A Cross-Layered Protocol Architecture for Highly-Dynamic Multihop Airborne Telemetry Networks

Abdul Jabbar, Erik Perrins, James P.G. Sterbenz
Department of Electrical Engineering and Computer Science
Information and Telecommunication Technology Center
The University of Kansas
Lawrence, KS 66045
{jabbar,esp,jpgs}@ittc.ku.edu

ABSTRACT

Highly-dynamic mobile wireless communication presents unique challenges to the network at all layers, and requires the design of new protocols and mechanisms. We discuss a cross-layer aware internetwork architecture and the various mechanisms to enable reliable communication in high-velocity multihop scenarios. We introduce AeroNP, an IP-compatible network protocol that is designed for telemetry applications in an aeronautical environment. A new routing algorithm is presented that leverages location information combined with snooping to forward packets in the absence of stable end-to-end routes along, with an implicit congestion control mechanism.

INTRODUCTION

Telemetry for airborne test and evaluation is an application that poses unique challenges. Traditionally, telemetry communication has consisted primarily of point-to-point links with multiple sources and a single sink. More recently, with the increasing number of sources in the typical telemetry test scenario, there is a need to move to networked systems in order to meet the demands of bandwidth and connectivity. This need has been recognized by various groups, including the Integrated Network Enhanced Telemetry (iNET) program for Major Range and Test Facility Bases across United States [1]. The objective of this paper is to address the architectural issues of multihop networks for the high-speed airborne environment in general, demonstrated with the help of a specific telemetry application for defense test and evaluation.

The current TCP/IP-based Internet architecture is not designed to address the needs of telemetry applications and there remain a number of issues to be solved at the network and transport layers [2]. In particular, the current Internet protocols are unsuitable for the specific constraints and requirements of the aeronautical environment in a number of respects [2]. These constraints include the physical network characteristics such as topology and mobility that present severe challenges to reliable end-to-end communication. In order to build a resilient network infrastructure [3], we need cross-layer enabled protocols at the transport, network and MAC layers that are particularly suited for the airborne telemetry networks.

At the same time, there is a need to be compatible with both TCP/IP-based devices located on the airborne nodes as well as with the control applications. Therefore, any new protocol suite while being specific to the aeronautical telemetry environment must also be fully interoperable with TCP/UDP/IP via gateways at the telemetry network edges.

Due to the limited bandwidth in telemetry networks and a priori knowledge of communication needs of a given test, the iNET community is developing a TDM (time division multiplex)-based MAC for this particular environment. In this paper, we assume that such a protocol is used at the MAC layer. The issues related to the transport layer in this environment are presented separately in a companion paper [4]. This paper focuses on the the network layer and its cross-layer interaction with the transport and MAC layers.

It is important to note that while the telemetry network constrains some aspects of network operations, there are also aspects that can be exploited by domain specific protocols, such as the knowledge of the airborne node location and trajectory. Previous research has developed several intelligent network protocols in the context of mobile ad hoc networks (MANETs) and wireless sensor networks (WSNs) that attempt to exploit additional information available [5, 6]. In order to achieve this, we need to facilitate cross-layering across the multiple layers. For example, location and trajectory information can be used find better paths if there exists a mechanism, either an implicit or explicit, for information exchange between the network and physical layer. As discussed in literature, strict layering in the network stack is not particularly suitable for wireless networks due to mobility, limited bandwidth, low energy, and quality of service (QoS) requirements. Therefore, it is commonly agreed upon that a tighter, more explicit, yet careful integration amongst the layers will improve the overall wireless network performance in general, and in the case of highly-dynamic, bandwidth constrained networks may provide the only feasible solution that meets the requirements of telemetry applications.

The rest of the paper is organized as follows: the next section presents the specific challenges to reliable network communication, specifically in the iNET scenario. This is followed by a discussion of the current Internet architecture and its inability to meet the demands of telemetry networks. Then, we present the cross-layer mechanisms that can be used to provide efficient communication amongst the nodes in a test environment. Finally, we present the framework of *AeroNP*, a network protocol tailored to the needs of the aeronautical applications, along with packet formats and the *AeroRP* routing algorithm that operates in several modes based on the available information.

CHALLENGES IN AERONAUTICAL ENVIRONMENT

In this section, we describe a typical airborne telemetry network and the challenges that must be addressed for successful communication. As shown in Figure 1, the network consists of three types of nodes: test articles (TA), ground stations (GS) and relay nodes (RN). The TAs are the airborne nodes involved in the test and contain several data collection devices that are typically IP-based (e.g. cameras). TAs house omnidirectional antennas with relatively short transmission range. The GSs typically have a higher transmission range than that of a TA due to the large steerable antennas and an unconstrained energy supply. In point-to-point communication mode, the GS tracks a given TA across some geographical space. However, due to the narrow beam width of the antenna, they can only track one TA at any give time. The

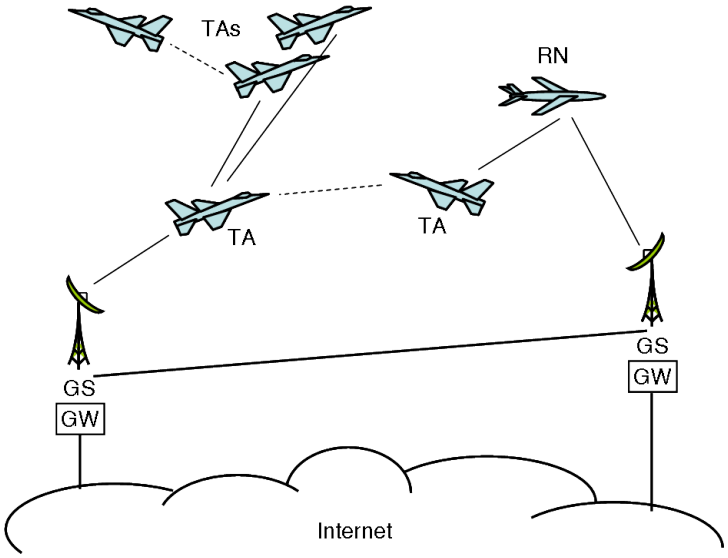

Figure 1: Aeronautical Telemetry Network

GS also houses a gateway (GW) that connects the telemetry network to Internet and several terminals that may run control applications for the various devices on the TA. Furthermore, the GSs can be interconnected to do soft-handoffs while tracking a TA. The relay nodes are airborne nodes that are dedicated to improve the connectivity of the network. These nodes have additional energy needed to forward data from multiple TAs and can be arbitrarily placed in the network.

A test and evaluation scenario may involve three types of communication: test data from the TA to the GS, internode communication between any two TAs, and command and control data from the GS to the TAs. Relay nodes can be used in any of the above mentioned cases, when the source and destination are not in direct communication range. The various challenges in this scenario are:

1. *Mobility*: The test articles can travel at speeds as high as Mach 3.5; the extreme is then two TAs closing with a relative velocity of Mach 7. Because of high velocity, the network is highly dynamic with constantly changing topology.

2. *Constrained bandwidth*: Due to limited spectrum allocation, the physical bandwidth available is constrained. Given the high volume of data that is sent from TA to GS, the network is severely bandwidth constrained.

3. *Limited energy*: The energy available for telemetry on a TA is limited due to design constraints of the test equipment.

4. *Connectivity*: Given the transmission range of the TA and high mobility, the contact duration between any two nodes may be extremely short leading to frequent network partitioning.

The numerical values from the network characteristics of iNET [7] are used to determine the stability of the links, as shown in Table 1. It is seen that even with an optimistic transmission range, the contact

duration between two nodes can be as low as 15 seconds. Note that in a multihop scenario with lower transmission power, the contact duration between a test article and ground station may be far less.

Table 1: Link stability analysis

Scenario	Tx range [nmi]	Relative velocity	Contact duration [sec]
Single-hop best case			
GS – TA	140	400 knots	2520
TA – TA	15	800 knots	135
Single-hop worst case			
GS – TA	100	Mach 3.5	300
TA – TA	10	Mach 7.0	15

INTERNET PROTOCOL ARCHITECTURE

In this section, we consider the current Internet protocol architecture and evaluate its suitability to the telemetry scenario under consideration. Then, we briefly summarize other network protocols developed for mobile networks.

The traditional wired Internet uses the TCP/IP stack at the transport and network layer respectively, over a stable links such as Ethernet or SONET, with various routing protocols such as OSPF and ISIS. Some of the shortcomings of this approach are:

1. Packet overhead: TCP/IP requires a packet overhead of 40 bytes per data and control packet. The overhead becomes significant if there is a lot of control traffic, which is the case with the per-segment acknowledgements of TCP.

2. Link assumptions: The current internet architecture is based on the fundamental assumption of long-lasting, stable links that does not hold true for a Mach-speed airborne network.

3. Routing: Internet protocols do not support dynamic topologies, requiring convergence of the routes, which is not suitable for the airborne telemetry environment [8].

4. Transport: The Internet transport protocol (TCP) is a closed-loop protocol designed on the assumption of stable end-to-end paths and does not perform well in case of a rapidly changing topology [8, 4].

5. Layering: The current architecture does not support explicit cross-layer information exchange to leverage unique information available in the network such as position and trajectory.

Ad Hoc Routing Protocols: In order to support mobile ad hoc wireless networks (MANETs), several routing protcols have been developed that adapt to changes in topology. Reactive routing protocols such as AODV [9] and DSR [10] attempt to construct source-to-destination paths and are not suitable because

of the delay involved in finding paths on-demand. Furthermore, such paths may not be valid for very long in a highly dynamic network. On the other hand, proactive routing protocols such as DSDV [11] and OLSR[12] forward packets on a hop-by-hop basis and depend on global route convergence. This generates excessive overhead due to frequent route updates (assuming convergence is even possible) and is not suitable for a bandwidth-constrained telemetry network.

There are several other protocols that adapt to mobility by forwarding packets one hop at a time without trying to build the entire path. These include simple algorithms such as flooding and other greedy algorithms that send multiple copies in the network. More complex routing schemes leverage specific information from the network. Most notable are the location-based routing protocols such as LAR, DREAM, SIFT, and GRID [13, 14, 15, 16, 17] that use GPS coordinates of the nodes to determine the next hop. However, to the best of our knowledge, none of the previous studies have tested these protocols at speeds as high as Mach 7. It is also possible to devise a routing scheme to track highly mobile endpoints that reach the reactive limit in which the speed of the nodes is comparable to time it takes for the location tracking to converge upon the position of the node. This is an extreme case that does not apply to the airborne test scenario as shown in Table 1.

CROSS-LAYER MECHANISMS

Despite the fact that link-load aware routing was developed as a part of the first ARPANET routing protocol [18], cross-layered routing utilizing link and physical layer information in route selection is not widely used. The reason for this tends to be twofold: firstly, intelligent cross-layer aware network protocols tend to be inherently complex, and secondly, physical links are highly reliable in wired networks and are frequently over-provisioned. This has led to shortest path being the most widely deployed routing algorithm. It has been noted that this is clearly not enough for effective routing in wireless networks [19]. Hence, we need to exploit available information through cross-layering in order to make forwarding decisions at each node.

Potential knobs at each layer as shown in Table 2 that enable higher layers to influence certain mechanisms at lower layers, based on the information made available through dials. For example, the transport layer influences path selection through *forwarding mode* knob, thus, requesting a certain level of reliability for given data flow.

Table 2: Knobs and dials for a telemetry network stack

Layer	Knobs	Dials	Layer influencing the knob
transport (AeroTP)	reliability mode	service requirements	application
network (AeroNP)	forwarding mode	path characteristics	transport
link and MAC	ARQ and FEC settings	link characteristics	network
physical	coding	channel conditions, available coding schemes	link

In the proposed architecture, we employ cross-layer optimizations not only among the transport (AeroTP) [4] and network (AeroNP) protocols, but also with the MAC and PHY layer. This involves investigating the tradeoffs in type and strength of FEC (forward error correction) at the PHY layer with respect to channel conditions and BER (bit error rate), as well as optimizing TDM parameters and slot assignment based on the transfer mode of AeroTP and QoS parameters (precedence and service type) of AeroNP. Furthermore, for the transport protocol to erasure code across multiple TA-GS paths [4] requires coordination of GS and iNET MAC slot assignment with AeroNP routing. Finally, the support for multicast and broadcast requires coordination of AeroNP routing with the broadcast capabilities of the iNET MAC.

AeroNP: NETWORK PROTOCOL FOR AERONAUTICAL TEST AND EVALUATION

AeroNP is designed for the iNET environment and includes the packet format and the AeroRP dynamic location-aware multihop routing protocol. The small contact duration between two TAs indicates the need for an intelligent multihop routing protocol for reliable communication over a highly-dynamic physical topology.

A. Header Format, Addressing, and IP Transparency

AeroNP is an *IP-compatible* network layer with the additional functionality needed for aeronautical telemetry. A preliminary format of the AeroNP packet, shown in Table 3, is 32 bits wide.

Table 3: AeroNP Packet Structure

<table>
<tr><td>version</td><td>CI</td><td>type</td><td>priority</td><td>protocol</td><td>ECN/DSCP</td></tr>
<tr><td colspan="4">source TA MAC address</td><td colspan="2">destination TA MAC address</td></tr>
<tr><td colspan="4">next hop TA MAC address</td><td>source dev ID</td><td>dest dev ID</td></tr>
<tr><td colspan="4">source TA location (optional)</td><td colspan="2">destination TA location (optional)</td></tr>
<tr><td colspan="4">length</td><td colspan="2">HEC</td></tr>
<tr><td colspan="6">payload</td></tr>
</table>

The *version* is the AeroNP protocol version, the congestion indicator (*CI*) is set by each node to notify the neighboring nodes of its congestion level as discussed later. The *type* and *priority* fields specify the QoS level of a given packet. The number of QoS classes can be customized for a given scenario. *Protocol* is the demux protocol (id) to which AeroNP hands off the packets. In order to be IP compatible, the *ECN/DSCP* (explicit congestion notification and diffserv code point) nibble is carried over from the IP header. Since the MAC is based on TDM, an AeroNP packet is inserted directly into a TDM slot, and thus contains the *MAC addresses*: *source*, *destination*, and *next hop*. Significant efficiency can be gained if the AeroNP header does not carry the 32-bit source and destination IP addresses (or the even worse 128 bit addresses for IPv6). By performing an ARP-like address translation process, the IP address can be mapped between iNET MAC addresses in the gateway. However, each TA can have multiple peripherals, each of which

has an IP address. Therefore, we include a *device id* field in the header, and the ⟨*MAC-address*, *device-id*⟩ tuple is mapped to IP address at the gateway. While dynamic mapping procedures are possible, it will be more efficient to preload the translation table at the beginning of each test. Optionally, *source* and *destination location* is included, which can be the GPS coordinates that are used in location aware routing described below. The *length* indicates the actual length of the header in bytes. A strong check on the integrity of the header, *HEC* (header error check), is included to protect against bit errors. Because of the TDM-based MAC there is no link layer framing and error control. Hence, this functionality is provided at the network layer. Unlike Internet protocols [20], the default behavior of the AeroNP is to forward the errored packets to the transport layer instead of dropping them at the network layer. This permits FEC at the transport layer to correct errors end-to-end[4].

B. Routing Algorithm

As discussed previously, existing routing protocol mechanisms generate significant overhead and do not converge quickly for a highly dynamic topology and are not appropriate for telemetry networks. We propose *AeroRP*: a proactive routing protocol that leverages location information combined with limited updates to build a next-hop forwarding table. In addition to the bandwidth constraints, telemetry networks may also impose security limitations on the extent of location and trajectory information made available and its advertisement in the network header. We propose several alternatives for cases where no information regarding the location is available.

The basic operation of the proposed routing protocol is to maintain a table of available neighbors at any given point of time. The primary mechanism used by the node to determine its neighbors is snooping. In this TDMA network, a node listens to all transmissions on the wireless channel when not transmitting itself. In AeorRP, when a node hears a data packet over the air interface, it adds the source MAC address of the decoded packet to the neighbors table. This implies that if a node can hear transmissions from a node, it can also communicate with that node. Stale entries are removed from the neighbor table if no transmissions from a node are heard for a predetermined interval of time related to the anticipated contact duration.

The second part of the AeroRP operation is to find the appropriate next hop to forward the data packets. In order to forward packets towards a specific destination, additional information such as location data or route updates is required. There are a variety of mechanisms through which such information can be obtained (in increasing stealthiness):

1. Nodes include state vector explicitly as a field in the header of AeroNP protocol.
2. Nodes include only their GPS location as a field in the network packet header.
3. The GS periodically broadcasts (optionally on a encrypted channel) the state vector of all the nodes so that each node can predict its connectivity ahead of time.
4. No location information is made available; instead nodes exchange their neighbor table upon contact.

In the first two cases, nodes discover both the neighbors and their locations by snooping network packets. In lightly loaded network conditions, a periodic *hello* message is sent by a node to inform other nodes of its presence. The data packets are forwarded to the node that is nearest to the destination as calculated from GPS coordinates. We assume that the all nodes are preprogrammed with the location of GSs. However, there is a time lag during which the node will snoop on its neighbors. In the third case, the GS broadcasts the topology information ahead of time so that the each node can predict its neighbors trajectory and forward the data packets to the appropriate nodes. In the last scenario, we assume that no location or trajectory information is made available due to security policy. Instead, when two nodes are in transmission range, they exchange their neighbor table, and thus each node can build a partial forwarding table. In case of a connected network, each node will have the complete forwarding table after an initial learning phase. However, this approach could generate significant overhead due to dynamic nature of the telemetry network and may have low efficiency due to the delay involved in learning the routes.

Ground Stations are special nodes in this network, which listen to all transmissions and forward packets that are destined to other GSs. In other words, GSs are universal sinks and may have the same MAC address. For uplink data, a GS forwards data to the node that is closest to the destination node. The GS is aware of the location of all nodes either from mission planning or learns it during the test while tracking various TAs.

Relay nodes are always the default next-hop, when present. They accept data from all the TAs and forward them directly to the ground station or another TA. Since the GS has narrow beam width and can only track one TA at a time, it is more efficient for the GS to track the relay nodes and have individual TAs forward the data to the corresponding relay nodes. Given the varied nature of the telemetry, we expect that the routing protocol should support multiple modes for both open and secure scenarios.

C. Quality of Service

The wireless links in the telemetry network are bandwidth constrained and are often under-provisioned for the traffic generated during a field test. Hence, it is essential to implement a quality of service mechanism in this network to ensure that high priority data such as command and control can be reliably delivered. The AeroNP protocol uses two fields in the header to specify the quality of service of data packets in the network: data *type* (e.g command and control, telemetry) and *priority* with in a given type. The application requirements determine the type and priority for a given data flow and is passed to the network layer through the transport layer (AeroTP) via out-of-band signaling. The scheduling at nodes is a weighted fair queue based on type and priority.

D. Broadcast and Multicast

The AeroNP protocol supports both broadcast and multicast natively. The typical all-ones MAC address is chosen as the broadcast address. Similarly, a range of MAC addresses are assigned to sub-groups in the network. These multicast address groups are pre-programmed in the nodes and GS. Given the highly dynamic nature of the network, for sparse networks multicast may not achieve any significant benefit over a simple broadcast in terms of efficiency.

E. Congestion Control

Telemetry networks are often bandwidth constrained, in which individual TAs are under provisioned for a given test scenario. Therefore, in a heavily loaded network with little bandwidth to spare, multi-hop routing can induce severe congestion in the nodes involved in multi-hop forwarding. A MAC level solution would be to assign more slots to the forwarding nodes than the non-forwarding nodes. Since this is too complex in the highly dynamic environment, we propose a simple congestion control mechanism at the network layer using *congestion indicators* or *back pressure*.

In the first mechanism, the node uses the *CI* (congestion indicator) field to indicate its own congestion level. All packet transmissions from a node carry the CI field along with the type and priority of the data. Neighboring nodes eavesdrop on the transmission and are made aware of the congestion at a given node. If a node is congested, the neighbors back off if the data that they have is of equal or lesser priority; higher priority data is nevertheless forwarded to a congested node.

The second mechanism through which congestion control is achieved in the telemetry network is back pressure. Each node listens to all transmissions and determines the congestion level of its neighbor through the CI field in snooped packets. This is possible because both the source MAC address and CI is carried in the header. Consequently, the source node backs-off and finds a different node to forward its packets. Similarly, in a multi-hop scenario, if a bottleneck is encountered, each intermediate hop either stops or slows down its transmissions to the congested node successively until the source of the traffic is reached.

CONCLUSIONS

The existing Internet protocol architecture is not well suited for telemetry applications in highly-dynamic airborne networks, which present unique challenges due to extreme mobility and limited bandwidth. In this paper, we discussed a internetwork architecture that addresses these issues with domain specific network layer. It is observed that exchange of information across layers provides significant benefit in the aeronautical environment. We presented an IP-compatible network layer, AeroNP, with a cross-layer aware routing protocol, AeroRP, that leverages location information to intelligently forward packets over a rapidly changing topology. In its default mode, the routing protocols relies on snooping instead of exchanging explicit route updates to make forwarding decisions. The proposed network protocol supports QoS and handles congestion using congestion indicators and back pressure.

REFERENCES

[1] "iNET system architecuture, version 2007.1." Central Test and Evaluation Investment Program (CTEIP), July 2007.

[2] "iNET technology shortfalls report, version 1.0." Central Test and Evaluation Investment Program (CTEIP), July 2004.

[3] J. P. G. Sterbenz and D. Hutchison, "ResiliNets: Multilevel resilient and survivable networking initiative." http://www.ittc.ku.edu/resilinets/index.html, July 2008.

[4] J. P. Rohrer, E. Perrins, and J. P. G. Sterbenz, "End-to-end disruption-tolerant transport protocol issues and design for airborne telemetry networks," in *Proceedings of the International Telemetering Conference (to appear)*, October 27–30 2008.

[5] M. Abolhasan, T. Wysocki, and E. Dutkiewicz, "A review of routing protocols for mobile ad hoc networks," *Ad Hoc Networks*, vol. 2, pp. 1–22, January 2004.

[6] L. Iannone, R. Khalili, K. Salamatian, and S. Fdida, "Cross-layer routing in wireless mesh networks," in *Proceedings 1st International Symposium on Wireless Communication Systems*, pp. 319–323, 2004.

[7] "iNET needs discernment report, version 1.0." Central Test and Evaluation Investment Program (CTEIP), May 19 2004.

[8] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A. W. Jackson, D. Levin, R. Ramanathan, and J. Zao, "Survivable mobile wireless networks: Issues, challenges, and research directions," in *WiSE '02: Proceedings of the 3rd ACM workshop on wireless security*, pp. 31–40, 2002.

[9] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing." RFC 3561 (Experimental), July 2003.

[10] D. Johnson, Y. Hu, and D. Maltz, "The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4." RFC 4728 (Experimental), Feb. 2007.

[11] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *Proceedings of SIGCOMM*, pp. 234–244, 1994.

[12] T. Clausen and P. Jacquet, "Optimized link state routing protocol (OLSR)." RFC 3626 (Experimental), Oct. 2003.

[13] W. H. Liao, J. P. Sheu, and Y. C. Tseng, "GRID: A fully location-aware routing protocol for mobile ad hoc networks," *Telecommunication Systems*, vol. 18, no. 1-3, pp. 37–60, 2001.

[14] M. de la Fuente and H. Ladiod, "A performance comparison of position-based routing approaches for mobile ad hoc networks," in *Proceedings of IEEE Vehicular Technology Conference*, pp. 1–5, October 2007.

[15] L. Galluccio, A. Leonardi, G. Morabito, and S. Palazzo, "A MAC/routing cross-layer approach to geographic forwarding in wireless sensor networks," *Ad Hoc Networks*, vol. 5, no. 6, pp. 872–884, 2007.

[16] M. Mauve, A. Widmer, and H. Hartenstein, "A survey on position-based routing in mobile ad hoc networks," *IEEE Network*, vol. 15, no. 6, pp. 30–39, 2001.

[17] M. Yuksel, R. Pradhan, and S. Kalyanaraman, "An implementation framework for trajectory-based routing in ad hoc networks," *Ad Hoc Networks*, vol. 4, no. 1, pp. 125–137, 2006.

[18] J. McQuillan, I. Richer, E. Rosen, B. Beranek, and N. Inc, "The new routing algorithm for the ARPANET," *IEEE Transactions on Communications*, vol. 28, no. 5, pp. 711–719, 1980.

[19] D. S. J. De Couto, D. Aguayo, B. A. Chambers, and R. Morris, "Performance of multihop wireless networks: Shortest path is not enough," in *Proceedings of the First ACM Workshop on Hot Topics in Networks (HotNets-I)*, SIGCOMM, October 2002.

[20] R. Braden, "Requirements for internet hosts – communication layers." RFC 1122 (Standard), Oct. 1989.