Continuous Update Traffic Statistics for Multipath Routing Anti Jamming

Shrinivas halahalli*1, M.Sandeep*2,
M.Tech (CSE) Student, Dept of CSE, MRCET, Medchal, D.t: Hyderabad, A.P, India
Assistant Professor, Dept of CSE, MRCET, Medchal, D.t: Hyderabad, A.P, India

ABSTRACT:

A systematic understanding of the decomposability structures in network utility maximization is key to both resource allocation and functionality allocation. Routing in wireless ad-hoc networks has received significant attention from recent literature due to the fact that the dynamic behavior of these networks poses many technical challenges on the design of an effective routing scheme. Though on-demand routing approaches have been shown to perform well, they generally lack the support for Quality-of-Service (QoS) with respect to data transmission. In order to select a subset of end to end paths to provide increased stability and reliability of routes, a new QoS metric, end-to-end reliability, is defined and emphasized in this paper. We present a distributed multi-path dynamic source routing protocol (MP-DSR) for wireless ad-hoc networks to improve QoS support with respect to end-to-end reliability our protocol forwards outgoing packets along multiple paths that are subject to a particular end-to-end reliability requirement. A simulation study is performed to demonstrate the effectiveness of our proposed protocol, particularly the fact that MP-DSR achieves a higher rate of successful packet delivery than existing best-effort ad-hoc routing protocols, such as the Dynamic Source Routing (DSR).

INDEX TERMS: Congestion control, cross-layer design, decomposition, distributed algorithm, network architecture, network control by pricing, network utility maximization, optimization, power control, resource allocation.

I.INTRODUCTION

Wireless ad-hoc networks are autonomous systems composed of mobile hosts that are free to move around arbitrarily. These mobile hosts are referred to as nodes. Rather than relying on a network infrastructure to perform routing in an ad-hoc network, each mobile host serves as a router to forward packets originated from other hosts. Such characteristics allow an ad-hoc network to be established on-the-fly with built-in fault tolerance and unconstrained connectivity. For such networks, an effective routing protocol is critical for adapting to node mobility as well as possible channel error to provide a feasible path for data transmission. In addition to basic routing, for mission-critical applications, Quality of-Service (QoS) routing protocols are needed to search for a path that can satisfy certain QoS requirements and constraints, such as bandwidth or data reliability. The focus of this paper is to propose a QoS routing protocol in wireless ad-hoc networks. In this paper, we design a QoS-aware multi-path source routing protocol (MP-DSR) focusing on a new QoS metric, *end-to-end reliability*. End-to-end reliability is used to reflect the probability of sending data successfully from the source node to the destination node within a time window. Note that it is not the focus of MP-DSR to provide strict *end-to-end reliability* guarantees. Rather, MP-DSR provides routes that satisfy a specific *end-to-end reliability* requirement and such routes persist with a high probability. Thus, it is possible to have a transient QoS disruption even with such a guarantee. Our major contributions in this paper are the following.

First, we define our QoS parameter of interest, *end-to-end reliability*. Second, we propose a fully distributed QoS routing protocol, MP-DSR, with respect to this QoS parameter. MP-DSR is based on the existing Dynamic Source Routing protocol (DSR) [1, 4] and takes advantage of its distributed on-demand nature. It seeks to compute a set of unicast routes that can satisfy a minimum *end-to-end reliability* requirement; it then maintains this requirement throughout the life time of transmission. Packets transmitted from the source node will arrive at the destination node with a higher successful probability than existing best-effort ad-hoc routing protocols. Finally, we evaluate the performance of our routing protocol using extensive network simulations, and compare this to the performance of DSR.

II.SYSTEM MODEL

The jamming adversary can fit a number of different profiles, depending on its inherent goals, ranging from unintentional interference from a device mistakenly left on by a passenger to targeted high-power jamming by a malicious adversary. Between these extremes are greedy users who attempt to monopolize Internet access by blocking other users and malicious users who seek to deny service to the onboard monitoring systems. Since game-theory rests on the assumption of players demonstrating rational behavior, we constrain our focus to exclude extreme malicious attacks. For a particular profile, an adversary can choose from a large number of strategies by varying the jamming type (random, constant, periodic, reactive, wide-band, narrow-band, etc.)13 and attack parameters (power, duty cycle, randomization model, jamming schedule, frequency-hopping pattern, etc.). To mitigate jamming attacks, the networked system can similarly choose from a variety of strategies, consisting of the communication protocol used (normal, using anti-jamming techniques14–18 such as spread spectrum or directional antennas, etc.), the associated parameters, and alerts to flight crew (e.g. alerting crew of a jammer's location), as in the example in Figure 1.

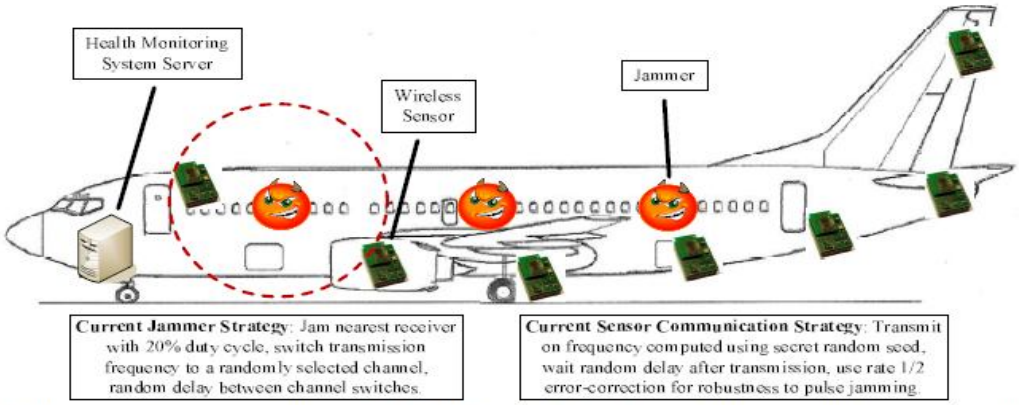

Figure 1. The interaction between the aircraft health monitoring system and the jamming adversary is illustrated. In the game-theoretic framework, these two parties compete to achieve conflicting performance goals by modifying protocols and parameters.

In this paper, we present a detailed game-theoretic framework to model the interaction between the aircraft networked systems and the jamming adversary interested in denying service to the aircraft systems. This model allows thorough equilibrium and worst-case analysis of the attack and mitigating strategies, which can be used to design optimal response mechanisms, so that the aircraft network can function within desired safety margins even during a worst-case attack. Game theory can be used to quantify the goals and payoffs of both players, allowing the design of protocols that remove all incentives for adversarial jamming.
Furthermore, game-theoretic modeling can allow the network to differentiate between adversarial profiles, so that unwanted circumstances such as a false alarm of attack warning due to benign passenger devices can be avoided. To demonstrate the use of the game-theoretic framework, we illustrate an example scenario in which a passenger introduces a wireless PED to jam and effectively monopolize network services. In this study, we consider various attack and mitigation strategies, and analyze the resulting non-cooperative game. Finally, we show how network response strategies can be formulated to ensure optimal network operations.

III. Network and Jammer Systems

Before addressing the interaction between the aircraft network and the jammers, we first provide an overview of the two systems independently. We introduce the parameters used in the network and jamming models, and describe basic jamming attacks and mitigation tactics.

3.1. Aircraft Wireless Network

We first consider the wireless network on the aircraft system, consisting of several distinct components including next-generation critical inter-aircraft communication systems, sensors for on-board health and system monitoring, and internet access points for passengers and crew. The goal of the network is to provide reliable service to all system components, with an obvious hierarchy in terms of service priority. For example, the network would prioritize critical communication operations over passenger entertainment.
Independently of the access control systems logically separating operational and passenger systems, the aircraft network must be robust to the wide variety of passenger devices brought onto the aircraft,19, 20 due to the resource sharing of the wireless medium. For example, the health monitoring sensor network may operate over a set of frequency bands which is disjoint from those commonly used by PEDs. In order to achieve the desired robustness to the highly variable operation of passenger systems, we consider the operation of a aircraft network that can be dynamically tuned in response to passenger system operation. We let Sn denote the set of possible operational states of the aircraft network, such that each state sn 2 Sn completely characterizes the behavior of the system in terms of frequency usage, medium access control, transmission power levels, error correction, etc. The choice of operational state depends on the presence or absence of interfering or jamming signals. However, to trigger a heightened state of network awareness and choose the appropriate state, the network must be able to reliably detect jamming. We thus assume that collaborative approaches for sensing interference and jamming are employed by the aircraft network using a network of sensors throughout the aircraft,21 as illustrated in Figure 2. Such a system can characterize the behavior of the jamming attack or localize the source of the interference, potentially alerting flight crew to the location of the jammer.

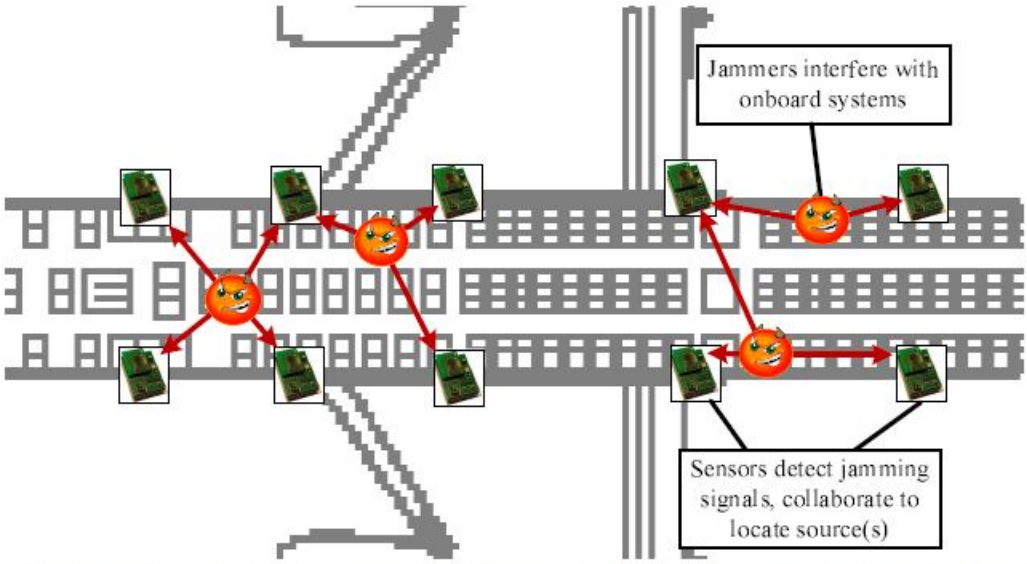

Figure 2. The onboard systems may be capable of detecting interfering signals and collaboratively determining the source of the interference.

Using the sensed information about the jammer and interference, the network can choose the appropriate operating state for robustness to jamming. For example, the network can choose an operating state sn which employs anti-jamming spread spectrum technology,14 such as direct-sequence spread spectrum (DSSS). Alternatively, the network can selectively employ directional antennas to filter and attenuate interfering signals.

Such techniques offer improved reliability of service using secret spreading information or specialized methods, but they require additional overhead in terms of communication bandwidth or hardware complexity. Hence, there are trade-offs between the reliability of service and the corresponding resource expenditure for different states in Sn. In addition to the resource concerns, however, the operational state of the aircraft network has social influences on the passengers. While safety is the primary concern, it is certainly undesirable to cause unnecessary panic or negative social response through hawkish responses to threat compensation.

IV Interfering and Jamming Devices

We next consider the passenger devices which either unintentionally interfere or intentionally jam the communications of the aircraft wireless network. On-board PEDs are in complete control of the passengers and may range from cellular phones to sophisticated high-power jammers. This diversity inherently presents an additional obstacle for the robustness of the aircraft network. As with the aircraft network, we suppose the jammer operation can be dynamically tuned. We thus let Sj denote the set of possible operational states of the jammer, such that each state sj 2 Sj completely characterizes the behavior of the jamming attack. Numerous type of jamming attacks have been proposed, and each has different behavior in terms of resource expenditure, detection, and impact on the target network. For example, jamming devices can transmit constant interfering signals, resulting in high error rates for the target network in trade for a high detection risk. Wideband jamming can be used to reduce the effectiveness of spread spectrum techniques by jamming over a wide range of communication channels, but this increased impact requires significantly more energy than narrow band jamming. Random and periodic jamming techniques13 allow the jammer to avoid detection by alternating between intervals of active jamming and hibernation. Cross-layer jamming8, 10, 11, 17 incorporates information from higher layers in the network protocol stack into physical layer jamming, allowing the jammer to reduce resource expenditure by several orders of magnitude, but requiring intimate knowledge of network protocols. Reactive jamming13 allows the jammer to reduce resource expenditure by only jamming the wireless channel when packet transmissions are detected, though the effectiveness of this technique is limited by network geometry. Each type of jamming attack has associated parameters, including transmission power, jamming duty cycle, and targeted network components. A certain jamming technique may be more suited to denying service to a wireless access point, while another may be able to accurately target primary communication systems. Finally, the adversary's degree of reluctance towards being detected and subsequently

prosecuted will determine to what extent a flight crew alarm could be used as a deterrent.

V. Related Works

On-demand routing protocols generally perform well for wireless ad-hoc networks, since the flooding of route request messages is only performed when a route is needed, rather than periodically as in proactive routing protocols. The degree of flooding is further reduced by using multi-path routing protocols, which have been proposed to discover multiple paths for data transmission. Such protocols can be considered as a hybrid of proactive and on-demand routing, because route discovery is invoked on-demand while route maintenance is done on a proactive basis. Examples of such multi-path protocols include Temporally-Ordered Routing Algorithm (TORA) [8] and Split Multi-path Routing (SMR) [5]. In TORA, the source node constructs multiple routes by flooding a query message followed by a set of update messages. However, TORA does not have any mechanisms to evaluate the quality of these multiple paths and this leads to its poor performance. MP-DSR overcomes this problem by selectively choosing more reliable paths and by providing soft guarantees on the end-to-end reliability. SMR [5] extends DSR in the way that the destination can discover two paths for each route request, in which one is the shortest path, and the other is the maximum disjoint path. There is no explicit enforcement of disjoint paths and this differs from our work, because our algorithm enforces the use of disjoint paths in its route discovery in order to use the definition of path reliability to provide end-to-end reliable service. Previous work in QoS routing for ad-hoc wireless networks focuses on guarantees with respect to bandwidth, cost and delay. One of such routing protocols is the ticket-based QoS routing protocol [2]. It considers two kinds of routing criteria: the delay-constrained least-cost routing and the bandwidth-constraint least cost routing. It uses ticket-based probing to control the number of route queries and to find multi-path in parallel.

In comparison, our MP-DSR considers the dynamic nature of network topology as well as the importance to offer continuous network connection in certain mission critical applications. Thus, the objective of our protocol is to improve the level of service by providing guarantee with respect to *end-to-end reliability*, and to probabilistically guarantee the required connection lifetime.

In addition, our MP-DSR differs in the way of searching multiple paths; the route discovery in our protocol relies only on local link availability information at each intermediate node to perform the route request (RREQ) message forwarding, without resorting to any global information as was used in [2].

VI Conclusions

In this paper, we have proposed a multi-path dynamic source routing (MP-DSR) protocol to provide data transmission with higher end-to-end reliability in wireless ad hoc networks. The objective is to provide a reliable route for packet transmission with a minimum network overhead.

We introduce a QoS parameter, *end-to-end reliability*, which is used for path selections. Applications can specify their end-to-end reliability requirements to control the routing failure probability. With our algorithm, data transmission can then be soft provisioned with limited extra overhead. End-to-end reliability is also maintained throughout the whole transmission life time. Simulation results show that our MP-DSR can offer higher and more consistent success delivery ratio than DSR. In addition, the lower error ratio of MP-DSR illustrates that its end-to-end transmission is more reliable. Finally, the control message overhead in MP-DSR is almost identical to that of DSR in average cases.

7 References

[1] J. Broch, D. B. Johnaon, and D. A. Maltz. Dynamic Source Routing (dsr). *Internet Draft, draft-ietf-manetdsr-03.txt*, 1999.

[2] S. Chen and K. Nahrstedt. Distributed Quality of Service Routing in Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 17(8), August 1999.

[3] S. Jiang, D. He, and J. Rao. A Prediction-based Link Availability Estimation for Mobile Ad Hoc Networks. In *INFOCOM*, pages 1745–52, 2001.

[4] D. B. Johnaon and D. A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. *Mobile Computing*, pages 153–181, 1996.

[5] S. Lee and M. Gerla. Split Multipath Routing with Maximally Disjoint paths in Ad Hoc Networks. In *Technical Report in University of California*, 2000.

[6] A. B. McDonald and T. F. Znati. A Mobility-Based Framework for Adaptive Clustering in Wireless Ad Hoc Networks. *IEEE Journal on Selected Areas in Communications*, 17(8), August 1999.

[7] A. B. McDonald and T. F. Znati. A Path Availability Model for Wireless Ad-Hoc Networks. In *Proceedings of IEEEWireless Communications and Networking Conference*, 1999.

[8] V. Park and S. Corson. Temporaly-ordered routing algorithm. *Internet Draft*, August 1998.

[9] C. Toh. Associativity-Based Routing for Ad-Hoc Mobile Networks. *Wireless Personal Communications*, 4:103– 139, 1997.

[10] X. Zeng, R. Bagrodia, and M. Gerla. GloMoSim: a Library for Parallel Simulation of Large-Scale Wireless Networks. In *Proceedings of the 12th Workshop on Parallel and Distributed Simulations*, May 1998.