Self-limiting adaptive protocols for controlled flooding in ad hoc networks

Larry Hughes and Ying Zhang
Electrical and Computer Engineering Department
Dalhousie University
Halifax, Nova Scotia, B3J 2X4, Canada
larry.hughes@dal.ca yzhang@dal.ca

Abstract

The growing popularity of ad hoc networks is making their limitations, such as bandwidth and power restrictions, more apparent. As a result, techniques that reduce power consumption, reduce traffic, and restrict flooding, are of growing importance. In this paper, a series of adaptive, connectionless protocols are presented, which, when working with location-aware nodes, can reduce the number of nodes involved in a transmission. Simulation results show that the protocols reduce the processing requirements on each mode, thereby addressing issues such as bandwidth utilization and power consumption.

1. Introduction

A mobile ad hoc network (MANET) is a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized communication [5]. Like most wireless networks, a MANET is both power and bandwidth sensitive. Communication in a MANET poses special challenges because the network is infrastructureless and topologically dynamic.

A number of MANET protocols have been proposed, including on-demand protocols for saving bandwidth, such as LAR [2], DSR [7] and CBRP [6], and for power saving, such as power-aware localized routing [9] and energy conserved routing [1].

Flooding is the most commonly used scheme in ad hoc routing protocols. In flooding, the source node broadcasts its packet to all its neighbouring nodes. Each neighbour node, upon receiving the packet, checks if it received the same packet previously, if so it discards the packet, otherwise, it rebroadcasts the packet to its own neighbours. Flooding is simple and effective; however, when the number of the nodes in the network increases, the traffic caused by flooding will increase tremendously. Therefore, the problem of bandwidth utilization and power consumption becomes even more prominent.

Cartesian Ad hoc Routing Protocols (CARPs) [4] are a set of three adaptive, connectionless protocols that address the problems of routing and power consumption in MANETs; they are loosely based on the Cartesian Routing Protocol [3]. Each protocol operates at the physical layer and the network layer; all nodes are location aware. The protocols designed for CARP have three objectives: restrict flooding, reduce power consumption, and save bandwidth.

2 CARP

All Cartesian Ad hoc Routing Protocols attempt to restrict transmission to those nodes that lie between the source and the destination. The protocol is used to limit the number of forwarding nodes in a logical *transmission area*.

As nodes in the network are location aware, when a source node transmits a packet, a logical rectangular transmission area is formed by comparing the coordinates of the source and destination node (see Figure 1); the nodes in the shadowed areas are excluded from the communication process. As the packet approaches the destination, forwarded by the intermediate nodes, the size of the transmission area is reduced, eliminating nodes from outside the area, thereby limiting traffic to within the transmission area. This is the algorithm used in Location Aided Routing (LAR) Scheme 1. Based on this concept, CARP tries to optimize the transmission area by using some simple calculation with the same location information. CARP allows any transmitting node to vary the size of the transmission area associated with a packet, adapting it to the density of the nodes.

The source and destination nodes are at opposite ends of the transmission area; each node within the transmission area is referred to as an *intermediate node*. A *current node* is a node that is forwarding a packet. Initially, the source node is the current node.

In addition to its payload, a CARP packet consists of the source address, the destination address, and transmis-

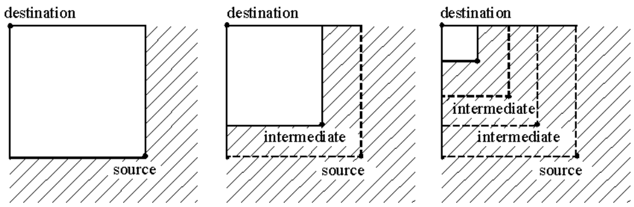

Figure 1. Bounding box reduced by hop

sion area information. At a minimum, the transmission area information is the address of the current node (x_c, y_c).

CARP resides between the MAC and MANET layer (see Figure 2). When a node receives a packet, the *Location Verification* subsystem determines whether the node is inside a packet's transmission area. If it is, the packet is forwarded to the upper layer. After processing the packet, the upper layer protocol passes the packet to the *Transmission Area Creation* subsystem to create a new transmission area for the next hop. The MANET protocols can use CARP algorithms to restrict flooding. Packet processing at nodes outside of the transmission area will be stopped at the CARP layer. Since CARP requires less processing than the table look-up and packet processing procedures found in most MANET protocols, the entire processing time at each individual node can be reduced, thus the overall efficiency of the MANET protocol will be improved.

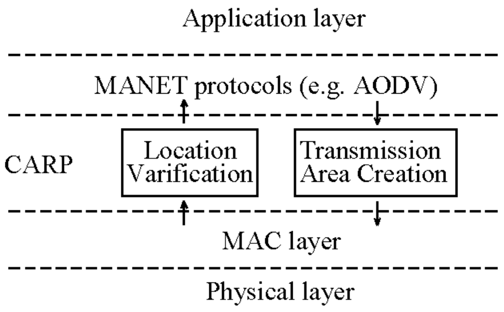

Figure 2. Application of CARP

Since the destination may move during a transmission, an "expected zone" is created. The expected zone is defined as a circle with radius r_{exp} centered at the destination. This is where the destination will most probably be found at the time when the destination receives the packet [8]. A node can determine whether it is inside the zone by calculating the distance between itself and the destination.

3 The CARP algorithms

Three CARP algorithms are implemented in the Location Verification and the Transmission Area Creations subsystems.

3.1 Trimmed Transmission Area (TTA)

Although the LAR Scheme described above reduces traffic, the volume of the flooding traffic can be problematic in a very dense network. The Trimmed Transmission Area (TTA) algorithm attempts to modify the shape through a simple optimization.

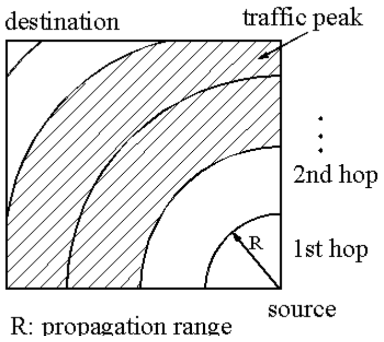

Figure 3. Transmission by hops

Figure 3 shows the packet forwarded by the intermediate nodes inside the transmission area. Each arc indicates the maximum transmission distance of each hop. Since the shadowed region accounts for the largest percentage of the entire transmission area, a traffic peak is formed here. To reduce unnecessary traffic, the TTA algorithm trims two corners off the transmission area, as shown in Figure 4. Each trimmed region is an arc with radius r. Trimming these two regions eliminate nodes that have a longer route length than nodes in the remaining part of the rectangular transmission area. This can be observed when comparing route 1 with route 2 in Figure 4.

In the packet format, the "transmission area information" field for the TTA algorithm consists of two subfields: the value of r and the current node address (x_c, y_c).

3.1.1 Transmission area creation subsystem

To determine the shape of the transmission area, the radius r of the trimmed areas is required. Two factors must be taken into consideration when deciding this value:

1. The size of the rectangular transmission area, determined from the source and destination locations. As

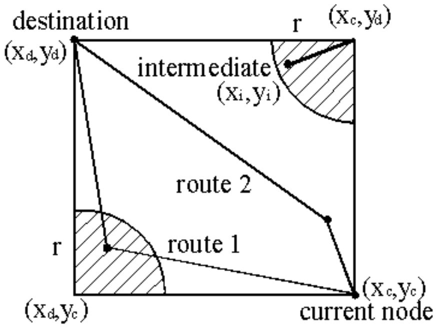

Figure 4. Trimmed transmission area

the protocol is location-aware, the co-ordinates of the current node and destination, (x_c, y_c) and (x_d, y_d) respectively, are known. The co-ordinates of the other two corners, (x_c, y_d) and (x_d, y_c), as shown in Figure 4, can be observed from the coordinates of the current and destination node. From this information, the size of the transmission area can be calculated. The value of r should not exceed the minimum of the length and width of the rectangular.

2. The density of the network, determined from the number of responses the node received in the previous transmissions. The value of r can be made adaptive to the density of the network, that is, the denser the network, the larger the value of r.

When the source initially creates the packet, it uses its initial value of r and its coordinates (x_s, y_s) as "source address" and "current node address". Should the destination fail to respond to a packet, the source can decrease the value of r and retransmit.

3.1.2 Location verification subsystem

The Location Verification subsystem is used to determine whether a node is inside the transmission area. Given an intermediate node with co-ordinates (x_i, y_i), the distances of the node to the two corners, D1 and D2 respectively, are:

$$D1 = \sqrt{(x_i - x_c)^2 + (y_i - y_d)^2} \tag{1}$$

$$D2 = \sqrt{(x_i - x_d)^2 + (y_i - y_c)^2} \tag{2}$$

The node is located within the trimmed regions when either $D1 < r$ or $D2 < r$, requiring the node to discard the packet; otherwise the packet can be forwarded.

The node can determine whether it is inside the expected zone by simply calculating the distance to the destination.

$$D_{exp} = \sqrt{(x_i - x_d)^2 + (y_i - y_d)^2} \tag{3}$$

If $D_{exp} < r_{exp}$, the node is located in the expected zone. Nodes located in the expected zone will just flood the packet instead of using the TTA algorithm for the following reasons:

1. It will not cause much traffic since there are few nodes inside this zone;
2. The destination is not at exactly the same location indicated in the packet at time t', so it would be easier to catch the destination by flooding.

Upon receiving a packet, the intermediate node first verifies whether it is inside the transmission area or not. If it is, the transmission area information is then updated with the new value of r and the node's address (x_i, y_i) as the new current node address (x_c, y_c). The packet is then forwarded to the upper layer protocols. These values are used by the downstream nodes, which follow the same procedure.

3.2 Transmission Area with Limiting Angle

Although traffic is reduced in the TTA algorithm, the shape of the transmission area is irregular. To further reduce the number of potentially unnecessary transmissions caused by the irregular shape, a transmission area with a *limiting angle* is proposed.

The limiting angle, ϕ, defines the shape of the transmission area between the current node, C, and the destination node, D, as shown in Fig. 5. Each intermediate node forms an angle ϕ_i with the current node and the destination node.

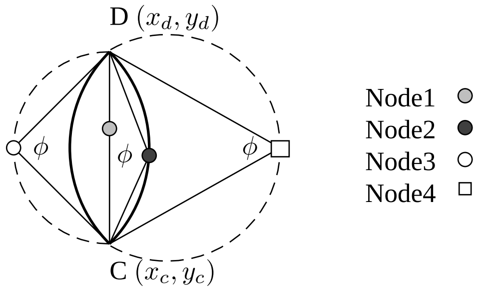

Figure 5. Transmission area with limiting angle

The transmission area information for this algorithm includes the value of ϕ and the current node address (x_c, y_c).

3.2.1 Transmission Area Creation Subsystem

Table 1 shows the relationship between ϕ and the shape of the corresponding transmission area. As the value of ϕ de-

Table 1. Nodes in the network

ϕ	Shape of Transmission Area	Example	Path Length
180°	Line connecting current node and destination	Node1	Shortest
90°..180°	Two symmetric minor arcs	Node2	↓
90°	Circle	Node3	
0°..90°	Two symmetric major arcs	Node4	Longest

creases, the size of the transmission area increases, potentially adding more nodes to the area, increasing the possible route length, and the number of packets. Therefore, there is a trade-off between the robustness of the protocol and the volume of traffic. Different ϕs can be defined based upon the density to determine the shape of the transmission area: the greater the density, the larger the value of ϕ.

Initially, the source node includes its own address (x_s, y_s) in the field of "source address" and "current node address" of the packet. It chooses a value of ϕ based on its knowledge of the network density, which is obtained from the historic statistics the node keeps in the previous communications.

3.2.2 Location Verification Subsystem

When a packet arrives at an intermediate node, (x_i, y_i), it contains the limiting angle ϕ, and the addresses of the destination and current nodes, (x_d, y_d) and (x_c, y_c), respectively. From this, the intermediate node can determine its value of ϕ_i as follows:

$$\phi_i = \arctan \frac{(y_c - y_i)(x_d - x_i) - (y_d - y_i)(x_c - x_i)}{(x_c - x_i)(x_d - x_i) + (y_c - y_i)(y_d - y_i)} \tag{4}$$

ϕ_i is then compared with the packet's ϕ. If $\phi_i > \phi$, the packet will be forwarded; otherwise it is discarded.

When the intermediate node decides to forward the packet, it substitutes the current node address (x_c, y_c) with its own address (x_i, y_i) and chooses its own value of ϕ to create the transmission area for the next hop.

3.3 Transmission Area with Fixed Path Length

As well as making the transmission area with a limiting angle, the area can also be determined from the path length. Since nodes with a fixed path length form an ellipse, the second CARP algorithm uses an ellipse as the transmission area. In Fig. 6, the current and destination nodes are two foci of an ellipse; the distance between these two nodes is $2c$. The major axis of the ellipse is $2a$ and the minor axis of ellipse is $2b$.

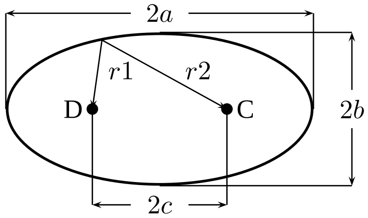

Figure 6. Ellipse

The following equations are of interest:

$$r_1 + r_2 = 2a \tag{5}$$
$$b^2 + c^2 = a^2 \tag{6}$$

All the nodes located on the ellipse boundary have the same path length $2a$, as shown in equation 5, while nodes located inside the ellipse have a shorter path length. These nodes are inside the transmission area.

An expected zone is defined as the overlapping area of a circle (centered at the destination) and the ellipse as shown in Fig. 7.

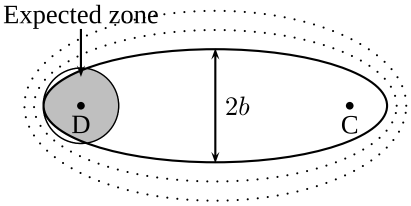

Figure 7. Fixed path length shapes

The transmission area information for this algorithm is the semiminor axis b and the current node address (x_c, y_c).

3.3.1 Transmission Area Creation Subsystem

The size of the ellipse is determined by the parameters a, b and c. When the current node tries to transmit a packet, the distance between the current node and the destination is fixed. Therefore, c is actually unchangeable. So if either a or b is decided, the size of the ellipse is fixed, as shown in equation 6. Since the semiminor axis b directly indicates the "width" of the ellipse, in the TAFP algorithm, b is made adaptive to the density of the network to change the size of the transmission area. The denser the network, the smaller the value of b.

An ellipse in a sparse network has a larger value of b than that in a dense network to include more nodes in the area. Fig. 7 shows the transmission area with different values of b in networks with different densities.

Initially, the source node includes its own address (x_s, y_s) in the field of "source address" and "current node address" of the packet. It chooses a value of b based on its knowledge of the network density, which is obtained from the historic statistics the node keeps in the previous communications.

3.3.2 Location Verification Subsystem

When an intermediate node receives a packet, it calculates the following:

1. Its distance to the current node $r1$ and to the destination $r2$;
2. Distance between the current node and destination $2c$;
3. Major axis of the ellipse $2a$ using equation 6.

If $r1 + r2 < 2a$, the node is inside the transmission area. Otherwise it is outside the transmission area, meaning that the node is not to forward the packet.

When the intermediate node decides to forward the packet, it substitutes the current node address (x_c, y_c) with its own address (x_i, y_i) and chooses its own value of b to create the transmission area for the next hop.

4 Simulation results

Four algorithms, LAR Scheme 1, TTA, TALA and TAFP have been implemented using OPNET Modeler 9.0. IEEE 802.11 is used in the MAC and physical layer. The simulation environment is defined as a 300m by 200m rectangular area with 25 nodes moving inside randomly at an average speed of 5m/s. Upon receiving a packet, nodes inside the logical transmission area formed by CARP algorithms will relay the packet to the intended destination; nodes outside of the packet will discard the packet.

The following performance metrics are evaluated in the experimental work:

- Load: total load in bit/sec (b/s) submitted to MAC layers by all other higher layers in all nodes.
- Traffic received by intermediate node: data traffic received by the station in b/s.
- Traffic sent by intermediate node: data traffic transmitted by the station in b/s.

In Figure 8, TALA is used as an example to show how much traffic is reduced by adjusting the size of the transmission area in the network. When changing the angle ϕ from $90°$ to $135°$, the size of the transmission area is reduced, thus the traffic of the network is reduced by about 85%.

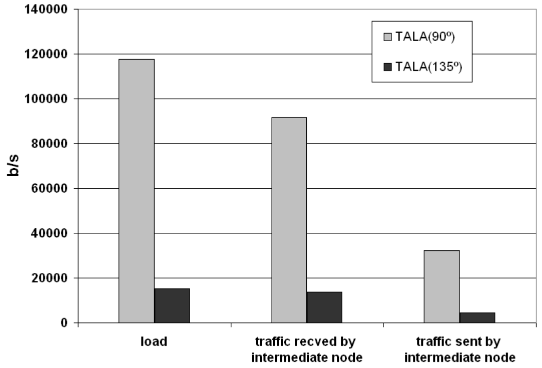

Figure 8. TALA with different angle

One main purpose of the CARP algorithm is to restrict flooding and eliminate the duplication of packet in the network. Figure 9 shows that when the source node sends one packet, the number of packets received by the destination node is reduced up to 78% while using the CARP algorithm.

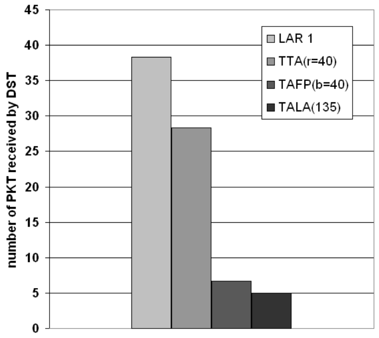

Figure 9. Number of packets received by the destination

Figure 10 is a comparison of the four algorithms. Compared to LAR Scheme 1, all three CARP algorithms reduce traffic significantly. TTA reduces less traffic due to its irregular transmission area.

Generally speaking, TALA and TAFP adjust the shape and size of the transmission area more flexibly that TTA. However, it is different to conclude which CARP algorithm outperforms the other two because as an adaptive protocol, the amount of traffic reduced by CARP depends on the

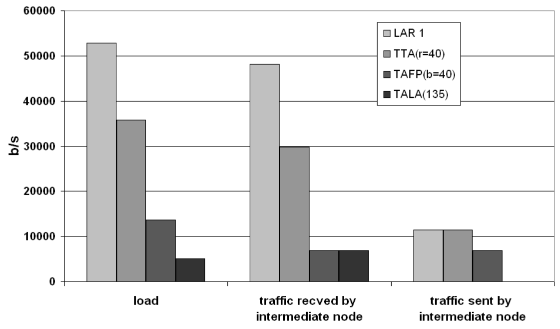

Figure 10. Comparison of the four algorithms

value of the parameters chosen by the node.

5. Concluding Remarks

This paper described the Cartesian Ad hoc Routing Protocols. These are adaptive and connectionless routing protocols which:

- restrict any flooding to within the transmission area.
- reduce power consumption of nodes outside the transmission area, since they are not involved in the communication.
- reduce the number of nodes in the communication by dynamically adjusting the transmission area.

CARP is a set of light-weight, low-overhead protocols that do not require the use of routing tables. The protocols restrict packet transmissions to the region between a source and the intended destination. The techniques employed in the three protocols allow the transmission area to be adjusted using the node density of the network.

Since flooding is a requirement in most MANET protocols, CARP can be used in conjunction with other ad hoc protocols to effectively restrict flooding. Simulation results showed that the CARP algorithms can reduce data traffic significantly compared with, for example, LAR. Also, given the simplicity of the CARP algorithms, the processing time on each node can be significantly reduced by avoiding the table look-up procedures required in most MANET protocols.

References

[1] J.-H. Chang and L. Tassiulas. Energy conserving routing in wireless as hoc networks. *Infocom*, 2000.

[2] X. Hong, K. Xu, and M. Gerla. Scalable routing protocols for mobile ad hoc networks. *IEEE Network*, August 2002.

[3] L. Hughes, O. Banyasad, and E. Hughes. Cartesian routing. *Computer Networks*, 34:455–466, 2000.

[4] L. Hughes, K. Shumon, and Y. Zhang. Cartesian ad hoc routing protocols. *Second International Conference ADHOC-NOW 2003 Montreal*, pages 287–292, October 2003.

[5] M. Ilyas. *The Handbook of Ad Hoc Wireless Networks*. CRC Press, January 2003.

[6] M. Jiang et al. The cluster based routing protocol (cbrp) for ad hoc networks. *IETF Internet Draft*, June 2003.

[7] D. Johnson et al. The dynamic source routing protocol for mobile ad hoc networks. *IETF Internet Draft*, 99, June 2003.

[8] Y. Ko and N. Vaidya. Using location information in wireless ad hoc networks. *IEEE 49th Vehicular Technology Conference*, 3:1952–1956, 1999.

[9] I. Stojmenovic and X. Lin. Power-aware localized routing in wireless networks. *IEEE International Parallel and Distributed Symp.*, 2000.