Towards Implementing IS-IS

Abdul Rehman Khan
Aamir Abbas
Hassan Sattar
Salma Rashid
And
Dr. Kiramat ullah

***Abstract*-This report briefly describes routing and then explains what is IS-IS routing protocol and how IS-IS works.**

***Keywords*: Routing, Routing Protocol, Autonomous System, Dijkstra's Algorithm, Network Entity Title, Network Service Access Point, Level-1 router, Level-2 router, Protocol Data Unit (PDU).**

I. INTRODUCTION

Routing is the process of selection path from source to destination to share data. Routers are devices that are used to implement Routing based on some rules, which are called as Routing protocols. There are two types of routing protocols.

1. Interior Gateway Protocol (IGP)

An Interior Gateway Protocol (IGP) is a type of protocol used for exchanging routing information between routers within an Autonomous System (AS). Interior gateway protocols can be divided into two categories:

Distance Vector Routing Protocols (DVRP) implemented as Routing Information Protocol (RIP) and Enhanced Interior Gateway Routing Protocol (EIGRP).

Link State Routing Protocols (LSRP) implemented as Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS).

2. Exterior Gateway Protocol (EGP)

An exterior gateway protocol is a routing protocol used to exchange routing information between autonomous systems. Exterior Gateway Protocols include Exterior Gateway Protocol (EGP), now obsolete, and Border Gateway Protocol (BGP).

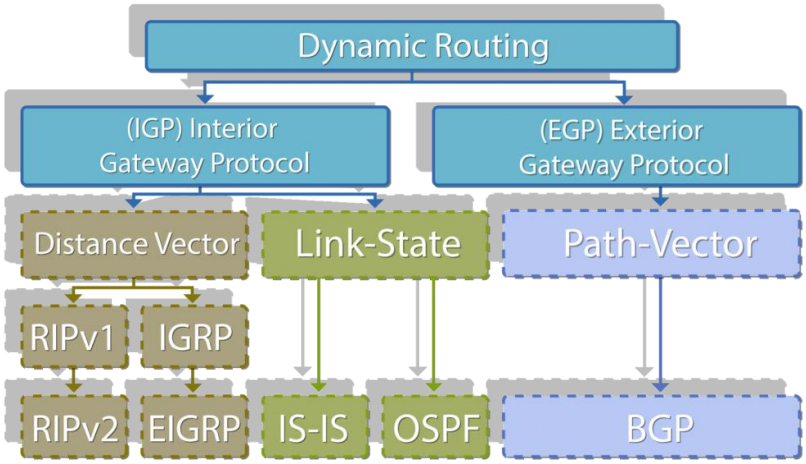


Figure 1:Routing Protocols

II. Intermediate System to Intermediate System (IS-IS)

Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a computer network, which consists of a group of physically connected computers. It accomplishes this by determining the best route for data through a packet-switched network. IS-IS has been called "the de facto standard for large service provider network backbones." IS-IS is an IGP, designed for use within an Autonomous System (AS it is a network formed by group of devices). This is in contrast to Border Gateway Protocol (BGP), which is used for routing between AS.

IS-IS is a link-state routing protocol. It operates by reliably flooding link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. Like the OSPF protocol, IS-IS uses Dijkstra's algorithm for computing the best path through the network. Packets (datagrams) are then forwarded, based on the computed ideal path, through the network to the destination. IS-IS uses multicast to discover neighbor routers by sending hello packets.

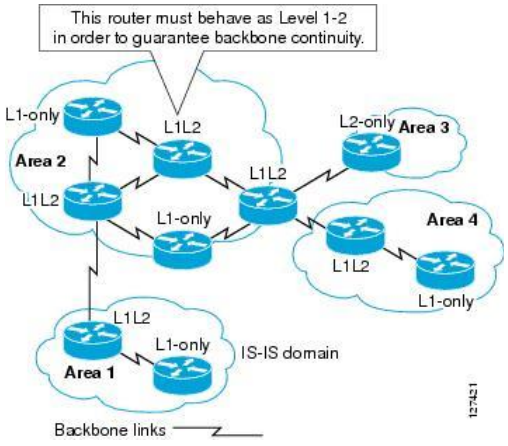


Figure 2:General Structure of IS-IS Network

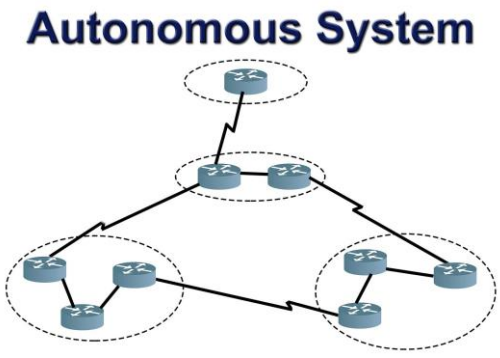


Figure 3:Autonomous System

III. PROPERTIES

A routing domain may be divided into one or more subdomains. Each subdomain is referred to as an area and is assigned an area address. Routing within an area is referred to as Level-1 routing. Routing between Level-1 areas is referred to as Level-2 routing. A device in OSI model is referred to as an Intermediate System (IS). An IS may operate at Level 1, Level 2, or both. An IS is identified by an address known as a Network Entity Title (NET). The NET is the address of a Network Service Access Point (NSAP), which identifies an instance of the IS-IS routing protocol running on an IS. The NET may be 8 to 20 octets in length and consists of three parts:

1. Area address—This field is 1 to 13 octets in length and is composed of high-order octets of the address.
2. System ID—This field is 6 octets long and immediately follows the area address. When the IS operates at Level 1, it must be unique among all the Level-1 devices in the same area. When the IS operates at Level 2, it must be unique among all devices in the domain.
3. NSEL—The N-selector field is 1 octet in length and immediately follows the system ID. It must be set to 00.

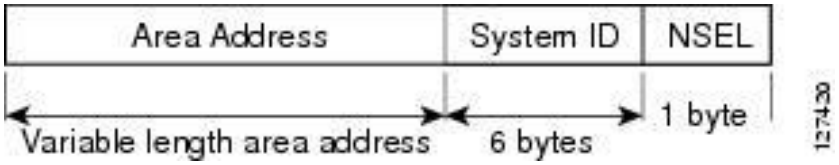


Figure 4:Network Entity Title Format

ISs exchange routing information with their peers using protocol data units (PDUs). The following types of PDUs are used:

1. Intermediate System-to-Intermediate System Hello PDUs (IIHs) are exchanged between IS neighbors on circuits on which the IS-IS protocol is enabled. IIHs include the system ID of the sender, the assigned area address, and the identity of neighbors that are known to the sending IS. There are three types: Point-to-Point IIHs, Level-1 LAN IIHs & Level-2 LAN IIHs.
2. An IS generates Link-State PDUs (LSPs) to advertise its neighbors and the destination that are directly connected to the IS. An LSP is uniquely identified by: System ID, Pseudonode ID, LSP number (0 to 255) & 32-bit sequence number. Whenever a new version of an LSP is generated, the sequence number is incremented.
3. Level-1 LSPs are generated by ISs that support Level 1. The Level-1 LSPs are flooded throughout the Level-1 area. The set of Level-1 LSPs generated by all Level-1 ISs in an area is the Level-1 LSP Database (LSPDB). All Level-1 ISs in an area will have an identical Level-1 LSPDB and will therefore have an identical network connectivity map for the area.
4. Level-2 LSPs are generated by ISs that support Level 2. Level-2 LSPs are flooded throughout the Level-2 subdomain. The set of Level-2 LSPs generated by all Level-2 ISs in the domain is the Level-2 LSP Database (LSPDB). All Level-2 ISs will have an identical Level-2 LSPDB and will therefore have an identical connectivity map for the Level-2 subdomain.
5. Sequence Number PDUs (SNPs) contain a summary description of one or more LSPs. There are two types of SNPs for both Level 1 and Level 2: Complete Sequence Number PDUs (CSNPs) that are used to send a summary of the LSPDB that an IS has for a given level & Partial Sequence Number PDUs (PSNPs) that are

used to send a summary of a subset of the LSPs for a given level that an IS either has in its database or needs to obtain.

III. ALGORITHM

It uses Dijkstra's Algorithm for finding route from source to destination. As in ISIS each router has information of whole network so it can use this algorithm to find shortest path. The path between nodes has value depending on distance, network traffic etc. In this algorithm the first node has distance zero and all nodes are at infinity. First node finds value of neighbors then the neighbor with less value calculates value of its neighbors then this process goes on and in end every node has some value which is used to find shortest value from source to destination.

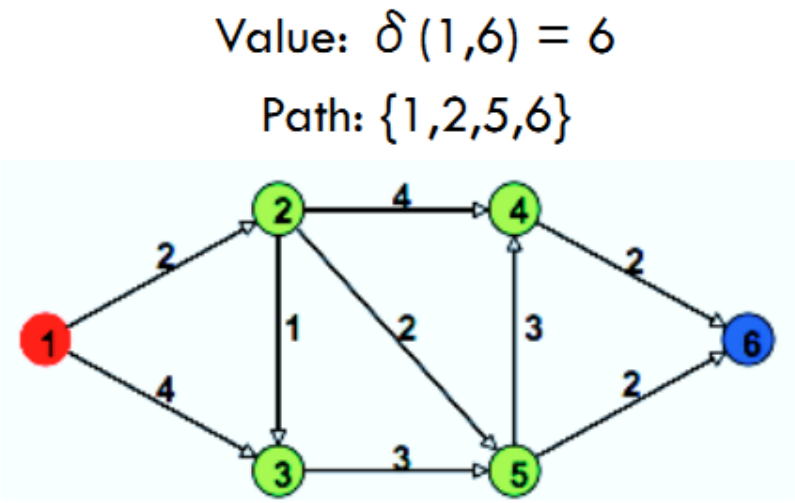


Figure 5:Source is 1 and Destination is 6, shortest path is (1, 2, 5, 6) with value 6

Let the starting node be called the initial node and let the distance of node N be the distance from the initial node to N. Dijkstra's algorithm will assign some initial distance values and will try to improve them step by step.

1. Mark all nodes unvisited. Create a set of all the unvisited nodes called the unvisited set.

2. Assign to every node a tentative distance value: set it to zero for our initial node and to infinity for all other nodes. Set the initial node as current.

3. For the current node, consider all of its unvisited neighbors and calculate their tentative distances through the current node. Compare the newly calculated tentative distance to the current assigned value and assign the smaller one. For example, if the current node A is marked with a distance of 6, and the edge connecting it with a neighbor B has length 2, then the distance to B through A will be 6 + 2 = 8. If B was previously marked with a distance greater than 8 then change it to 8. Otherwise, keep the current value.

4. When we are done considering all of the unvisited neighbors of the current node, mark the current node as visited and remove it from the unvisited set. A visited node will never be checked again.

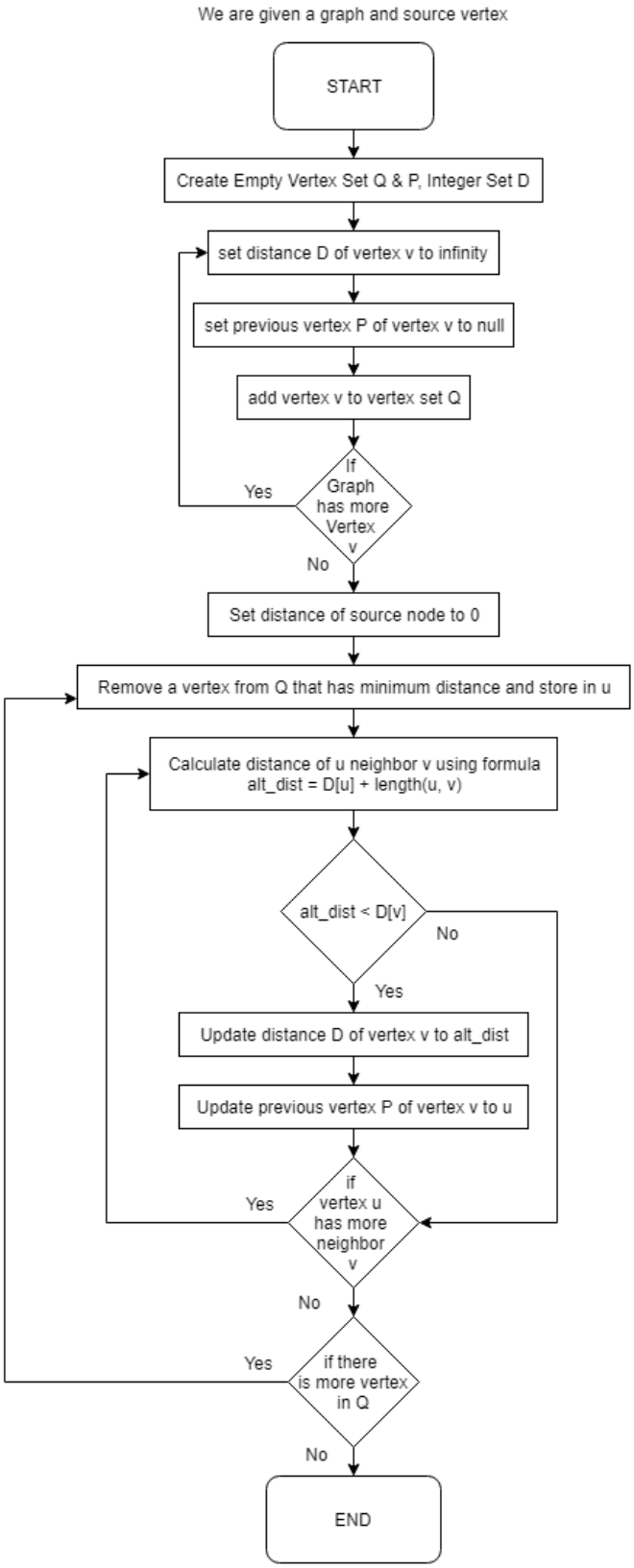
5. If the destination node has been marked visited (when planning a route between two specific nodes) or if the smallest tentative distance among the nodes in the unvisited set is infinity (when planning a complete traversal;

occurs when there is no connection between the initial node and remaining unvisited nodes), then stop. The algorithm has finished.

6. Otherwise, select the unvisited node that is marked with the smallest tentative distance, set it as the new "current node", and go back to step 3.

When planning a route, it is actually not necessary to wait until the destination node is "visited" as above: the algorithm can stop once the destination node has the smallest tentative distance among all "unvisited" nodes (and thus could be selected as the next "current").

III. FLOWCHART



III. SCENARIO

Consider five routers A, B, C, D & E. Router A is connected to B, C & E. Router B is connected to A, D & E. Router C is connected to A & D. Router D is connected to B & C. Router E is connected to A & B. Each router has its own neighbors set stored in its database LSPDB as shown in figure 6. Each router transmits it neighbor data to other routers through LSP (Link-State PDU). When a router receives LSP it checks it against its own LSPDB and if LSP contains router not in its database then database is updated. In the end all routers in one area will have same data in their databases as shown in figure 7. Now if Router A wants to send data to Router D it first finds the shortest path from path (A, C, D), path (A, B, D) & path (A, E, D) depending on weights of edges.

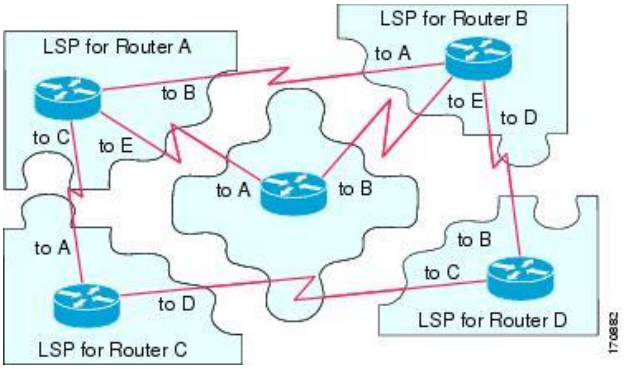


Figure 6: Initial State of Routers before Sending PSU's

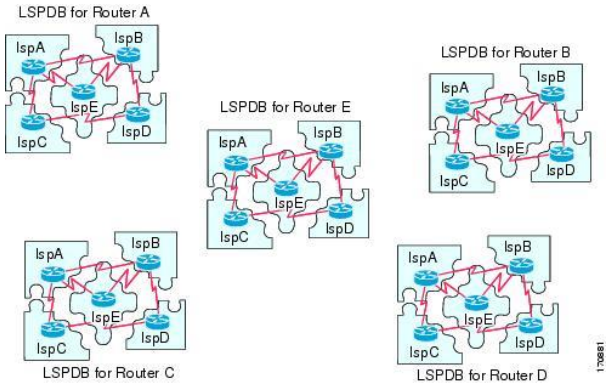


Figure 7: Final State of Routers after Updating Databases

REFERENCES

[1] Z. Haider, M. Saleem, and T. Jamal, "Analysis of Interference in Wireless", in Proc. of ArXiv, arXiv:1810.13164 [cs.NI], Oct. 2018.

[2] T. Jamal and P. Mendes, “Relay Selection Approaches for Wireless Cooperative Networks”, in Proc. of IEEE WiMob, Niagara Falls, Canada, Oct. 2010.

[3] T. Jamal, P. Mendes, and A. Zúquete, “Opportunistic Relay Selection for Wireless Cooperative Network”, in Proc. of IEEE IFIP NTMS, Istanbul Turkey, May 2012.

[4] T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions”, in Proc. of IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, Dec 2014.

[5] P. Mendes, W. Moreira, T. Jamal, and Huiling Zhu, “Cooperative Networking in User-Centric Wireless Networks”, In: Aldini A., Bogliolo A. (eds) User-Centric Networking. Lecture Notes in Social Networks. Springer, Cham, ISBN 978-3-319- 05217-5, May 2014.

[6] T. Jamal, P. Mendes, and A. Zúquete, “Relayspot: A Framework for Opportunistic Cooperative Relaying”, in Proc. of IARIA ACCESS, Luxembourg, June 2011.

[7] T. Jamal, and SA Butt, "Malicious Node Analysis in MANETS", in Proc. of International Journal of Information Technology, PP. 1-9, Springer Publisher, Apr. 2018.

[8] T. Jamal, and P. Mendes, “COOPERATIVE RELAYING FOR DYNAMIC NETWORKS”, EU PATENT, (EP13182366.8), Aug. 2013.

[9] T. Jamal, and P. Mendes, “802.11 Medium Access Control In MiXiM”, in Proc. of Tech Rep. SITILabs-TR-13- 02, University Lusófona, Lisbon Portugal, Mar. 2013.

[10] T Jamal, M Alam, and MM Umair, "Detection and Prevention Against RTS Attacks in Wireless LANs", in Proc. of IEEE C-CODE, Islamabad Pakistan, Mar. 2017.

[11] L. Lopes, T. Jamal, and P. Mendes, "Towards Implementing Cooperative Relaying", In Proc. of Technical Report COPE-TR-13-06, CopeLabs University Lusofona Portugal, Jan 2013.

[12] T. Jamal, P. Mendes, and A. Zúquete, “Interference-Aware Opportunistic Relay Selection”, In Proc. of ACM CoNEXT student workshop, Tokyo, Japan, Dec. 2011.

[13] T. Jamal, "Cooperative MAC for Wireless Network", In Proc. of 1st MAP Tele Workshop, Porto, Portugal, 2010.

[14] T. Jamal and P. Mendes, “Analysis of Hybrid Relaying in Cooperative WLAN”, In Proc. of IEEE IFIP Wireless Days (WD), Valencia, Spain, November 2013.

[15] T. Jamal, and P. Mendes, “Cooperative Relaying for Wireless Local Area Networks”, In: Ganchev I., Curado M., Kassler A. (eds) Wireless Networking for Moving Objects. Lecture Notes in Computer Science, vol 8611. Springer, Cham, (WiNeMo), Aug. 2014.

[16] T. Jamal, and SA Butt, “Cooperative Cloudlet for Pervasive Networks”, in Proc. of Asia Pacific Journal of Multidisciplinary Research, Vol. 5, No. 3, PP. 42-26, Aug 2017.

[17] T. Jamal, P. Mendes, and A. Zúquete, “Wireless Cooperative Relaying Based on Opportunistic Relay Selection”, in Proc. of International Journal on Advances in Networks and Services, Vol. 5, No. 2, PP. 116-127, Jun. 2012.

[18] SA Butt, and T. Jamal, “Frequent Change Request from User to Handle Cost on Project in Agile Model”, in Proc. of Asia Pacific Journal of Multidisciplinary Research 5 (2), 26-42, 2017.

[19] T. Jamal, and P. Amaral, “Flow Table Congestion in Software Defined Networks”, in Proc. of IARIA 12th ICDS, Rome Italy, Mar. 2018.

[20] R. Sofia, P. Mendes, W. Moreira, A. Ribeiro, S. Queiroz, A. Junior, T. Jamal, N. Chama, and L. Carvalho, “Upns: User Provided Networks, technical report: LivingExamples, Challenges, Advantages”, Tech. Rep. SITI-TR- 11- 03, Research Unit in Informatics Systems and Technologies (SITI), University Lusofona, Lisbon Portugal, Mar. 2011.

[21] T. Jamal, and P. Mendes, “Cooperative Relaying in Wireless User-Centric Networks”, Book Chapter In: Aldini, A., Bogliolo, A. (eds.) User Centric Networking. Lecture Notes in Social Networks, Springer, Cham, pp. 171–195, 2014.

[22] T. Jamal, P. Mendes, and A. Zúquete, “Design and Performance of Wireless Cooperative Relaying”, PhD Thesis MAP-Tele, University of Aveiro, Oct. 2013.

[23] T. Jamal, P. Mendes, and A. Zuquete, “RelaySpot: Cooperative Wireless Relaying”, in Proc. of MAP-Tele Workshop, Aveiro, Portugal, May 2011.

[24] T. Jamal, and P. Mendes, “Cooperative Wireless Relaying, Key Factors for Relay Selection”, in Proc. of MAP- Tele Workshop, Porto, Portugal, Dec. 2009.

[25] SA Butt, and T. Jamal, “Study of Black Hole Attack in AODV”, in Proc. of International Journal of Future Generation Communication and Networking, Vol. 10, No.9, pp. 37-48, 2017.

[26] T. Jamal, and SA Butt, “Low-Energy Adaptive Clustering Hierarchy (LEACH) Enhancement for Military Security Operations”, In Proc. Of Journal of Basic and Applied Scientific Research, ISSN 2090-4304, 2017.

[27] T. Jamal, and P. Mendes, “RelaySpot, OMNET++ Module”, Software Simulator Extension In Proc. of COPE- SW-13-05, 2013.

[28] T. Jamal and Z. Haider, "Denial of Service Attack in Cooperative Networks", in Proc. of ArXiv, arXiv: CoRR Vol. abs/1810.11070 [cs.NI], Oct. 2018.