Adaptive Location Aided Mobile Ad Hoc Network Routing*

Jeff Boleng
Dept. of Computer Science
U.S. Air Force Academy
Colorado Springs, CO
boleng@ieee.org

Tracy Camp
Dept. of Math. and Computer Sciences
Colorado School of Mines
Golden, CO
tcamp@mines.edu

Abstract

We combine location information and mobility feedback to create an innovative Mobile Ad Hoc Network (MANET) routing protocol which we demonstrate is effective over a wide range of mobility conditions typical in a MANET. We use link duration as our mobility feedback metric, and we demonstrate that mobility feedback using link duration effectively enables adaptive MANET protocols. Using our mobility feedback agent, we develop a hybrid MANET routing protocol which adapts between two MANET routing protocols in order to combine the strengths of both component protocols while avoiding their weaknesses. Our hybrid, adaptive protocol achieves data packet delivery ratios above 80% in VERY demanding network mobility conditions (i.e. link durations less than 4 seconds). In more stable networks (i.e., link durations more than 15 seconds), our protocol achieves data packet delivery ratios above 90%. While other existing MANET routing protocols can achieve similar data packet delivery ratios in more stable networks, no other existing MANET routing protocol can achieve such high performance in VERY unstable networks.

I. Introduction

Ad hoc networking involves computers, typically wireless mobile nodes (MNs), that cooperatively form a network without specific user administration or configuration. In other words, ad hoc networking allows an arbitrary collection of MNs to create a network on demand. A node in the ad hoc network, whether it be a laptop, autonomous agent, or sensor, is in charge of routing information between its neighbors, thus maintaining connectivity of the network.

There are numerous scenarios that do not have an available network infrastructure which could benefit from the creation of an ad hoc network:

- rescue/emergency operations: rapid installation of a communication infrastructure during a natural/environmental disaster, or a disaster due to terrorism, that demolished the previous communication infrastructure;
- law enforcement activities: rapid installation of a communication infrastructure during special operations;
- tactical/military missions: rapid installation of a communication infrastructure in a hostile and/or unknown territory.

For these reasons, ad hoc networks have been a major focus of research in the last few years (see the reference lists below). We assume the environment for creating an ad hoc network is a broadcast physical medium with limited range, such as the physical medium offered by infrared or radio frequency wireless communications.

There are many challenges in the creation of an ad hoc network: routing challenges (i.e., how to route information to a mobile node that is, perhaps, moving rapidly), wireless medium challenges (e.g., lower bandwidths, higher error rates, more frequent disconnections, and less security than fiber lines), and portability challenges (e.g., lower power than desktop computers). Although experts initially considered only ad hoc networks for a small group of cooperating nodes, many experts now envision very large groups of MNs located over a large geographical area belonging to the same ad hoc network as well. Thus, scalability is another challenge that exists in the creation of an ad hoc network.

Since wireless computing devices are becoming more portable, network-oriented, and popular, the interest in ad hoc networking is growing. This interest is observable by the recent appearance of numerous proposals for routing in an ad hoc network [9], [11], [12], [16], [24], [32], [33], [36], [38], [42], by the formation of a working group in the Internet Engineering Task Force (IETF) [30][1], and by multiple Internet drafts for routing in a mobile ad hoc network (MANET) [2], [10], [18], [19], [25], [35], [43]. Reviews of unicast routing protocols are provided in [28], [39] and [40], and performance evaluations for some of these protocols are provided in [6], [8], and [23].

Location information has recently been applied to MANET protocols in order to improve the performance of a protocol, to enable scalability, or both [1], [26], [27], [29], [44]. The application of location information has demonstrated performance improvements and promised dramatic scalability [8], [26]. As a result, much of our research involves protocols that use location information.

A. Motivation

In contrast to wired networks, routing in mobile ad hoc networks is challenged by a complicated interaction of three

*This work supported in part by NSF Grants ANI-0073699 and ANI-0208352. Research group's URL is *http://toilers.mines.edu*. Reference for this manuscript: Technical Report MCS-03-09, The Colorado School of Mines, June 2003.

[1]The charter of the IETF Mobile Ad Hoc Networks (MANET) Working Group is to develop a solution for routing in an ad hoc network.

fundamental difficulties. First is contention. The nature of mobile computing devices demands wireless communication. The nature of wireless communication results in significant contention for the shared medium (the wireless channel). Second is congestion. Another aspect of wireless communication is decreased bandwidth which results in much higher congestion when compared to a similar wired network configuration. The links between wireless nodes can support less data traffic than is attainable with wired connections.

Finally, and most importantly, is the unique set of challenges created by mobility. Node mobility in MANETs makes communication links break, and these breaks may occur at a rapid rate. This changing network topology is the key challenge that MANET routing protocols must overcome. Several existing MANET routing protocols have been proposed that deal with this mobility problem in different ways. These protocols and their mechanisms are described in Section I-B. Any attempt to provide effective routing mechanisms in MANETs must deal with the changing network topology created by mobility.

In addition to mobility, contention, and congestion, MANET protocols must deal with other significant issues. Mobile computing devices are often battery powered and therefore have limited power and lifetime. They may also be constrained by limited memory or processing capabilities. These additional factors combine with the above three key challenges to make routing in Mobile Ad Hoc Networks extremely difficult.

Our research goals are aimed at improving the effectiveness and scalability of routing in MANETs, especially in VERY demanding network mobility conditions. More specifically, this research enables MANET routing protocols to adapt their operation based on the current network mobility conditions present. The delivery and use of location information, when combined with adaptive protocols, promises dramatic improvements.

B. Related Work

In this section, we categorize the current proposed unicast routing protocols for an ad hoc network. We begin with unicast routing algorithms which do not use location information, then we discuss the inclusion of such information. Details on protocols that directly impact our research are presented in [8].

1) Unicast Routing Protocols: Many unicast routing protocols have been proposed for ad hoc networks. There are two primary approaches to routing in MANETs, and as a result existing protocols can generally be grouped into one of three categories. The first type of MANET protocols are proactive routing protocols, which include The Wireless Routing Protocol (WRP) [31], Destination-Sequenced Distance Vector Routing (DSDV) [37], Optimized Link State Routing Protocol (OLSR) [10], Topology Broadcast based on Reverse Path Forwarding (TBRPF) [2], and Fisheye State Routing (FSR) [14]. These protocols proactively maintain network topology through the periodic exchange of control information. In general, proactive protocols are not responsive enough and have too much overhead to be effective when nodes are mobile [6].

The second type of MANET protocols are reactive routing protocols, which include Dynamic Source Routing (DSR) [25], Ad Hoc On-Demand Distance Vector (AODV) [35], and Associativity Based Routing (ABR) [43]. The key to the operation of these protocols is that routes to destinations are only determined and maintained when they are needed (i.e., data is being sent). Unlike proactive protocols, no effort is made to maintain the total network topology. This class of protocols has shown to be more effective when nodes are mobile [40].

The third category of MANET protocols are hybrid in nature. These protocols combine proactive and reactive techniques, and include the Zone Routing Protocol (ZRP) [18] and [19], The Bordercast Resolution Protocol [17], the Temporally-Ordered Routing Algorithm (TORA) [34], and the Landmark Routing Protocol (LANMAR) [13]. As an example of a hybrid MANET protocol, consider ZRP. ZRP defines a zone around each node where the local topology is proactively maintained via the Intrazone Routing Protocol (IARP) [19]. When routes are required outside the local zone, a reactive route discovery mechanism is used via the Interzone Routing Protocol (IERP) [18].

2) Unicast Routing Using Location Information: A number of recent MANET unicast routing protocols use location information. Six of these protocols are the Location-Aided Routing (LAR) algorithm [27], the Distance Routing Effect Algorithm for Mobility (DREAM) [1], the Greedy Perimeter Stateless Routing (GPSR) algorithm [26], the Geographical Routing Algorithm (GRA) [22], the Geographic Distance routing (Gedir) protocol [41], and the GRID protocol [29]. A review for some of these protocols is provided in [44]. The results presented in [8] show that the use of location information in an ad hoc network significantly improves routing performance of unicast communication.

In these location-based routing protocols, each node maintains a location table that records the location of each other node and the time at which that location information was received. A sender node then uses this information (perhaps combined with a directional antenna [20], [45]) to improve the efficiency in the transmission of packets.

C. Organization

In the remainder of the paper, we present an innovative MANET protocol which uses both feedback for adaptation and location information to improve routing performance. The use of location information has been shown to increase the performance of unicast routing [8]. Feedback is provided by a mobility metric which enables MANET protocols to adapt [4]. Link duration is proposed as an effective mobility metric in [5]. The inspiration behind the utilization of link duration as the basis for a mobility metric is due initially to [12] and [21]. These protocols use link durations to indicate the stability of an individual link or route. Unlike these protocols, we declare a low network mobility condition if nodes

are experiencing long average link durations, and a high network mobility condition if nodes are experiencing short average link durations. Using link duration to indicate network stability is different than using link duration as a measure of the goodness of links or routes. Our hybrid MANET protocol adapts between component protocols using the determined network mobility condition in real-time.

First we present our approach for the development of the Adaptive Location Aided Routing from Mines (ALARM) protocol (see Section II). Next is an overview of the protocol (see Section III) followed by a short summary of the protocol parameters in Section IV. In Section V the details of ALARM are presented, followed by a summary of the simulation parameters used for tuning and testing (see Section VI). Section VII provides a discussion of the tuning of the protocol parameters. Lastly we present and analyze the performance results of ALARM by comparing the tuned protocol with its component protocols (see Section VIII).

II. Approach

Our initial approach to protocol adaptation is to combine the LAR protocol with a directed flooding method[2]. Figure 1 illustrates that LAR is effective at delivering packets if the link duration is longer than 10 seconds. (See Tables III–VII in Section VI for simulation parameter details on Figure 1.)

Table I illustrates the relationship between link duration, speed, and pause time when the random way-point mobility model [6] is used in a simulation. Figure 1 illustrates that when network dynamics create links that break quickly, LAR is unable to "keep up with" topology changes. Other protocols (e.g., DSR, AODV, and ZRP) would also be unable to "keep up with" such a dynamic network. In other words, when VERY demanding network mobility conditions exist, the *only* solution for routing is to flood (or box flood) data packets.

When location information is available to the protocol, directed flooding can be used to reduce the number of packets transmitted in the network. Directed flooding consists of flooding the data packet in a box oriented in the direction of the destination. Such a box can be determined based on the last known location of the destination, in a manner similar to directed flooding of route request packets in LAR [8].

III. ALARM Overview

We use a link duration feedback agent [4] to create an adaptive MANET unicast routing protocol. The protocol chosen for adaptation is the Location Aided Routing (LAR) protocol originally described in [27] and further refined, tested, and evaluated in [8]. Our goal is not to create Yet Another MANET Protocol (YAMP). Instead, the goal is to optimize existing protocols and to create a mechanism to enable the combination of multiple protocols into a hybrid protocol. Our hybrid protocol uses the most effective protocol technique (i.e., LAR or directed flooding) based on the network conditions currently being experienced by a given mobile node. Ironically, for simplicity, we refer to this hybrid protocol development as a MANET protocol.

[2]Throughout this discussion, we use the terms directed flooding and box flooding interchangeably.

TABLE I
Node Speed, Pause Time, and Link Duration for the Random Waypoint Mobility Model.

Speed (m/s)	Pause Time (seconds)	Link Duration (seconds)
40	0	3.536
30	0	4.713
40	10	6.065
20	0	7.073
30	10	7.087
40	20	9.015
20	10	9.336
30	20	10.043
40	30	12.065
20	20	12.149
30	30	13.025
10	0	14.116
20	30	15.019
40	40	15.231
10	10	16.125
30	40	16.169
20	40	18.113
40	50	18.286
10	20	18.682
30	50	19.324
20	50	21.268
10	30	21.450
10	40	24.502
10	50	27.348
5	0	28.545
5	10	30.354
5	20	32.524
5	30	34.979
5	40	37.663
5	50	40.646

Our combined or hybrid protocol, Adaptive Location Aided Routing from Mines (ALARM), uses link duration feedback at each node to determine the appropriate forwarding method for data packets. When link durations of nodes on the source route in the packet header are longer than a predetermined threshold, ALARM forwards data packets along this source route (i.e., ALARM uses LAR). When link durations of a node on the source route are shorter than the threshold, that node initiates a directed flood of the data packet toward the destination. This flood is automatically "dampened" when the flooded packets reach nodes that have link durations longer than the threshold. In other words, ALARM may adapt between LAR and directed flooding multiple times as the data packet is routed from the source to the destination.

There are three possibilities for a packet which was flooded on its last hop. First, if the packet reaches a node which has

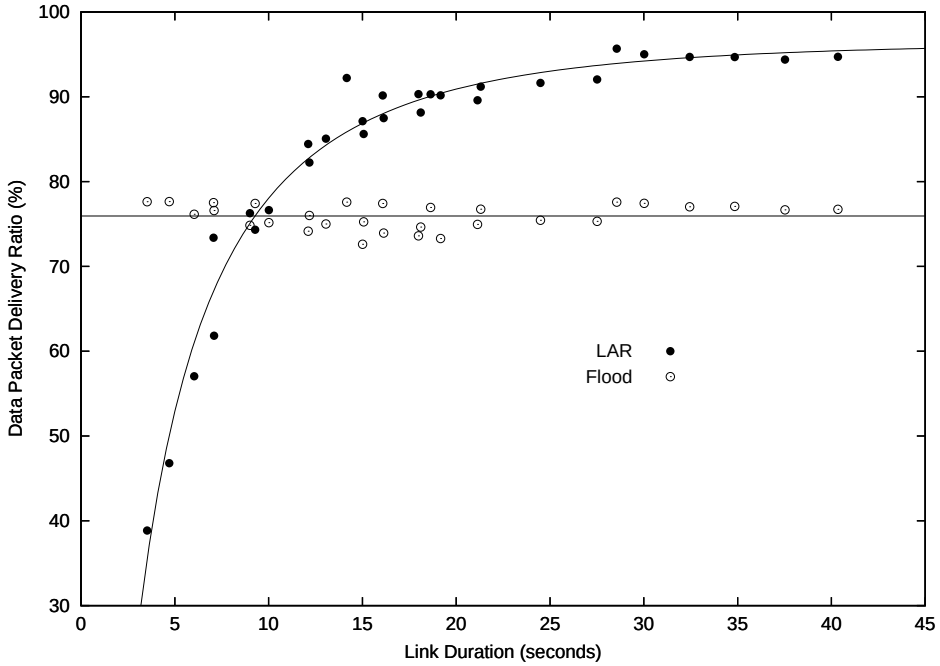

Fig. 1. Data Packet Delivery Ratio - LAR and Flood

link durations below the threshold (signaling an unstable area of the network), the packet continues to be flooded. Next, if the packet reaches a node which has link durations longer than the threshold (which signals a more stable network), one of two options is possible. If the node is on the original source route, the packet continues on the source route toward the destination. On the other hand, if the packet reaches a node with long link durations which was not on the original source route, the packet is dropped. The emphasis is on delivering packets through regions of high network instability. Either the packet reaches the final destination via directed flooding, or it picks up the original source route after flooding through a network "hot spot".

One additional detail included in ALARM is a flood horizon. The flood horizon signifies how many hops a packet continues to be flooded past the mobility hot spot. This flood horizon increases the chance that either the destination or a node on the original source route is reached. Obviously, a tradeoff between increased overhead and increased reliability exists in choosing the value of the flood horizon.

The node that initiates the directed flood (i.e., the first node reached with short link durations) unicasts an ALARM packet, via the reverse source route, to the data packet source. It is then possible for the source node to take preemptive action, such as initiating a new route discovery. Initiating a new route request before a route error is received was first discussed in [15] for DSR. In [15] low signal strength (not link duration between two nodes on the source route) is the trigger for a preemptive action.

In reactive protocols such as DSR and LAR, routes must be repaired when a link on an existing route fails. Route failures are signaled by a route error mechanism. When this occurs, the current packet that experienced the route error is either lost or incurs significant delays as a new route is determined. ALARM allows for the successful delivery of these packets, without an increase in delay, by flooding the packets through network mobility "hot spots".

IV. ALARM Parameters

The following parameters are required for the ALARM protocol to operate.

- Duration Window Size - the moving window, in seconds, that the link duration is averaged by the feedback agent,
- Link Duration - current link duration averaged over the last duration window seconds,
- ALARM Threshold - when the link duration falls below a threshold, the protocol adapts, and
- Flood Horizon - the number of hops that a flooded data packet continues to flood past a mobility "hot spot".

The duration window size (WS) is the length of time the feedback agent uses to average the previously heard links when determining the current link duration. A value for WS is supplied to the feedback agent which in turn reports back the current link duration for the node. The link duration supplied is a measure of the average link duration for all the node's one hop neighbor links. In other words, this average represents the current network stability for the node. Based on the feedback agent discussion in [4] we use a duration window size of 30 seconds. ALARM threshold and flood horizon are the key ALARM parameters. A detailed discussion of protocol optimization using these parameters occurs in Section VII.

Finally, the calculation of the information provided by the feedback agent depends on three key parameters:

TABLE II
FEEDBACK AGENT PARAMETERS

Beacon Period	1 second
Link Break Time	3 seconds
Duration Window Size	30 seconds

- beacon period, which controls the frequency of the feedback beacon during active mode operation (see [4]),
- link break time, which indicates how much time can pass without traffic on a current link before that link is declared broken, and
- duration window size, which is provided by the ALARM protocol.

See Table II for the values of these parameters in all our simulations. We note that our feedback agent (described in [4]) is designed to promiscuously gather link duration information when sufficient data traffic is present. Since our traffic scenarios provide sufficient traffic (see Table VI), no additional overhead is contributed by the feedback agent in the simulation results presented herein. In other words, the default beacon period of 1 second is never needed.

V. ALARM DETAILS

This section presents the ALARM protocol algorithm as pseudo code. We discuss both the protocol and implementation details.

Sender

Send Data Packet

```
if (LinkDuration < ALARMThreshold)
{
  if (no source route)
  {
    Initialize source route to Null
  } else {
    Use source route from local route table
  }
  Initialize FloodHorizon
  Box flood data packet
} else {
  Initialize FloodHorizon to zero
  use LAR algorithm to send packet
}
```

Receive ALARM packet

```
Increment number of received alarms for
  node which sent alarm
if (alarms[node] > ALARM route error trigger)
{
  send Route Request packet
}
```

We note the following features in the sending algorithm:

- The sending node (source of a data packet) determines if it is experiencing high network mobility (short link durations). If it is, then it uses a box flood to send the data packet. Otherwise, the packet is sent by LAR.
- If there is an existing *good source route*, i.e., one which is recent and has not experienced a previous route error, ALARM includes the route within a flooded data packet.
- If the sending node does not have a *good source route*, then the data packet is box flooded with a null source route. The LAR route request/reply mechanism has little chance of success when a sending node is experiencing very short link durations.

Forwarding Node

Receive Packet for Forwarding

```
if (PacketType in
    [routeRequest, routeReply,
     routeError, ALARMpacket])
{
  use LAR algorithm to forward
    or reply to packet appropriately
} else if (PacketType == Data) {
  if (source route is Null)
  {
    if (source route in local route table)
    {
      Add route to data packet header
    } else {
      Initialize FloodHorizon
      Box flood data packet
      return
    }
  }
  if ((LinkDuration < ALARMThreshold)
              or
      (routeError detected))
  {
    if (this is the first node to
        initiate box flood)
    {
      Send ALARM packet to source
        of data packet
    } else if (routeError detected) {
      Send routeError packet
    }
    Initialize FloodHorizon
    Box flood data packet
  } else {
    if (FloodHorizon > 0)
    {
      Decrement FloodHorizon
      Box flood data packet
    } else {
      use LAR algorithm to send packet
    }
  }
}
```

We note the following action by the sending node upon receipt of an ALARM packet:

- When a sending node receives an ALARM packet, it records which node sent the packet.

- When some threshold of ALARM packets have been received, an LAR-style route request is triggered. We use a value of *three* received ALARMs from one intermediate node as an indication of an imminent route break. This condition invalidates all the routes which use that link and triggers a route request/reply cycle for the route and destination affected. When a newer route is discovered for a destination, for instance by promiscuous listening, the ALARM counter is reset for each node on the new route.

We note the following features in the forwarding algorithm:

- If the packet is not a data packet, handle it using LAR.
- If the source route in the received data packet is null, check the local route table for a route. If a *good route* is in the local route table, insert it into the data header and continue with the ALARM algorithm. If there is not a *good route* to the destination in the local route table, re-initialize FloodHorizon and continue box flooding the data packet.
- If the data packet is received by a node that is experiencing network instability or has detected a route error, re-initialize the FloodHorizon and box flood the data packet. If this node is the initiator of the box flood, send an ALARM packet to the data packet originator. If this node detected the route error, send a route error packet to the data packet originator. We note that every node experiencing network instability re-initializes FloodHorizon. Thus, the dampening procedure begins when the packet has passed the mobility "hot spot".
- If the flood horizon is greater than zero, the node is not experiencing network instability, and has not detected a route error, continue to box flood the packet and decrement the flood horizon.
- If a data packet is received by a node that is not experiencing network instability, the packet's flood horizon equals zero, and the node is not on the original source route, drop the packet. In other words, the flood is dampened.
- If a data packet is received by a node that is not experiencing network instability, the packet's flood horizon equals zero, and the node is on the original source route, the data packet is unicast to the next node in the route via LAR.

VI. Simulation Environment

The goal of simulating network protocols is to test their effectiveness in a wide range of network conditions. This section contains the specific simulation parameters which are used for all results presented herein. The discussion of parameters in this section corresponds to simulation lessons learned in previous research (see [7] and [8]).

The simulation input parameters are listed in Table III. Derived parameters (see Table IV) are calculated directly from the input parameters [3]. Node density is simply the number of nodes divided by the total simulation area. Coverage area is the area of the circle whose radius is the transmission distance. The transmission footprint of a node is the percentage of the simulation area covered by a node's transmission. It is derived from the transmission range of the node and the size of the simulation area. The maximum path length is the distance from the lower left corner to the upper right corner in the simulation area. The network diameter is the maximum path length divided by the transmission range. Finally, the average number of neighbors indicates the network connectivity. The value labeled "no edge affect" is calculated by dividing the coverage area by the node density. The value labeled "edge affect" takes into account the fact that nodes near the edges do not have neighbors on all sides of the node.

TABLE III
INPUT PARAMETERS

Simulation time	1000 seconds Note: See [8] for a discussion on the simulation duration. Specifically, the simulation duration is 2000 seconds; data, however, is only transmitted during the final 1000 seconds.
Simulation area	300x600m
Number of MNs	50
Transmission range	100m

TABLE IV
DERIVED PARAMETERS

Node density	1 node per 3,600 m^2
Coverage area	31,416 m^2
Transmission footprint	17.45%
Maximum path length	671m
Network diameter (max. hops)	6.71 hops
Average neighbors	8.73 (no edge affect)
Average neighbors	7.76 (edge affect)

We use the random way-point mobility model with the average speed and pause times shown in Table V. The data traffic model and parameters used are included in Table VI. Finally, we simulate all protocols in NS-2 with the specific parameters shown in Table VII.

In our research, we gather a standard set of performance results. The standard metrics gathered are:

- data packet delivery ratio,
- end-to-end delay,
- protocol overhead (packets and bytes per data packet delivered),
- data overhead (packets and bytes per data packet delivered), and
- total overhead (packets and bytes per data packet delivered).

We note that all overhead values (packets and bytes) are divided by the number of data packets or bytes actually delivered. In other words, we normalize results to ensure that the overhead values won't appear to improve as a result of the protocol performance degrading.

Table VIII lists the simulation parameters that we used along with those of [6] and [23] (the random scenarios). We

TABLE VIII
SIMULATION PARAMETERS

	in [6]	*in* [23]	*herein*
Simulator	NS2	NS2	NS2
Simulation time	900s	250s	1000s
Simulation area	1500x300m	1000x1000m	300x600m
Number of MNs	50	50	50
Transmission range	250m	250m	100m
Average neighbors	11.72	6.32	7.76
Movement model	random waypoint	random waypoint	random waypoint
Maximum speed	1 and 20 m/s	0-20 m/s	4.5-44 m/s
Average speed	1 and 10 m/s	not specified	5-40 m/s
Pause time	0, 30, 60, 120, 300, 600, 900 s	1 s	0-50 s
CBR sources	10, 20, or 30	15	20
Data payload	64 bytes	64 bytes	64 bytes
Packet rate	4 packets/s	5 packets/s	4 packets/s
Traffic pattern	peer-to-peer	random	peer-to-peer

TABLE V
MOBILITY MODEL

Mobility model	random way-point
Mobility model parameters for Figures 1 and 8–10	speed = [5, 10, 20, 30, 40] m/s pause time = [0, 10, 20, 30, 40, 50] seconds
Mobility model parameters for Figures 2–7	speed = [10] m/s pause time = [10] seconds

TABLE VI
DATA TRAFFIC MODEL

Traffic type	Constant Bit Rate (CBR)
Number of senders	20
Number of receivers	20
Data payload	64 bytes
Packet rate	4 packets per second
Link bandwidth	2 Mbps
Traffic pattern	communicating pairs (peer-to-peer)

compare our choices with the choices made in [6] and [23] in order to validate our choices and emphasize the increased range and difficulty of the mobility conditions presented in the results. For example, the maximum speed in [6] and [23] is 20 m/s; our maximum speed is 44 m/s. Our main goal was to evaluate ALARM in both stable and unstable network mobility conditions. Our simulation parameters accomplished this goal.

VII. ALARM OPTIMIZATION

The primary parameters in the ALARM protocol are the ALARM threshold and flood horizon. The other essential parameters (duration window size and link duration) are obtained directly from the feedback agent (see [4]). The following three points provide challenges in determining appropriate values for the two ALARM parameters. First the two

TABLE VII
SIMULATOR

Simulator Used	NS-2 (version 2.1b7)
Medium Access Protocol	IEEE 802.11
Number of Trials	10 minimum, 20 on some cases
Confidence Interval	95%

parameters are inter-dependent. They are also sensitive to the actual link duration, data load, data traffic distribution, etc. Finally, since we want to optimize ALARM for all three protocol options (the following discussion defines the three options), the process of determining values for protocol parameters becomes even more complex.

Another difficulty with a complex protocol is selecting which performance metrics to maximize, and what is considered an acceptable cost for the improvement of each performance metric. Section VI lists three performance areas:

1) data packet delivery ratio,
2) end-to-end delay, and
3) protocol overhead.

The consideration of protocol overhead is further divided in Section VI and requires evaluation of packet and byte overheads for control, data, and total transmissions. While our primary focus is on data packet delivery ratio, we discuss the cost (i.e., protocol overhead) in detail as well. Results for delay are also presented.

We optimize ALARM using a moderate link duration of 16.125 seconds, which corresponds to a random way-point mobility model scenario of 10 m/s node speed and 10 second pause times (see Table I). We evaluate five different values for the ALARM threshold, $[0, 3, 6, 9, 12]$ seconds, and five different values for the flood horizon, $[0, 1, 2, 3, 10]$ hops. Table II lists the three parameters associated with our feedback agent. Finally, there are three ALARM protocol options which we evaluate. These are described below with the corresponding label used in the following figures and discussion.

1) ALARM-all: the ALARM mechanism is used by all nodes, both sending and forwarding.
2) ALARM-fwd: the ALARM mechanism is enabled only on forwarding nodes and not the sending node.
3) ALARM-err: the ALARM mechanism is disabled except when a route error occurs.

The above combination of possibilities creates a "performance volume" for the ALARM parameters (see, for example, Figure 2). This volume has the ALARM threshold on the x-axis, the flood horizon on the y-axis, and the performance metric of concern on the z-axis. Each volume includes three surfaces which correspond to the protocol options enabled. We note that on all figures each data point represents an average of ten simulation trials. A 95% confidence interval was calculated for each point, and in all cases the intervals are quite small. These confidence intervals are not shown on the figures in order to increase their clarity.

A. Data Packet Delivery Ratio

Figure 2 shows the data packet delivery ratio for the possible values of our ALARM parameters and protocol options. The figure shows a decrease in performance for the ALARM-fwd and ALARM-all protocol options as the ALARM threshold increases. It also shows a clear ranking of the protocol options with ALARM-err performing the best, ALARM-all the worst, and ALARM-fwd in between.

We note that the only versions of ALARM-fwd and ALARM-all that perform well, compared to ALARM-err, are when the ALARM threshold is set to zero seconds (see Figure 2). Examining the algorithm in Section V reveals that both ALARM-fwd and ALARM-all operate essentially the same as ALARM-err when ALARM threshold is zero, i.e.,

```
(LinkDuration < ALARMThreshold)
```

can never occur. In other words, ALARM-fwd and ALARM-all only initiate a box flood of a data packet when a link error is detected.

Figure 3 extracts data from Figure 2 in order to aid us in understanding the ALARM threshold. ALARM-fwd and ALARM-all (with flood horizon equal to one and ten) both perform worse as the ALARM threshold increases while ALARM-err (regardless of the flood horizon) is not affected by the ALARM threshold value. Both ALARM-fwd and ALARM-all base a significant protocol decision on the ALARM threshold value, that is, whether to initiate a box flood or not. ALARM-err, on the other hand, makes flooding and dampening decisions based on link breakage only, not on the mobility value (link duration) experienced. As the ALARM threshold increases, ALARM-fwd and ALARM-all behave as a pure flooding protocol. Thus, their performances decrease appropriately.

Figure 3 also illustrates the effect of the flood horizon on the best performing protocol option, ALARM-err. A value of zero for flood horizon, which means a data packet encountering a link error is box flooded for only one hop, performs worse than when the flood horizon is increased. The other two values of flood horizon shown (one and ten) have similar delivery percentages. Other non-zero values of flood horizon perform similarly as well. In summary, ALARM-err performance improves when flood horizon is greater than zero. In the next section we examine the effect of flood horizon and ALARM threshold on protocol overhead.

B. Overhead

Figure 4 shows the protocol overhead associated with the various versions of the ALARM protocol. While we focus on control, or protocol packet overhead, all other overhead types (total packet and byte overhead) follow the same patterns. In other words, the observations and conclusions made by examining the control packet overhead are equally applicable to the other forms of overhead. As before, ALARM-err is unaffected by the ALARM threshold, while the protocol overhead for ALARM-fwd and ALARM-all increases as the ALARM threshold increases.

Figure 5 examines the protocol overhead of ALARM-err in more detail[3] This figure reveals that there is a reduction in overhead per data packet delivered when a box flooded data packet is allowed to travel past the network "hot spot" before the flooding is dampened, i.e., for values of the flood horizon greater than zero. As seen in Section VII-A, using zero hops for the value of flood horizon results in fewer delivered data packets, so the overhead ratio is higher.

While protocol packet overhead is comparable for all values of the flood horizon greater than zero (see Figure 5), Figure 6 demonstrates that greater values of the flood horizon increases the number of packets in the system due to data packet flooding. This extra flooding has been shown to have little or no benefit to delivery ratio (see Section VII-A and Figure 3).

C. End-to-End Delay

Figure 7 presents the end-to-end delay of the ALARM variants. Examining the figure reveals that end-to-end delay is stable for all three protocol options as both the flood horizon and ALARM threshold change. In all cases, end-to-end delay only varies between 0.1680 and 0.2766 seconds. Furthermore, the range of delay for ALARM-err, the variant of choice, is only 0.2295 to 0.2759 seconds.

TABLE IX
OPTIMIZED ALARM PARAMETERS

Threshold	9 seconds
Flood Horizon	1 hop

In conclusion, ALARM-err demonstrates the best data packet delivery ratio, the lowest overhead, and acceptable delay. Thus, we use ALARM-err in our comparison to LAR and Flood. We decided, based on our evaluation of protocol parameters, to set the ALARM threshold to *nine seconds* and the flood horizon to *one hop*. These values are an effective combination to ensure high data packet delivery and

[3]Again, we note that no beacon traffic exists in our simulations due to the high data load transmitted.

low overhead. Table IX summarizes our optimized ALARM parameters.

VIII. Performance Comparison: ALARM, LAR, and Flood

Our initial goal was to combine the strengths of the LAR protocol in mild to moderate mobility with the ability of flooding to effectively deliver data packets in high mobility (see Figure 1). Figure 8 demonstrates we have met our goal. The combination of directed flooding with Location Aided Routing (LAR) creates a hybrid protocol which can out-perform both component protocols when VERY unstable network conditions exist. As expected, when stable network conditions exist, ALARM performs identical to the component protocol that performs the best in that situation (i.e., LAR).

Compared to LAR and Flood, Figure 8 demonstrates that ALARM improves the delivery ratio, and Figure 9 shows that ALARM reduces protocol overhead, in VERY demanding network mobility conditions. The raw overhead of ALARM is similar to LAR; however, since ALARM delivers significantly more packets, the protocol overhead per data packet delivered is smaller for ALARM. We note that Figure 9 reports total packet transmissions since Flooding has no control packets. The entire cost associated with Flooding is only due to duplicate data packet transmissions.

Figure 10 shows the end-to-end delay for the ALARM, LAR, and Flood protocols. Flood has the lowest delay since no route request/reply cycle exists. ALARM improves upon the delay of LAR when mobility is high (i.e., link durations are short). The delay of ALARM is smaller than LAR in unstable networks since ALARM does not wait for a new route to be established. When mobility is low, ALARM and LAR have similar delays and are both comparable to the delays provided by Flood.

IX. Conclusions

The development of a hybrid protocol by combining existing protocols is an effective way to optimize protocol performance over a wide range of network scenarios. We developed an effective hybrid protocol (ALARM) which is superior to both component protocols in VERY demanding network mobility conditions. ALARM adapts between LAR and directed flooding in real-time; thus, ALARM combines the low overhead of LAR in times of mild to moderate mobility with the high delivery ratio of Flood in times of high mobility.

We note the following conclusions. First, combining two protocols (in our case, one simple and one complex) results in a much more complex protocol. Not necessarily more complex to implement or operate, but much more complicated to optimize and understand (see Section VII).

Next, recall that in ALARM-err, nodes only begin to box flood data packets when a route error occurs. The other two ALARM options preemptively box flood data packets when short link durations are experienced, regardless of whether or not the source route link is intact. Figure 2 reveals that this preemptive flooding is always a mistake. If a source route link is still active, a protocol should always use it. In other words, reactive protocols should use an available route as long as possible. The full benefit that can be derived from mobility (link duration) feedback in proactive and hybrid protocols remains an open question.

The feedback agent of [4] is inherently a proactive networking element. Coupling this proactive element with a completely reactive protocol such as LAR was not as beneficial as expected. However, our feedback agent proved beneficial in dampening of the directed flood. Our dampening mechanism allows us to obtain higher deliver ratios with minimal cost.

Finally, ALARM successfully demonstrates the effectiveness of combining protocols to exploit the strengths of each while also avoiding their weaknesses. Our hybrid, adaptive protocol achieves data packet delivery ratios above 80% in VERY demanding network mobility conditions (i.e. link durations less than 4 seconds). Since flooding (or directed flooding) is the only option in such an unstable network environment, no existing MANET routing protocol can achieve such high performance operating alone. The keys to our success are in using an effective mobility metric (such as link duration) and adding the ability to provide feedback via that metric. The application of feedback and adaptation to combine protocols opens up numerous possibilities for investigation and research.

References

[1] S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward. A distance routing effect algorithm for mobility (DREAM). In *Proceedings of the Fourth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 1998)*, pages 76–84, 1998.

[2] B. Bellur, R. Ogier, F. Templin, and M. Lewis. Topology broadcast based on reverse-path forwarding (TBRPF). Internet Draft: draft-ietf-manet-tbrpf-08.txt, April 2003.

[3] J. Boleng. Normalizing mobility characteristics and enabling adaptive protocols for ad hoc networks. In *Proceedings of the 11th Local and Metropolitan Area Networks Workshop (LANMAN 2001)*, pages 9–12, March 2001.

[4] J. Boleng. *Exploiting Location Information and Enabling Adaptive Mobile Ad Hoc Network Protocols*. PhD thesis, Colorado School of Mines, 2002.

[5] J. Boleng, T. Camp, and W. Navidi. Metrics to enable adaptive protocols for mobile ad hoc networks. In *Proceedings of the International Conference on Wireless Networking (ICWN 2002)*, pages 293–298, 2002.

[6] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva. Multi-hop wireless ad hoc network routing protocols. In *Proceedings of the Fourth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 1998)*, pages 85–97, 1998.

[7] T. Camp, J. Boleng, and L. Wilcox. Location information services in mobile ad hoc networks. In *Proceedings of the IEEE International Communications Conference (ICC 2002)*, pages 3318–3324, 2002.

[8] T. Camp, J. Boleng, B. Williams, L. Wilcox, and W. Navidi. Performance comparison of two location based routing protocols for ad hoc networks. In *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom 2002)*, pages 1678–1687, 2002.

[9] C. Chiang, H.K. Wu, W. Liu, and M. Gerla. Routing in clusterhead multihop, mobile wireless networks with fading channel. In *Proceedings of the IEEE Singapore International Conference on Networks (SICON 1997)*, pages 197–211, 1997.

[10] T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR). Internet Draft: draft-ietf-manet-olsr-10.txt, May 2003.

[11] S. Corson and A. Ephremides. A distributed routing algorithm for mobile wireless networks. *ACM Journal on Wireless Networks*, 1(1):61–81, 1995.

[12] R. Dube, C.D. Rais, K.-Y. Wang, and S.K. Tripathi. Signal stability based adaptive routing (SSA) for ad hoc mobile networks. *IEEE Personal Communications*, pages 36–45, February 1997.

[13] M. Gerla, X. Hong, L. Ma, and G. Pei. Landmark routing protocol (LANMAR) for large scale ad hoc networks. Internet Draft: draft-ietf-manet-lanmar-04.txt, June 2002.

[14] M. Gerla, X. Hong, and G. Pei. Fisheye state routing protocol (FSR) for ad hoc networks. Internet Draft: draft-ietf-manet-fsr-03.txt, June 2002.

[15] T. Goff, N. Abu-Ghazaleh, D. Phatak, and R. Kahvecioglu. Preemptive routing in ad hoc networks. In *Proceedings of the Seventh Annual ACM International Conference on Mobile Computing and Networking (MobiCom 2001)*, pages 43–52, 2001.

[16] Z. Haas. A new routing protocol for reconfigurable wireless networks. In *Proceedings of the IEEE International Conference on Universal Personal Communications (ICUPC 1997)*, pages 562–565, Oct. 1997.

[17] Z. Haas, M. Pearlman, and P. Samar. The bordercast resolution protocol (BRP) for ad hoc networks. Internet Draft: draft-ietf-manet-zone-brp-02.txt, July 2002.

[18] Z. Haas, M. Pearlman, and P. Samar. The interzone routing protocol (IERP) for ad hoc networks. Internet Draft: draft-ietf-manet-zone-ierp-02.txt, July 2002.

[19] Z. Haas, M. Pearlman, and P. Samar. The intrazone routing protocol (IARP) for ad hoc networks. Internet Draft: draft-ietf-manet-zone-iarp-02.txt, July 2002.

[20] M. Horner and D. Plassmann. Directed antennas in the mobile broadband system. In *Proceedings of the 15th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom 1996)*, pages 704–712, 1996.

[21] Y. Hu and D. Johnson. Caching strategies in on-demand routing protocols for wireless ad hoc networks. In *Proceedings of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 2000)*, pages 231–242, 2000.

[22] R. Jain, A. Puri, and R. Sengupta. Geographical routing using partial information for wireless ad hoc networks. *IEEE Personal Communications*, pages 48–57, February 2001.

[23] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark. Routing protocols for mobile ad-hoc networks - a comparative performance analysis. In *Proceedings of the Fifth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 1999)*, pages 195–206, 1999.

[24] D. Johnson and D. Maltz. Dynamic source routing in ad hoc wireless networks. In T. Imelinsky and H. Korth, editors, *Mobile Computing*, pages 153–181. Kluwer Academic Publishers, 1996.

[25] D. Johnson, D. Maltz, and Y. Hu. The dynamic source routing protocol for mobile ad hoc networks. Internet Draft: draft-ietf-manet-dsr-09.txt, April 2003.

[26] B. Karp and H. T. Kung. GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 2000)*, pages 243–254, 2000.

[27] Y. Ko and N.H. Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. In *Proceedings of the Fourth Annual ACM International Conference on Mobile Computing and Networking (MobiCom 1998)*, pages 66–75, 1998.

[28] S.-J. Lee. *Routing and Multicasting Strategies in Wireless Mobile Ad hoc Networks*. PhD thesis, University of California, Los Angeles, 2000.

[29] W.-H. Liao, Y.-C. Tseng, and J.-P. Sheu. Grid: A fully location-aware routing protocol for mobile ad hoc networks. *Telecommunication Systems*, 18(1):37–60, 2001.

[30] J. Macker and S. Corson (Chairs). Mobile ad hoc networks (MANET). http://www.ietf.org/html.charters/manet-charter.html. Page accessed August 14, 2002., 1997.

[31] S. Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. *Mobile Networks and Applications*, 1(2):183–197, 1996.

[32] S. Murthy and J.J. Garcia-Luna-Aceves. A routing protocol for packet radio networks. In *Proceedings of the First Annual ACM International Conference on Mobile Computing and Networking (MobiCom 1995)*, pages 86–95, 1995.

[33] V. Park and S. Corson. A highly adaptive distributed routing algorithm for mobile wireless networks. In *Proceedings of the 16th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom 1997)*, pages 1405–1413, April 1997.

[34] V. Park and S. Corson. Temporally-ordered routing algorithm (TORA) version 1 functional specification. Internet Draft: draft-ietf-manet-tora-spec-04.txt, July 2001.

[35] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc on demand distance vector (AODV) routing. Internet Draft: draft-ietf-manet-aodv-13.txt, February 2003.

[36] C. Perkins and P. Bhagwat. Destination sequenced distance vector routing for mobile computers. *Computer Communication Review: SIGCOMM*, 24(4):234–244, October 1994.

[37] C. Perkins and P. Bhagwat. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. In *Proceedings of the ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM 1994)*, pages 234–244, 1994.

[38] C. Perkins and E.M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999)*, pages 90–100, 1999.

[39] Charles E. Perkins, editor. *Ad Hoc Networking*. Addison-Wesley, 2001.

[40] E. Royer and C.-K. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Communications Magazine*, pages 46–55, April 1999.

[41] I. Stojmenovic and X. Lin. Loop-free hybrid single-path/flooding routing algorithms with guaranteed delivery for wireless networks. *IEEE Transactions on Parallel and Distributed Systems*, 12(10):1023–1032, 2001.

[42] C.-K. Toh. Associativity-based routing for ad hoc mobile networks. *Wireless Personal Communications*, 4(2):1–36, 1997.

[43] C.-K. Toh. Long-lived ad hoc routing based on the concept of associativity. Internet Draft: draft-ietf-manet-longlived-adhoc-routing-00.txt, March 1999.

[44] Y.-C. Tseng, S.-L. Wu, W.-H Liao, and C.-M. Chao. Location awareness in ad hoc wireless mobile networks. *Computer*, 34(6):46–52, 2001.

[45] T.-S. Yum and K.-W. Hung. Design algorithms for multihop packet radio networks with multiple directional antennas stations. *IEEE Transactions on Communications*, 40(11):1716–1724, 1992.

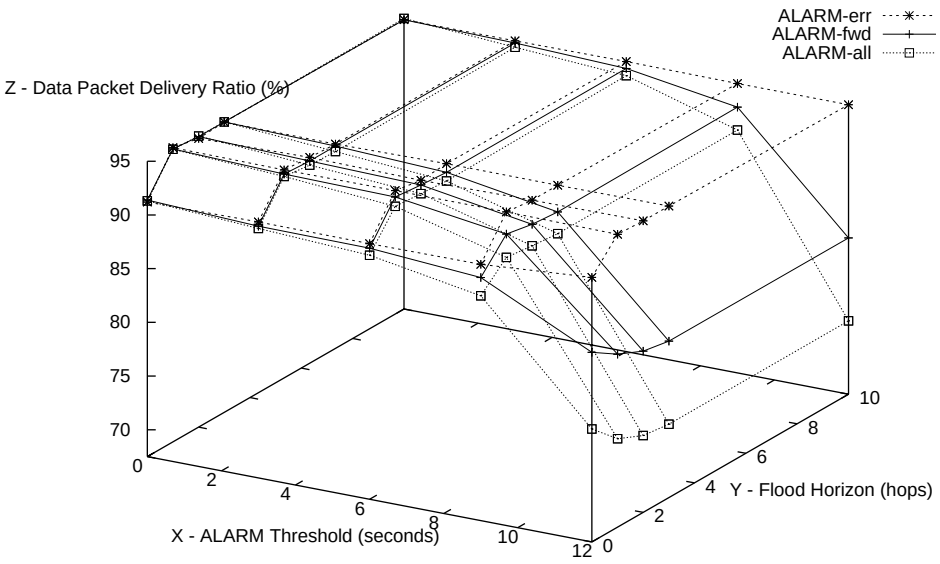

Fig. 2. ALARM Performance Volume - Data Packet Delivery Ratio

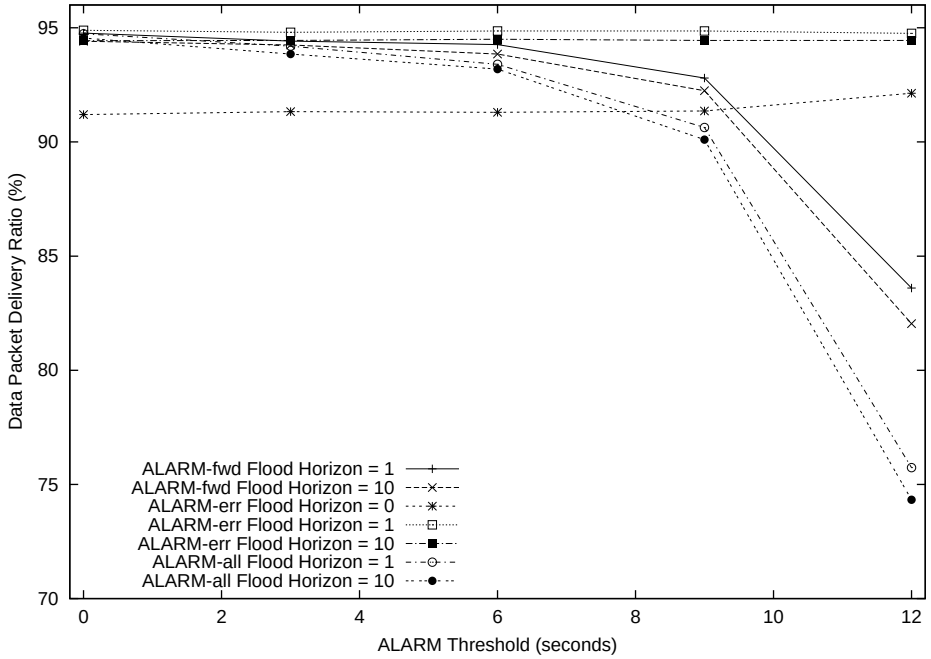

Fig. 3. ALARM Data Packet Delivery Ratio vs. ALARM Threshold

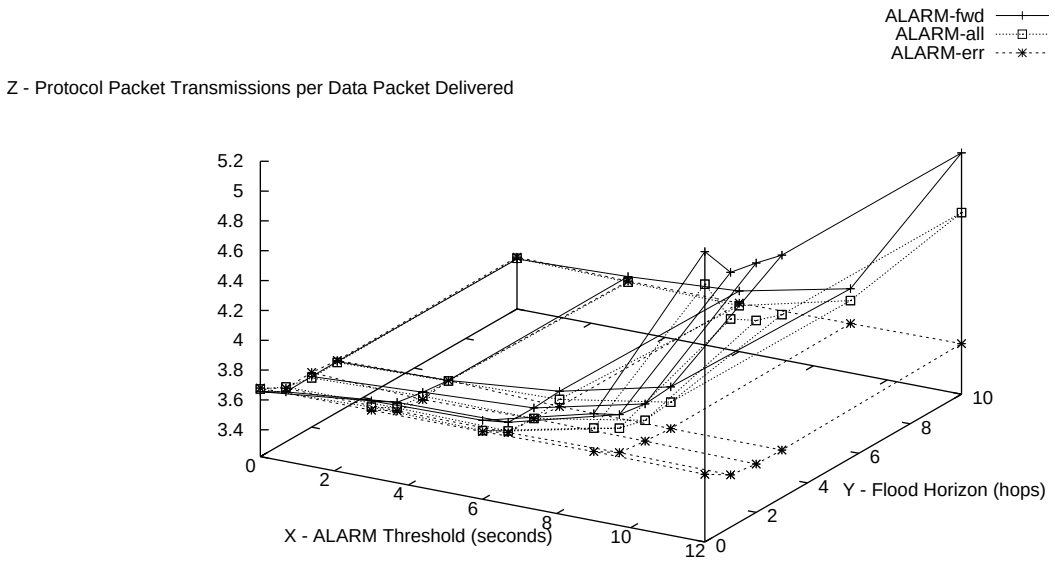

Fig. 4. ALARM Performance Volume - Protocol Packet Transmissions per Data Packet Delivered

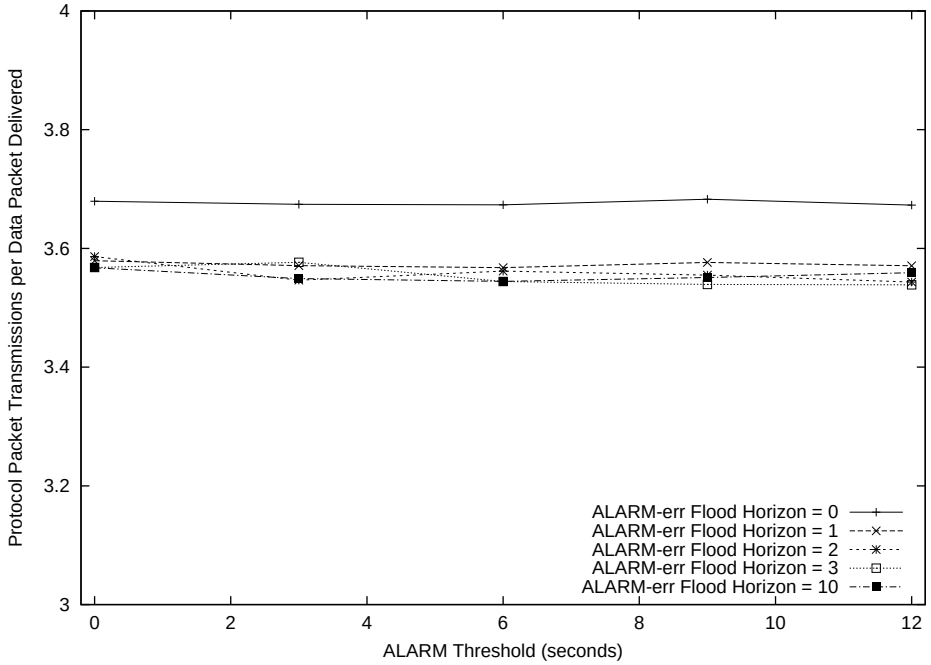

Fig. 5. ALARM Protocol Packet Transmissions per Data Packet Delivered vs. ALARM Threshold

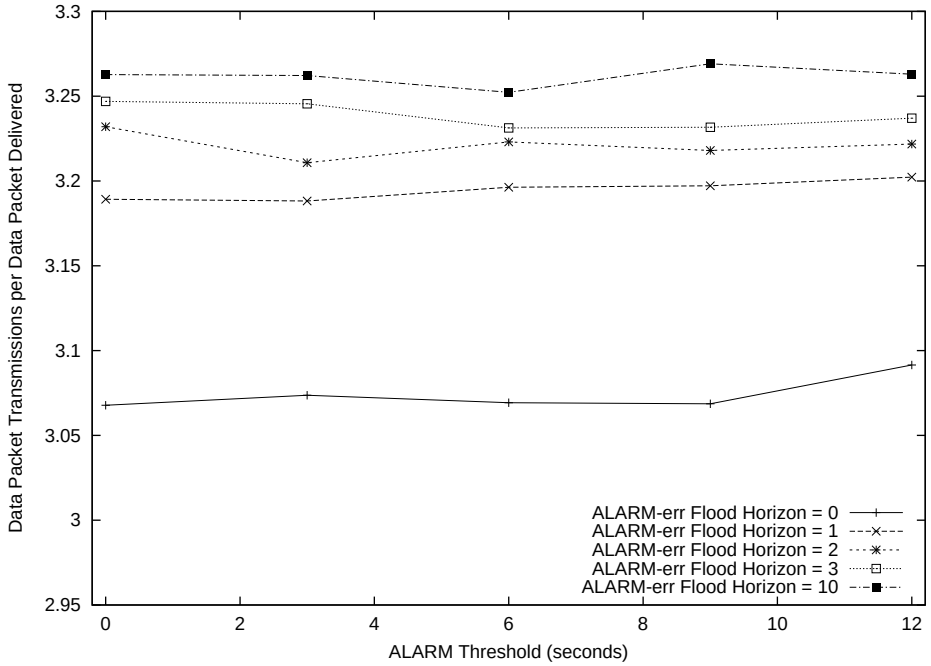

Fig. 6. ALARM Data Packet Transmissions per Data Packet Delivered vs. ALARM Threshold

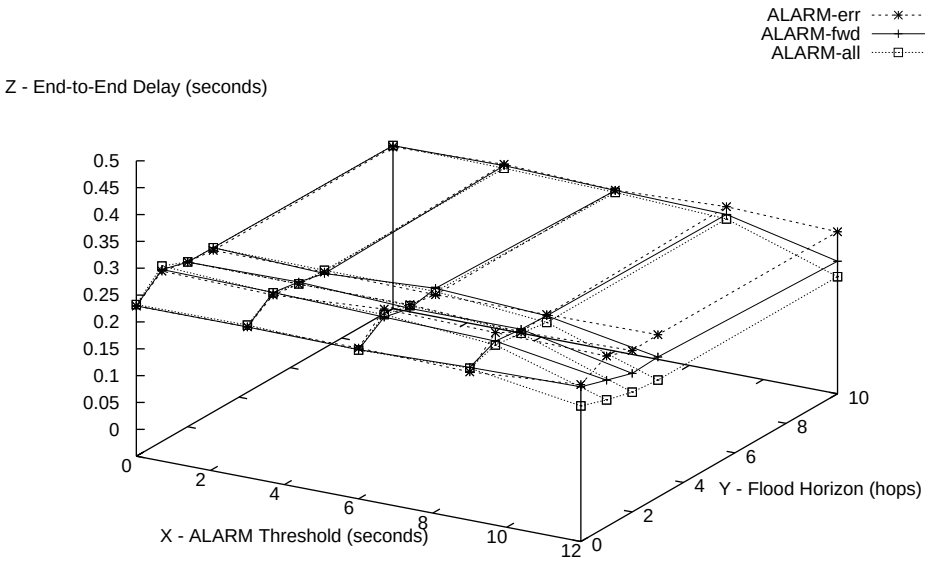

Fig. 7. ALARM Performance Volume - End-to-End Delay

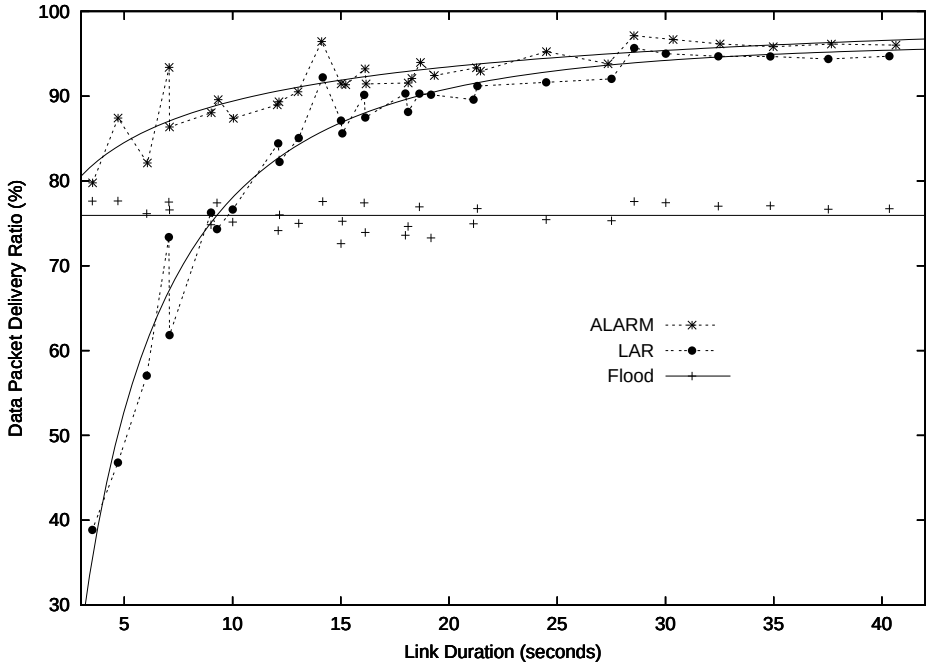

Fig. 8. Data Packet Delivery Ratio - ALARM, LAR, and Flood

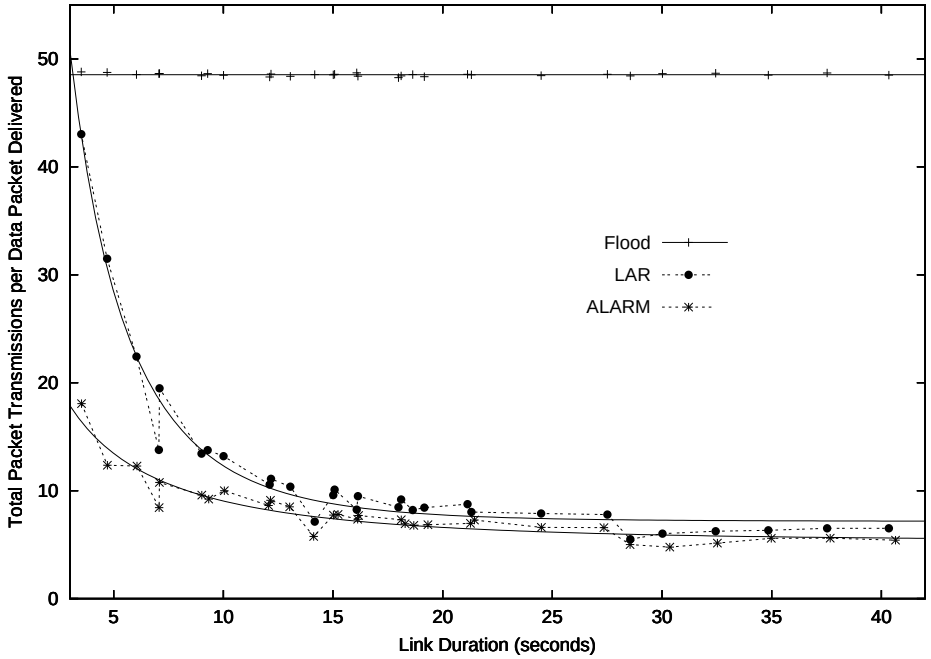

Fig. 9. Total Packet Transmissions per Data Packet Delivered - ALARM, LAR, and Flood

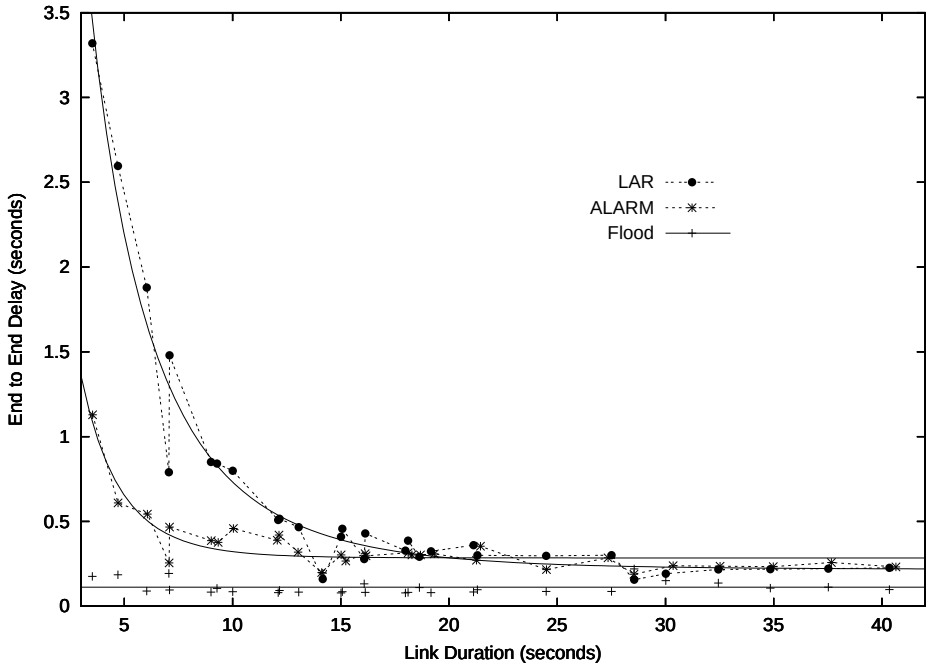

Fig. 10. End-to-End Delay - ALARM, LAR, and Flood