A Study on Efficient Route Optimization using Border Gateway Protocol in Mobile Adhoc Networks

N.Vijay kumar[1], T.Santhi Sri[2], Dr.J.Rajendra Prasad[3], Y.Vijayalakshmi[4]
II MCA II Semester, PVP SIT, Vijayawada, India[1]
Department of CA, PVP SIT, Vijayawada, India[2, 4]
Department of IT, PVP SIT, Vijayawada, India[3]

Abstract

Mobile Adhoc networks are being developed for a variety of applications. Routing for communication operations in such Mobile Adhoc networks is crucial and challenging. This paper studies the problem of determining different types of Routings for packet transmission over a multi-hop communication path using modulation scaling. The goal is to optimize the path selection overall nodes while satisfying a specific latency constraint. This paper presents (to the best of our knowledge) the first in-depth analysis of different routing protocols; among those basically concentrate on Border Gateway Protocol. In this BGP how to route while transmission the data and how to filter the routes, different parameters by taking into considerations we propose to optimize the route for data transmission.

Keywords: *Mobile Adhoc Networks (MANETS), Border Gateway Protocol (BGP).*

I. INTRODUCTION

The Border Gateway Protocol (BGP) is an inter autonomous system routing protocol. An autonomous system is a network or group of networks under a common administration and with common routing policies. BGP is used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP). Customer networks, such as universities and corporations, usually employ an Interior Gateway Protocol (IGP) such as RIP or OSPF for the exchange of routing information within their networks. Customers connect to ISPs, and ISPs use BGP to exchange customer and ISP routes. When BGP is used between autonomous systems (AS), the protocol is referred to as External BGP (EBGP). If a service provider is using BGP to exchange routes within an AS, then the protocol is referred to as Interior BGP (IBGP).

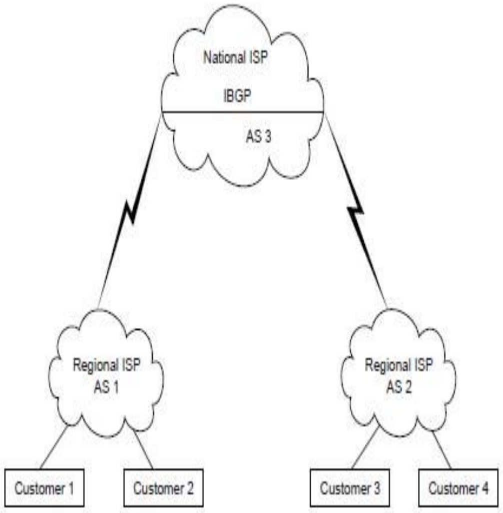

Fig 1: External and Internal BGP

BGP is a very robust and scalable routing protocol, as evidenced by the fact that BGP is the routing protocol employed on the Internet.

II. OVERVIEW OF MOBILE AD HOC NETWORKS

In MANETs communication between nodes is done through the wireless medium. Because nodes are mobile and may join or leave the network, MANETs have a dynamic topology. Nodes that are in transmission range of each other are called neighbors. Neighbors can send data directly to each other. However, when a node needs to send data to another non-neighboring node, the data is routed through a sequence of multiple hops, with intermediate nodes acting as routers. An example ad hoc network is depicted in Figure 2. There are numerous issues to consider when deploying MANETs. The following are some of the main issues. Two nodes that are in transmission range of each other are connected by a line.

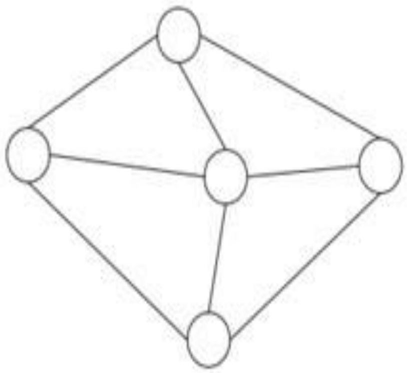

Fig. 2: An Example Ad Hoc Network, With Circles Representing Nodes

1. Unpredictability of environment: Ad hoc networks may be deployed in unknown terrains, hazardous conditions, and even hostile environments where tampering or the actual destruction of a node may be imminent. Depending on the environment, node failures may occur frequently.

2. Unreliability of wireless medium: Communication through the wireless medium is unreliable and subject to errors. Also, due to varying environmental conditions such as high levels of Electro-Magnetic Interference (EMI) or inclement weather, the quality of the wireless link may be unpredictable. Furthermore, in some applications, nodes may be resource-constrained and thus would not be able to support transport protocols necessary to ensure reliable communication on a lossy link. Thus, link quality may fluctuate in a MANET.

3. Resource-constrained nodes: Nodes in a MANET are typically battery powered as well as limited in storage and processing capabilities. Moreover, they may be situated in areas where it is not possible to re-charge and thus have limited lifetimes. Because of these limitations, they must have algorithms which are energy-efficient as well as operating with limited processing and memory resources. The available bandwidth of the wireless medium may also be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

4. Dynamic topology: The topology in an ad hoc network may change constantly due to the mobility of nodes. As nodes move in and out of range of each other, some links break while new links between nodes are created.

As a result of these issues, MANETs are prone to numerous types of faults including,

1. Transmission errors: The unreliability of the wireless medium and the unpredictability of the environment may lead to transmitted packets being garbled and thus received in error.

2. Node failures: Nodes may fail at any time due to different types of hazardous conditions in the environment. They may also drop out of the network either voluntarily or when their energy supply is depleted.

3. Link failures: Node failures as well as changing environmental conditions (e.g., increased levels of EMI) may cause links between nodes to break.

III. MULTIPATH ROUTING COMPONENTS

Multipath routing consists of three components: route discovery, route maintenance, and traffic allocation.

Route Discovery and Maintenance: Route discovery and route maintenance consists of finding multiple routes between a source and destination node. Multipath routing protocols can attempt to find node disjoint, link disjoint, or non-disjoint routes. Node disjoint routes, also known as totally disjoint routes, have no nodes or links in common. Non-disjoint routes can have nodes and links in common. Refer to Figure 3 for examples of the different kinds of multipath routes.

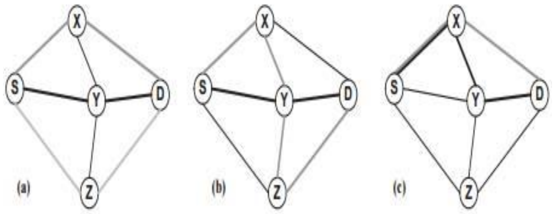

Fig. 3: Routes SXD, SYD, and SZD in (a) have no links or nodes in common and are therefore node disjoint. Routes SXYZD and SYD in (b) have node Y in common and are therefore only link disjoint. Routes SXD and SXYD in (c) have node X and link SX in common and are therefore non-disjoint.

Disjoint routes offer certain advantages over non-disjoint routes. For instance, non-disjoint routes may have lower aggregate resources than disjoint routes, because non-disjoint routes share links or nodes. In principle, node disjoint routes offer the most aggregate resources, because neither links nor nodes are shared between the paths. Disjoint routes also provide higher fault-tolerance. When using non-disjoint routes, a single link or node failure can cause multiple routes to fail. In node or link disjoint routes, a link failure will only cause a single route to fail. However, with link disjoint routes, a node failure can cause multiple routes that share that node to fail. Thus, node disjoint routes offer the highest degree of fault-tolerance.

The main advantage of non-disjoint routes is that they can be more easily discovered. Because there are no restrictions that require the routes to be node or link disjoint, more non-disjoint routes exist in a given network than node or link disjoint routes. Because node-disjointedness is a stricter requirement than link disjointedness, node-disjoint routes are the least abundant and are the hardest to find. It has been shown that in moderately dense networks, there exist a small number of node disjoint routes between any two arbitrary nodes, especially as the distance between the nodes increases [5]. This is because there may be sparse areas between the two nodes that act as bottlenecks. Given the trade-offs between using node disjoint versus non-disjoint routes, link disjoint routes offer a good compromise between the two. In the following subsection, we review some of the proposed multipath protocol for finding node disjoint, link disjoint, and non-disjoint paths.

IV. BGP OPERATION

BGP is a protocol between two BGP speakers, which are called *peers*. Two routers become BGP peers when a TCP connection is established between them.

- BGP peer sessions start in the "Idle state". In this state, BGP refuses all incoming BGP connections and does not allocate resources to peers. When you trigger a Start event by enabling a peer, the router initiates a TCP connection to the peer and moves that peer session into the Connect state.
- If the TCP connection attempt to a peer fails, the session moves into the "Active state", waits until its Connect Retry time expires, then tries to establish the connection again.
- When the TCP connection is established, BGP peers immediately identify themselves to each other by simultaneously sending *open* messages, and move into the "OpenSent state". The open messages let the peers agree on various protocol parameters, such as timers, and negotiate shared capabilities.
- When each router receives an open message, it checks all the fields. If it “disagrees” with the contents of the open message, it sends a *notification* message, closes the connection and goes into the "Idle state".
- If it finds no errors, it moves into the "OpenConfirm" state and sends back a keep alive message. When both routers have received a keep alive message, they move into the Established state. The BGP session is now open. BGP sessions typically stay in the Established state most of the time. They only leave the Established state if an error occurs, or the hold time expires with no contact from the far end.

A. BGP Path Selection

BGP could possibly receive multiple advertisements for the same route from multiple sources. BGP selects only one path as the best path. When the path is selected, BGP puts the selected path in the IP routing table and propagates the path to its neighbours. BGP uses the following criteria, in the order presented, to select a path for a destination:

- If the path specifies a next hop that is inaccessible, drop the update.
- Prefer the path with the largest weight.
- If the weights are the same, prefer the path with the largest local preference.
- If the local preferences are the same, prefer the path that was originated by BGP running on this router.
- If no route was originated, prefer the route that has the shortest AS_path.
- If all paths have the same AS_path length, prefer the path with the lowest origin type (where IGP is lower than EGP and EGP is lower than incomplete).
- If the origin codes are the same, prefer the path with the lowest MED attribute.
- If the paths have the same MED, prefer the external path over the internal path.
- If the paths are still the same, prefer the path through the closest IGP neighbour. Prefer the path with the lowest IP address, as specified by the BGP router ID.

B. BGP Route Filtering

BGP route filtering enables network providers to control their routing tables and meet the terms of business relationships they have with the networks they are connected. As a provider, you can filter the routing information that your routers receive from the networks they connect to, and that they advertise to those networks. This gives you control over the path of any traffic originating from or traversing your network. Usually, one or more of your BGP routers form peer relationships with BGP routers at other ISPs with which you have entered into data transporting agreements. The process of BGP filtering is, in effect, the process of specifying the routes that your routers send or receive from each of their peers.

There are three filter types that you can apply to the BGP update messages that your router exchanges with a particular BGP peer:

AS path filters:

Path filters look at the AS path attribute in update messages. If the attribute in the update message matches the filter criteria then the whole update message is filtered out (or accepted, depending on what action the filter entry has been configured to carry out).

Prefix filters:

Prefix filters look at the individual prefixes within an update message, and compare them against an IP routing filter. If a prefix within the update message matches the filter criteria then that individual prefix is filtered out (or accepted).

Route maps:

Route maps have a complex combination of match criteria and actions. When applied to a BGP peer, they can:

- Accept or reject update messages on the basis of origin, community, AS path or MED

- Accept or reject particular routes, by comparing the update message's routes with a prefix list

- Alter the attribute values in matching update messages.

You can use filters in both the incoming and outgoing directions. In the incoming direction, they filter the update packets that the router receives from the peer. In the outgoing direction, they filter the update packets that the router sends to the peer.

If you create more than one type of filter, the router first applies the AS path filter, then the prefix filter, then the route map. Note that the router stops checking after the first filter entry that excludes the update or prefix, so an update or prefix is only included if all the applied filters result in it being included.

V. CONCLUSION

In this paper we have proposed a multipath routing protocol BGP which optimizes the routing process by considering node disjoint, link disjoint and route disjoint paths. Both BGP path selection and BGP path filtering protocols help optimizing route discovery process.

REFERENCES

[1] Hedrick, C.: Routing Information Protocol. Internet Request For Comments 1058 (1988).

[2] Johnson, D.B., Maltz, D.A.: Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Computing. (1996) 153-181.

[3] Halabi, Bassam. Internet Routing Architectures. Cisco Press: Indianapolis, 1997.

[4] Border Gateway Protocol version 4 (BGP-4) Software Release 2.7.1 C613-03091-00 REV A.

[5] Ye, Z., Krishnamurthy, S.V., Tripathi, S.K.: A Framework for Reliable Routing in Mobile Ad Hoc Networks. IEEE INFOCOM (2003).