Implementation of OSPF and CSPF Protocols in Ad Hoc Networks

Podili V S Srinivas¹, D Vamsi Krishna², P L P Goutham³, G Nethrika⁴
Department of Computer Science and Engineering, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad- 500 090, India
Corresponding Author Email: pvs.srinivas@griet.ac.in

Abstract:
A wireless ad hoc network (WANET) is a decentralized wireless network, which does not rely on a preexisting infrastructure. Instead, each node participates in routing by forwarding the data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to classic routing, Ad hoc networks can use flooding for forwarding the data. This paper proposes two novel protocols namely OSPF and CSPF that are used to compute the shortest distance in an Adhoc networks.

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) for routing Internet Protocol (IP) packets solely within a single routing domain, such as an autonomous system. It gathers link state information from available routers and constructs a topology map of the network. The topology is presented as a routing table to the Internet Layer which routes data grams based solely on the destination IP address found in IP packets. OSPF detects changes in the topology, such as link failures, and converges on a new loop-free routing structure within seconds.

Constrained Shortest Path First (CSPF) is an extension of shortest path algorithms. The path computed using CSPF is a shortest path fulfilling a set of constraints. It simply means that it runs shortest path algorithm after pruning those links that violate a given set of constraints.

Keywords: Ad Hoc Network, OSPF, CSPF

1. Introduction
A computer network or data network is a telecommunication network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along data connections (network links). Data is transferred in the form of packets. The connections between nodes are established using either cable media or wireless media. The best-known computer network is the Internet. Apart from any physical transmission medium there may be, networks comprise additional basic system building blocks, such as network interface controller (NICs), repeaters, hubs, bridges, switches, routers, modems, and firewalls. Here we consider network building blocks as routers.

Routing is the process of selecting best paths in a network. Routing is performed for many kinds of networks, including the telephone network (circuit switching), electronic data networks (such as the Internet), and transportation networks. In packet switching networks, routing directs packet forwarding through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. General-purpose computers can also forward packets and perform routing, though they are not specialized hardware and may suffer from limited performance. Routing schemes differ in their delivery semantics:

- Unicast delivers a message to a single specific node.
- Broadcast delivers a message to all nodes in the network.
- Multicast delivers a message to a group of nodes that have expressed interest in receiving the message.
- Anycast delivers a message to anyone out of a group of nodes, typically the one nearest to the source.
- Geocast delivers a message to a geographic area.

Routing protocols specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

Distance vector algorithms use the Bellman–Ford algorithm. This approach assigns a cost number to each of the links between each node in the network. Nodes will send information from point A to point B via the path that result in the lowest total cost.

Link-state algorithms: When applying link-state algorithms, a graphical map of the network is the fundamental data used for each node. To produce its map, each node floods the entire network with information about the other nodes it can connect to. Each node then independently assembles this information into a map. Using this map, each router
independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is a tree graph rooted at the current node, such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node [8]. Examples of link-state routing protocols include open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS)[9].

2. Related Work

Developing support for routing is one of the most significant challenges in ad hoc networks and is critical for the basic network operations. Certain unique combinations of characteristics make routing in ad hoc networks interesting. First, nodes in an ad hoc network are allowed to move in an uncontrolled manner. Such node mobility results in a highly dynamic network with rapid topological changes causing frequent route failures [6]. A good routing protocol for this network environment has to dynamically adapt to the changing network topology. Second, the underlying wireless channel provides much lower and more variable bandwidth than wired networks. The wireless channel working as a shared medium makes available bandwidth per node even lower. So routing protocols should be bandwidth-efficient by expending a minimal overhead for computing routes so that much of the remaining bandwidth is available for the actual data communication. Third, nodes run on batteries which have limited energy supply. In order for nodes to stay and communicate for longer periods, it is desirable that a routing protocol be energy-efficient as well. This also provides another reason why overheads must be kept low. Thus, routing protocols must meet the conflicting goals of dynamic adaptation and low overhead to deliver good overall performance. Routing protocols developed for wired networks such as the wired Internet are inadequate here as they not only assume mostly fixed topology but also have high overheads.

In packet switching networks, routing directs packet forwarding through intermediate nodes. Intermediate nodes are typically network hardware devices such as routers, bridges, gateways, firewalls, or switches. Here we consider intermediate nodes as routers.

Dijkstra’s algorithm is used to calculate the shortest path among the routers. When applying link-state algorithms, a graphical map of the network is the fundamental data used for each node. To produce its map, each node floods the entire network with information about the other nodes it can connect to. Each node then independently assembles this information into a map. Using this map, each router independently determines the least-cost path from itself to every other node using Dijkstra's algorithm[1].

Flooding (or network-wide broadcasting) is the simplest way to deliver data from a node to any other node in the network. In flooding, the source simply broadcasts the data packet to its neighboring nodes via a MAC layer broadcast mechanism. Each node hearing the broadcast for the first time re-broadcasts it. Thus, the broadcast propagates in "layers" outwards from the source, eventually terminating when every node has heard the packet and transmitted it once.

The rule “every node transmits only once” guarantees termination of the procedure and also avoids looping. This can be achieved using unique identifiers on all packets being flooded. The flooding technique delivers the data to every node in the connected component of the network. With flooding, no topological information needs to be maintained or known in advance. In network scenarios where node mobility is so high that a given unicast routing protocol may fail to keep up with the rate of topology changes, flooding may become the only alternative for routing data reasonably. However, in other scenarios where node mobility is trackable by a routing protocol, flooding can be a very inefficient option. This is because the total number of transmissions to deliver a single message to a destination with flooding is in the order of network size, as opposed to the network diameter with a unicast routing protocol[8] (assuming that a route is already found). Although flooding is not usually attractive for efficiently delivering data, it is still very useful in carrying out certain routing tasks such as route discovery and topology dissemination, and as a bootstrapping mechanism when nothing is known a priori about the network topology.

Therefore, flooding appears as a key component in many routing protocols (OSPF [10] is a classic example). In the simple flooding protocol as described above (also called pure flooding), each node transmits (broadcasts) the data once. As a result, a node may receive the same packet from several neighbors. Thus, depending on the network density, simple flooding may take far more transmissions than necessary for the flood to reach every node. Such redundancy can be eliminated to achieve less contention and collisions at the radio link layer, thus increasing network utilization. Several efficient alternatives have been proposed that use only a small subset of nodes to transmit the data packet during a flood, however ensure that all nodes in the network receive the packet.

Hello messages are used as a form of greeting, to allow a router to discover other adjacent routers on its local links and networks. The messages establish relationships between neighboring devices (called adjacencies) and communicate key parameters about
how OSPF [6] is to be used in the autonomous system or area. The Database Description messages contain descriptions of the topology of the autonomous system or area. They convey the contents of the link-state database (LSDB) for the area from one router to another. Communicating a large LSDB may require several messages to be sent by having the sending device designated as a master device and sending messages in sequence, with the slave (recipient of the LSDB information) responding with acknowledgements.

**Link State Request**: These messages are used by one router to request updated information about a portion of the LSDB from another router. The message specifies exactly which link(s) about which the requesting device wants more current information[2].

**Link State Update**: These messages contain updated information about the state of certain links on the LSDB. They are sent in response to a Link State Request message, and also broadcast or multicasted by routers on a regular basis. Their contents are used to update the information in the LSDBs of routers that receive them.

### 3. Implementation

OSPF & CSPF defines the following overlapping categories of routers:

- **Internal Router (IR)** has all its interfaces belonging to the same area.
- **Area Border Router (ABR)** is a router that connects one or more areas to the main backbone network. It is considered a member of all areas it is connected to. An ABR keeps multiple copies of the link-state database in memory, one for each area to which that router is connected.
- **Autonomous System Boundary Router (ASBR)** is a router that is connected by using more than one routing protocol and that exchanges routing information with routers autonomous systems. ASBRs typically also run an exterior routing protocol (e.g., BGP), or use static routes, or both. An ASBR[4] is used to distribute routes received from other, external ASs throughout its own autonomous system. An ASBR creates External LSAs for external addresses and floods them to all areas via ABR. Routers in other areas use ABRs as next hops to access external addresses. Then ABRs forward packets to the ASBR that announces the external addresses. The router type is an attribute of an OSPF process. A given physical router may have one or more OSPF processes. In addition to the four router types, OSPF & CSPF uses the terms designated router (DR) and backup designated routers (BDR), which are attributes of a router interface.

- **Designated router (DR)** is the router interface elected among all routers on a particular multi-access network segment, generally assumed to be broadcast multi-access. The basic neighbor discovery process (Hello),...
distance to the current assigned value and assign the smaller one.

Step 4: When we are done considering all of the 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.

Step 5: If the destination node has been marked visited or if the smallest tentative distance among the nodes in the unvisited set is infinity, then stop. The algorithm has finished.

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

5. Conclusion & Future Scope

The OSPF routing policies for constructing a route table are governed by link cost factors (external metrics) associated with each routing interface. Cost factors may be the distance of a router (round-trip time), data throughput of a link, or link availability and reliability, expressed as simple unit less numbers. This provides a dynamic process of traffic load balancing between routes of equal cost.

When these protocols are implemented on a centralized server which guides all the remaining routers then the work load on each router will be minimized. This prevents individual management of packet routing by all the base stations/hosts. Therefore all the base stations need not take care of themselves regarding the packet routing.

References


