Nasir *et al* *LGURJCSIT* 2018

LGURJCSIT
ISSN: 2519-7991

LGU R Journal for
Computer Sciences IT

Research Article

Vol. 2 Issue 2 April-June 2018

A Comparative Study of Routing Protocols Including RIP, OSPF and BGP

Ayesha Nasir, Unsa Tariq

ayeshanasir@lgu.edu.pk, unsatariq23@gmail.com

Lahore Garrison University

Abstract:

In network communication, routing is the process of transferring data across network between different end devices. Communication can be within a local area network (LAN) or a wide area network (WAN). Despite of the network type, routing is considered as an important process in network communication. Router works with routing protocols. Routing protocol basically determines the way in which different routers communicate and transfer data. Different protocols have different attributes, algorithms and architecture that makes them capable to achieve reliable communication. So, we can say that the basics for transferring data across network is routing protocols. The data moves across different network topologies and different protocols working within and outside an autonomous system handles this data. Various protocols used in routing includes: Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP) and many more. The purpose of this paper is to provide a comparison of different routing protocols. The main focus of this paper will be on OSPF, RIP, BGP and its types.

1. 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.

In computer networks, a router is a device that links different networks and defines the best path to transmit packet from source to destination. Routing table is generated inside a router which contains the path information. Router in addition to this information uses certain algorithms to find the best path for packet to travel.

Static routing is a manual way to create a routing table which means that in static routing, the routing table is created and maintained by the network administrator [4]. To establish a full connectivity, each router must be configure with the static route to all networks. Static routing does not tolerate any fault. The following figure give a graphical view of routing protocols.

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

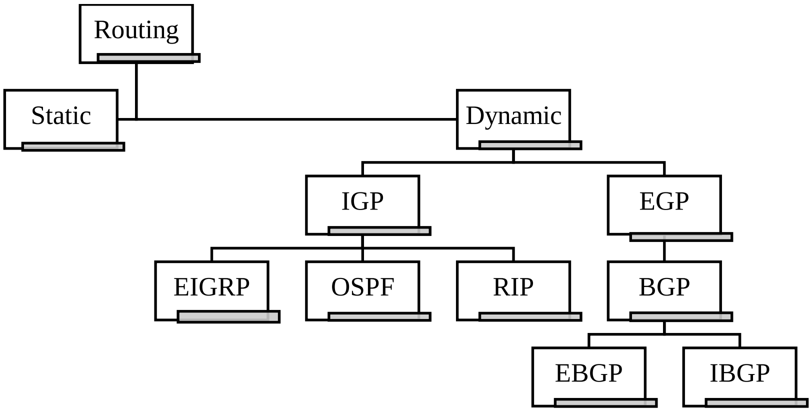


Figure No 1: Routing Protocols

2. Interior Gateway Protocol:

Interior Gateway Protocol is abbreviated as IGP. The protocol is classified as dynamic routing protocol. As we know that internet is a collection of many autonomous systems. 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. These protocols keeps records of the path from source to destination. 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].

3. 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 Bellman Ford algorithm and Ford Fulkerson 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 routing 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:

a. Neighbor discovery/ recovery
b. Reliable transport protocol
c. DUAL finite state machine
d. Protocol dependent modules

In neighbor discovery, the information about other routers that are connected directly connected with them are processed and stored [2]. 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 in order 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 [3].

The figure below shows the message format of EIGRP:

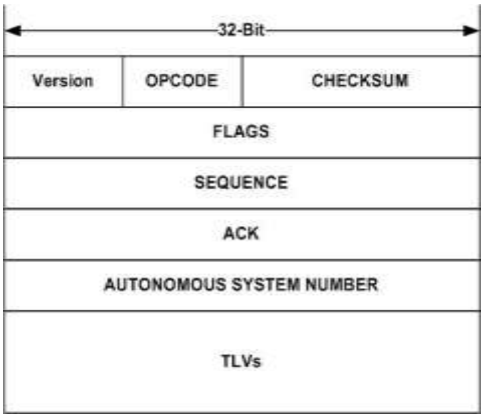


Figure No 2: Message Header of EIGRP

Where the version is a 4 bit block which is used to indicate the version of protocol. Opcode is also a 4 bit field which will specify message type of EIGRP. Checksum is a 24 bit field which runs sanity 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 its 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:

a. 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.
b. Acknowledgement: It is a message that have no data. It is referred as hello packet. These packets ensure the reliable transfer of EIGRP packets.
c. Update Packet: It is used to ensure the reachability of destination and contains routing updates. Update packets are send when a new neighbor is found.
d. Query Packet: Quires are sent when router is in active mode.
e. Reply Packet: These packets are send in response of query packet.
f. 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].

4. Open Shortest Path First (OSPF):

As we know that, networks are collection of routers which are connected together 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 have the ability to 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.

a. Neighbor Table	It will store all discovered neighbors with which the information is to be shared
b. Topology Table	As its name implies it will store the network topology map. Best and alternate paths are also computed.
c. 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 of all 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 Exstart state, a master slave relationship is created between the routers and their DR and BDR. 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.

5. Routing Information Protocol (RIP):

It is a distance vector routing protocols. It uses the method of hop count to find the best path to destination. Hop count is refers to the number of middle devices through which data travels from source to destination. Maximum number of hops that are included in RIP is 15. If the number of hops exceeds 15 the path is considered to be 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 considered to be 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 [5].

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 [6].

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 build 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: Due to the absence of the original RIP recognition, RIP version 2 (RIPv2) was proceed in 1993 and last organized in 1998. It covers the ability to contain subnet details, thus maintaining Classless Inter-Domain Routing (CIDR). To support backward compatibility, the hop count limit of 15 endured. RIPv2 has solutions to completely practical with the prior identification if all Must Be Zero protocol fields in the RIPv1 communications are appropriately identified. In totaling, a compatibility switch characteristics permit fine-grained interoperability accommodation. In an attempt to keep away from unwanted weight on hosts that do not engaged in routing, RIPv2 multicasts the complete routing table to all alongside routers at the address 224.0.0.9, as against to RIPv1 which utilizes broadcast. Unicast addressing is still authorized for particular 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:

a. Maintenance of IPv6 networking.
b. While RIPv2 cares RIPv1 updates validation, RIPng does not. IPv6 routers stayed, at the time, thought to use IPsec for verification.

c. RIPv2 encodes the upcoming-hop into each path admission, RIPng involves particular encoding of the afterward hop for a set of route entrances.

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

6. 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 where as 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.

7. 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 router which is known as core autonomous systems. To communicate within core autonomous system these routers uses 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 system 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 also 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 routes 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 figure below shows the connectivity using BGP route reflector and BGP confederations.

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:

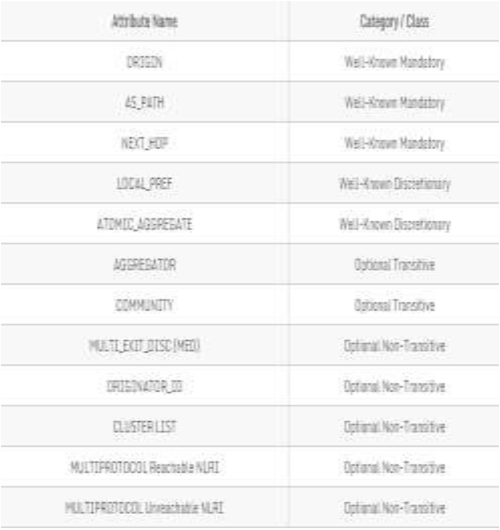
a. Well Known Attributes: Well-known attributes are defined as those attributes that must be recognized by every BGP router. BGP well-known attributes are further classified as:

1. 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.
2. Discretionary: These attributes may or may not be the part of update messages. But are recognized by BGP peers.

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

1. 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.
2. Non-Transitive: If the attribute is not recognized update can be ignored and is not advertised to peers.

The table 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

Table No 1: BGP Attributes

Origin indicates the origin of the prefix. There are three origin codes (IGP, EGP, incomplete). Where IGP indicates the prefix originated by Interior Gateway Protocol, EGP indicates prefix originated by Exterior Gateway Protocol and Incomplete shows the prefix originated from some unknown source.

All BGP messages share a common header which includes a type field. This field will indicate the type of BGP message. BGP message packets are classified into 4 types:

a. Open
b. Keep-alive
c. Notification
d. Update

Open Message is used to establish BGP session. The open message contains information about BGP router which must be accepted by both routers before they could start sharing information. Open message contain 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 system 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 consists of six steps.

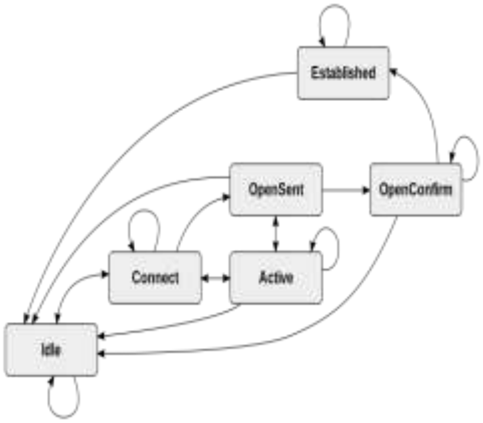


Figure No 4: Finite State Machine

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 keep 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.

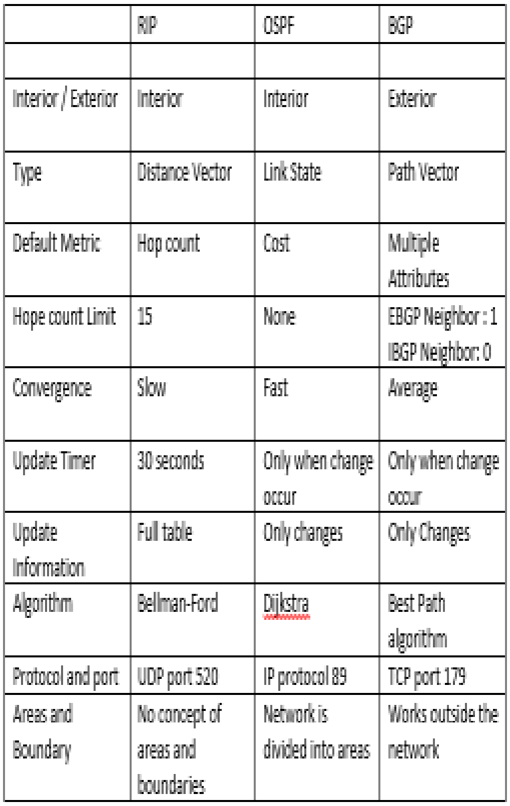
BGP falls into two categories:

a. EBGP
b. 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.

8. Comparison of RIP, OSPF and BGP:

The table below a comparison between different internet routing protocols [13].



	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

Table No 2: Comparison of Different Routing Protocols

9. *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 have 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.

10. References:

[1]. Comparison of RIP, EIGRP, OSPF, IGRP Routing Protocols in Wireless Local Area Network (WLAN) by using OPNET Simulator tool - A Practical Approach. (2014, Aug). *OSR Journal of Computer Engineering, 16*(4), 8.

[2]. Abhishek Verma, Neha Bhardwaj. (2016, April). A Review on Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) Routing Protocol. *International Journal of Future Generation Communication and Networking Online, 9*(4), 10.

[3]. David Bauery, Murat Yukselz, Christopher Carothersyand Shivkumar Kalyanaramanz. (n.d.). A Case Study in Understanding OSPF and BGP Interactions Using EfficientExperiment Design. 8.

[4]. E. Edwin Lawrence, Dr.R.Latha. (2014, November). A Comparative Study of Routing Protocols for Mobile Ad-Hoc Networks. *International Journal of Computer Science and Mobile Computing, 3*(11), 8.

[5]. Guangjie Han, Xu Jiang, Aihua Qian, Joel J. P. C. Rodrigues, and Long Cheng. (2014, June). A Comparative Study of Routing Protocols of Heterogeneous Wireless Sensor Networks. (J. Lloret, Ed.) *Te Scientifc World Journal*, 12.

[6]. Muhammad Umar Aftab, Amna Nisar, Dr. Muhammad Asif Habib, Adeel Ashraf. (2014, April). A Review Study of Interior and Exterior Gateway Protocols. *Journal of Basic and Applied Scientific Research*, 11.

[7]. N.Nazumudeen, C.Mahendran. (2014, February). Performance Analysis of Dynamic Routing Protocols Using Packet Tracer. *International Journal of Innovative Research in Science, Engineering and Technology, 3*(1), 5.

[8]. Pinky, Umesh Gupta. (2016, June). Research Paper on Implementation of OSPF Protocol in MATLAB. *International Journal of All Research Education and Scientific Methods (IJARESM), 4*(6), 7.

[9]. Sahil Thapar, A. K. (2014, November). Comparative Analysis of Routing Protocols. *International Journal of Computer Applications, 106*(9), 6.

[10]. Suresh Kumar , Jogendra Kumar. (2012, June). Comparative Performance Analysis of Routing Protocols in MANET using Varying Pause Time. *International Journal of Computer Applications, 47*(12), 6.

[11]. Tarikuzzaman emon, tarin kazi and nazia hossain. (2014, August). A comparative analysis on routing protocols of mobile ad hoc network. *International Journal of Computer Science, Engineering and Information Technology, 4*(4), 13.