RIPng involves encoding of the afterward hop for a set of route entrances.

RIPng guides informs on UDP port 521 using the multicast group FF02::9.

E. Exterior Gateway Protocol (EGP)

It is a routing protocol which is used to select path between different networks. IGP is used within single autonomous system whereas EGP is used to connect two autonomous systems. The routing table of EGP includes the known routers, addresses and selection path. EGP mechanism involves acquiring neighbors, monitoring the neighbors, and then exchanging data as updates. Border gateway protocol is the only EGP used for communication.

F. Border Gateway Protocol (BGP)

It is an important interdomain routing protocol. It is a type of path vector routing protocol [7]. In early days, there was a set of centralized routers which is known as core autonomous systems. To communicate within core autonomous system

these routers use gateway to gateway protocol and exterior gateway protocol is used when communication is to be done outside the core. But as internet grew the number of autonomous systems becomes larger certain weakness of EGP were observed. It becomes important to introduce a new exterior gateway protocol [8]. So, BGP was introduced to overcome the flaws of EGP [5]. In path vector routing. In path vector routing path information is maintained in routing table and information gets updated dynamically. The table contains the address of destination and the path used to reach destination. The main purpose of this protocol is to share reachability information between different BGP peers [9]. The BGP node saves all information which is sent by neighbors but by using some policies it selects the best path and transmits data on that path. A backup path is also stored which is advertised and used if the first path fails or went down [7]. As discussed above, internet is a collection of autonomous systems (AS). BGP is used to communicate between or to link two or more autonomous systems. BGP sessions are created between edge routers and after that route are exchanged between neighbors [10]. It is an incremental protocol. Once routing table is shared between neighbors, only updated information is distributed. These changes may include withdrawal of the route or advertising a new route [10]. BGP4 is currently used BGP version. It is based on TCP/IP and uses port 179 of TCP/IP. The protocol guarantees loop free routing. The routers in BGP are linked together using mesh topology which will cause scalability issues. BGP uses route reflectors and confederations to improve scalability.

To implement route reflector in an autonomous system, one or more router is termed as route reflector and all other routers are connected to it. Updates in a single router are sent to route reflector which will in turn reflects the changes in all routers that are connected to it. While in confederation the routers are divided into multiple autonomous system. The Fig. 3. below shows the connectivity using BGP route reflector and BGP confederations.

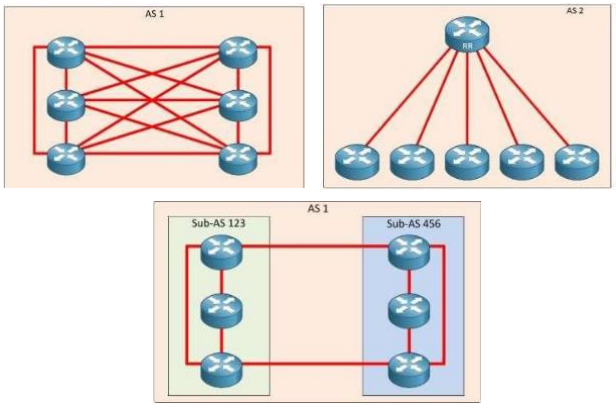

Fig. 3. a) Mesh Topology, b) BGP Reflector, c) BGP Confederation.

BGP make decisions based on path information, policies made by network administrator. Path is represented as a list of attributes. Path attributes are the characteristics of BGP route. Routing policies are set, and communication takes place using these attributes [11]. These attributes are divided into 2 groups:

Well Known Attributes: Well-known attributes are defined as those attributes that must be recognized by every BGP router. BGP well-known attributes are further classified as:

- Mandatory: Mandatory attributes are also known as well-known mandatory. These attributes are always attached with update messages and must be understood by all BGP peers.
- Discretionary: These attributes may or may not be the part of update messages. But are recognized by BGP peers.

Optional Attributes: These are the attributes that need not to be recognized by every router. These are further divided into two types:

- Transitive: If any attribute is not recognized by the BGP peers, BGP will look whether the transitive flag is turned set or not. If the flag is set, then the attribute must be accepted and advertised to all peers.
- Non-Transitive: If the attribute is not recognized update can be ignored and is not advertised to peers.

The Fig. 4. below shows the examples of some BGP attributes:

Attribute Name	Category / Class
ORIGIN	Well-Known Mandatory
AS_PATH	Well-Known Mandatory
NEXT_HOP	Well-Known Mandatory
LOCAL_PREF	Well-Known Discretionary
ATOMIC_AGGREGATE	Well-Known Discretionary
AGGREGATOR	Optional Transitive
COMMUNITY	Optional Transitive
MULTI_EXIT_DISC (MED)	Optional Non-Transitive
ORIGINATOR_ID	Optional Non-Transitive
CLUSTER LIST	Optional Non-Transitive
MULTIPROTOCOL Reachable NLRI	Optional Non-Transitive
MULTIPROTOCOL Unreachable NLRI	Optional Non-Transitive

Fig. 4. BGP Routing Protocol Attributes

Origin indicates the origin of the prefix. There are three origin codes (IGP, EGP, incomplete. Where IGP demonstrates the prefix started by Interior Gateway Protocol, EGP shows prefix began by Exterior Gateway Protocol and Incomplete shows the prefix began from some obscure source. All BGP messages share a common header which includes a type of field. This field will indicate the type of BGP message. BGP message packets are classified into 4 types:

- Open
- Keep-alive
- Notification
- Update

BGP session is create a link using Open Message and containing the regarding information as well which must be

accepted by both routers before they could start sharing information. Open message contains certain fields which involves: Version that indicates the BGP version that is running on both routers. If the version does not match there will be no BGP session. My autonomous system number will show the number of autonomous systems which is assigned by IETF. Hold time is a time BGP router wait for response from other side. If router does not receive any keep alive message or update within defined time from next router the router will be considered dead, and session will be broken down. BGP Identifier will define the router that send the message. Option parameter contains some optional capabilities of router. Using update message network reachability information is exchanged using this message. New routes are advertised or already routes are withdrawal using update message. Keep-alive messages are used maintain the session. Keep alive message is sent after every 60 seconds. It only contains a BGP header. It does not have any data field. Notification Message whenever an error occurs the router will close the session and will send a notification message that carries information about error [12].

To make decisions BGP peers uses Finite state machine. The finite state machine have six steps as shown in Fig. 5.

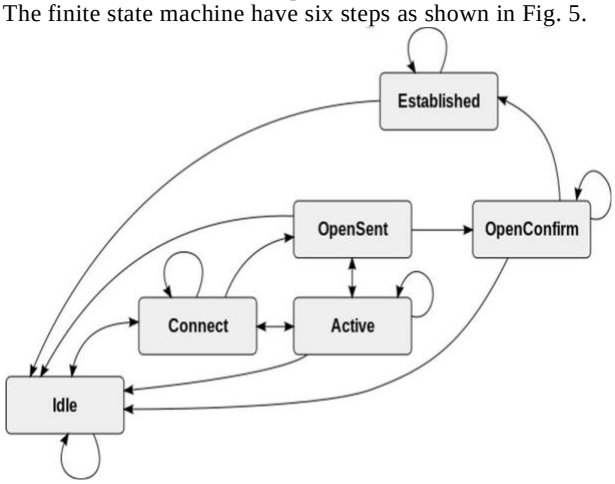

Fig. 5. Finite Machine of BGP Routing Protocol.

The first state in finite state machine is idle state. In this state BGP will start TCP connection with all its peers. And changes its state from idle to connect. In connect state, the router will wait for the completion of connection. On successful completion of connection, the router will set itself to Open-sent state. If connection is not successful connect retry timer will start. On expiration of time the router will move to active state. In active state the connect retry time is set to be zero and router will move to connect state. In open sent state the finite state machine will check for Open message from peer. And router will check the validity of the Open message. If an error occur the router will send notification about error to the peer.

Otherwise keep alive message is sent and state is changed to Open Confirm. If time expires before keeping alive message is received the router will again go back to idle state. Whereas on successful receiving of keep alive messages router moves to established state. In established state routers can send as well as receive update messages from its peer.

BGP falls into two categories:

- EBGP
- IBGP

BGP may be used for communication within same autonomous system or between different autonomous systems. When BGP is implemented between routers within in single autonomous system it is known as IBGP or Internal border gateway protocol. While when communication between different autonomous systems is achieved by implementing BGP the BGP is referred to as EBGP or External Border Gateway Protocol.

	RIP	OSPF	BGP
Interior / Exterior	Interior	Interior	Exterior
Type	Distance Vector	Link State	Path Vector
Default Metric	Hop count	Cost	Multiple Attributes
Hope count Limit	15	None	EBGP Neighbor : 1 IBGP Neighbor: 0
Convergence	Slow	Fast	Average
Update Timer	30 seconds	Only when change occur	Only when change occur
Update Information	Full table	Only changes	Only Changes
Algorithm	Bellman-Ford	Dijkstra	Best Path algorithm
Protocol and port	UDP port 520	IP protocol 89	TCP port 179
Areas and Boundary	No concept of areas and boundaries	Network is divided into areas	Works outside the network

III. Comparison of RIP, OSPF and BGP

The Fig. 6. below a comparison between different internet routing protocols of RIP, OSPF, BGP.

Fig. 6. Comparison of Different Routing Protocols.

IV. Conclusion

It is concluded that routing protocols plays an important role in digital communication. Different routing protocols works in different environments by applying certain techniques. Every protocol has some drawbacks which were eliminated by introducing certain new versions of these protocols. Like the scalability issue of EGP was reduced by BGP route reflectors and BGP confederations. Also, BGP was introduced to overcome some other flaws of EGP. Similarly, different versions of RIP were introduced to enhance the working of routing protocols. The aim of this paper is to provide a comprehensive summary of different internet routing protocols.

References

[1] Aftab, M. U., Nisar, A., Habib, M. A., Ashraf, A., & Burhan, M. (2014). A Review Study of Interior and Exterior Gateway Protocols. Journal of Basic and Applied Scientific Research, 4(6), 57–67.

[2] Deng, J., Wu, S., & Sun, K. (2014). Comparison of RIP, OSPF and EIGRP Routing Protocols based on OPNET, 23.

[3] Jha, R. K., & Kharga, P. (2015). A comparative performance analysis of routing protocols in MANET using NS3 simulator. *International Journal of Computer Network and Information Security*, *7*(4), 62-68.

[4] Piechowiak, M., Zwierzykowski, P., Owczarek, P., & Wasłowicz, M. (2016, July). Comparative analysis of routing protocols for wireless mesh networks. In *2016 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)* (pp. 1-5). IEEE.

[5] Nazumudeen, N., & Mahendran, C. (2007). Performance Analysis of Dynamic Routing Protocols Using Packet Tracer. International Journal of Innovative Research in Science, Engineering and Technology An ISO Certified Organization, 3297(1), 570–574.

[6] Verma, A., & Bhardwaj, N. (2016). A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol. International Journal of Future Generation Communication and Networking, 9(4), 161–170.

[7] Kakarla, J., Majhi, B., & Battula, R. B. (2015). Comparative analysis of routing protocols in wireless sensor–actor networks: a review. *International Journal of Wireless Information Networks*, *22*(3), 220-239.

[8] Sharma, K., Mittal, N., & Rathi, P. (2014). Comparative Analysis of Routing Protocols in Ad-hoc Networks. International Journal of Advanced Science and Technology, 69(9), 1–12.

[9] Farid, S., & Rehman, A. U. (2018). Enhancement in Quality of Services Using Integrated Services in 4G Cellular Network. Technical Journal, 23(03), 82-93.

[10] Xuehui, W. (2013). BGP Fast Convergence Based on Message Classification, 6(6), 151–160.

[11] Vistro, D. M., Munawar, A., Iftikhar, A., Qasim, A., & Rehman, A. U. (2020). TERTIARY CARE HOSPITAL MONITORING SYSTEM USING WIRELESS SENSORS. Journal of Critical Reviews, 7(10), 1504-1511.

[12] Sharma, K., Mittal, N., & Rathi, P. (2014). Comparative Analysis of routing protocols in ad-hoc networks. *International Journal of Advanced Science and Technology*, *69*, 1-12.

[13] Vistro, D. M., Rehman, A. U., Mehmood, S., Idrees, M., & Munawar, A. (2020). AN IOT BASED APPROACH FOR SMART AMBULANCE SERVICE USING THINGSPEAK CLOUD. Journal of Critical Reviews, 7(9), 1697-1703.

[14] Krijestorac, S., & Beck, M. (n.d.). Border Gateway Protocols.

[15] Prashar, L., & Kapur, R. K. (2016, September). Performance analysis of routing protocols under different types of attacks in MANETs. In *2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 405-408). IEEE.

[16] Caesar, M., & Rexford, J. (2005). BGP routing policies in ISP networks. IEEE Network, 19(6), 5.