Reliable Distributed Computing on Unreliable Radio Channels *

[Extended Abstract]

Shlomi Dolev
Ben-Gurion University
Beer-Sheva, Israel

Seth Gilbert,
Rachid Guerraoui
EPFL IC
Lausanne, Switzerland

Dariusz R. Kowalski
U. Liverpool, CS Dept.
Liverpool, UK

Calvin Newport†
Fabian Kuhn,
Nancy Lynch
MIT CSAIL
Cambridge, MA, USA

ABSTRACT

Much of the future of wireless networking will unfold in the unlicensed bands of the radio spectrum. These bands are increasingly crowded and vulnerable. Designers of protocols in this setting must take into account a variety of interference sources, including selfish devices, malicious jammers, and incidental electromagnetic radiation (radar, microwaves, etc.). This paper surveys results from our recent research that models this *adversarial interference* and aims to answer fundamental questions about what can be solved reliably (and efficiently) in this increasingly relevant yet difficult environment.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless Networks

General Terms

Algorithms, Theory

1. THE AGE OF OPEN AIRWAVES

In a recent SIGCOMM paper [9], a research team led by Ramakrishna Gummadi asked a simple question: *what is the impact of RF interference on the increasingly crowded unlicensed bands of the radio spectrum?* They setup an 802.11 access point and connected a laptop client. They then introduced several common sources of radio interference, including a Zigbee node, cordless phone, and two different types of malicious jammers. They found that even "relatively small amounts" of RF interference can result in "substantial performance problems for commodity 802.11 NICs." They were able, for example, to disrupt a link with a signal 1000 times weaker than the 802.11 signal, and shut down a network running multiple access points on multiple channels, using only a single interferer. Changes to standard operational parameters, such as CCA threshold, bit rate, and packet size, could not eliminate these effects.

This result underscores an important reality: much of the future of wireless computing will unfold in the unlicensed bands of the radio spectrum. Furthermore, these bands are increasingly crowded and vulnerable. Designers of protocols that use the unlicensed bands must take into account a variety of interference sources, including: (a) selfish devices that use the band without consideration of other protocols; (b) malicious devices that actively try to prevent communication; and (c) electromagnetic interference from unrelated sources (e.g., military radar, microwaves, and medical equipment).

For simplicity, we will refer to this diversity of disruption with the generic term *adversarial interference*, because its behavior is unpredictable and falls outside of the control of the individual protocol designer. The systems community has been attacking adversarial interference from multiple angles, including *hardware solutions* (e.g., more resilient signal encoding), *regulatory solutions* (e.g., additional rules for the proper use of the relevant bands), and *systematic solutions* based on new approaches to wireless networking (e.g., cognitive networks).

The theoretical distributed algorithms community, by contrast, lags in their study of this increasingly important topic. To date, the bulk of wireless networking papers at distributed algorithms conferences such as PODC still consider networks inhabited only by (non-faulty) devices running the same protocol. In this extended abstract, I describe recent research that aims to close this gap. Specifically, I describe a series of recent papers that introduce and use the *disrupted ra-*

*This work has been support in part by Cisco-Lehman CUNY A New MAC-Layer Paradigm for Mobile Ad-Hoc Networks, AFOSR Award Number FA9550-08-1-0159, NSF Award Number CCF-0726514, and NSF Award Number CNS-0715397.

†Contact Author: cnewport@mit.edu

Copyright is held by the author/owner(s).

MobiHoc S³'09, May 18–21, 2009, New Orleans, Louisiana, USA.
ACM 978-1-60558-531-4/09/05.

dio network model—a theoretical model motivated by the problems of adversarial interference. We begin, however, by briefly summarizing the related work that precedes the introduction of this new model.

2. A BRIEF HISTORY OF ADVERSARIES IN WIRELESS NETWORK MODELS

The theoretical distributed algorithms community has only recently devoted attention to wireless networks with adversarial behavior. The first such work is the 2004 paper of Koo [10] which studies byzantine-resilient reliable broadcast. Koo assumes that at most some bounded fraction, t, of any device's neighbors might suffer from Byzantine faults—allowing them to deviate from the protocol. The faulty devices, however, are restricted to broadcasting on a TDMA schedule that prevents collisions. It is also assumed that source addresses cannot be spoofed. Koo proves that reliable broadcast is possible only for $t < \frac{1}{2}R(2R+1)$, where R is the transmission radius of devices on the grid (using the L_{inf} distance metric). In a 2005 paper, Bhandari and Vaidya [2] prove Koo's bound tight by exhibiting a matching algorithm. In 2006, Koo, Bhandari, Katz, and Vaidya [11] extend the model to allow for a bounded number of collisions and spoofed addresses.

Others have considered wireless network models with probabilistic message corruption. Drabkin et al. [5] allow Byzantine devices to interfere with communication; each honest message, however, is successfully delivered with some non-zero probability, and authentication is available via public-key cryptography. Pelc and Peleg [12] also assume that messages may be corrupted (or lost) with some non-zero probability.

In [7, 8], we consider a single hop model with an external adversary. In contrast to previous work, we do not constrain adversarial behavior—allowing unbounded jamming and overwriting of messages. We study the *efficiency* of the adversary, producing tight bounds on the *jamming gain*—the minimum possible ratio of honest broadcasts to adversarial broadcasts that can prevent termination for a variety of problems, including reliable broadcast, leader election, k-selection, and consensus.

In recent work, Awerbuch et al. [1] consider a similar problem. They assume an adversary that can jam a single hop wireless network for a $(1-\epsilon)$ fraction of the rounds. They produce an efficient MAC protocol that achieves a constant throughput on the non-jammed steps, even when only loose bounds on ϵ and the number of devices are known.

3. DISRUPTED RADIO NETWORKS

In [3], we introduce the *disrupted radio network* (DRN) model. This model assumes a single hop radio network, but can be generalized to multiple hops without undue difficulty. Executions proceed in synchronized time slots which we call *rounds*. The radio channel is divided into $\mathcal{F} \geq 1$ narrowband communication frequencies. During each round each device chooses a single frequency on which to participate, and decides whether to broadcast or receive. If two or more devices broadcast on the same frequency during the same round then the devices receiving on that frequency receive nothing due to collision.

We incarnate the various sources of possible interference with a bounded adversary that, in each round, can choose up to $t < \mathcal{F}$ frequencies to disrupt—preventing any messages from being received on those frequencies during that round. The adversary can base its disruption decision for round r based on the messages sent through round $r-1$ and knowledge of the protocol used by the honest devices. We assume t is a known upper bound on possible interference.

The DRN model is simple enough to generate strong upper and lower bounds. At the same time, it is designed to capture enough of the possible interference sources to preserve correctness in real world deployments. Due to the power of the adversary, we intend the DRN model to be used for the development and verification of *safety-critical* primitives—such as agreement, leader election, and parameter initialization—not necessarily high-throughput, best-effort style protocols. For example, a routing protocol that is provably resilient to this worst-case adversarial interference might be too inefficient to support a standard TCP flow. At the same time, however, the model might reasonably support the design of a resilient *resynchronization protocol* that can be used by the sender and receiver to reliably change their frequencies or sending parameters when they encounter unexpected disruption.

4. RESULTS SURVEY

In [3] we study deterministic *oblivious* solutions to the gossip problem in the DRN model. (Deterministic oblivious algorithms, which can be described as pre-computed lists of broadcast and receive steps, are useful for resource-constrained devices such as RFID tags and sensors.) We produce a tight bound of $\Theta(\frac{n}{\epsilon\mathcal{F}^2})$ rounds for disseminating $(1-\epsilon)n$ of the n total rumors with a disruption parameter of $t = 1$. For $1 \leq t < \mathcal{F}$, we describe an upper bound that requires $O(\frac{n\epsilon^{t+1}}{\mathcal{F}\epsilon^t})$ rounds, and prove that for the worst case of $\epsilon = t/n$, any deterministic oblivious solution requires $\binom{n}{t+1}/\binom{\mathcal{F}}{t+1}$ rounds to complete.

At the core of our upper bounds is a broadcast/disseminate model in which a dedicated group of *listener* devices monitor the frequencies and then attempt to disseminate what they received back to the full system. The trick is to minimize the number of rounds required to guarantee that *enough* devices have received the disseminated messages (regardless of the adversary's disruption behavior). Our lower bound is based on a novel connection to Turán's Theorem [13], a seminal result from extremal graph theory.

In [6], we consider deterministic *adaptive* solutions to gossip, focusing our attention on the optimal case of disseminating at least $n-t$ rumors (i.e., $\epsilon = t/n$). We show that for $\mathcal{F} = \Omega(t^2)$, there exists a linear-time solution. This is a significant improvement over the exponential bounds for these same parameters in the oblivious case. For larger t, however, the performance of the adaptive deterministic solution degrades to exponential complexity. We show this complexity to be fundamental. At the core of our protocols is a new combinatorial object called a *multi-selector*, which captures efficient patterns for separating receiving devices among the available frequencies in a way that minimizes the impact of disruption.

In [4], we close our study of gossip by considering randomized solutions. Due to the power of randomization, we are able to strengthen the adversary by allowing it to send spoofed messages in addition to disrupting frequencies. We begin by generalizing gossip with a problem we call *Authenti-*

cated Message Exchange (AME), which attempts to disseminate messages according to an arbitrary "exchange graph"—a graph with one node for each device and edges describing the messages to be exchanged. We then present f-AME, a "fast" solution to AME that requires $\Theta(|E|t^2 \log n)$ rounds, where $|E|$ describes the edge set of the exchange graph. Initializing this protocol with a complete graph, we can solve gossip for $\epsilon = t/n$ and $t = \mathcal{F} - 1$ in $\Theta(n^2 t^2 \log n)$ rounds—a significant improvement over the exponential bounds of [3, 6] for these same values of ϵ and t.

In this same paper, we also show how to use f-AME to solve shared secret key agreement. Specifically, we allow at least $n - t$ of the honest devices to agree on the same shared secret key—unknown to the adversary. We then show how to use this shared key to initialize an efficient emulation of a reliable, secure, and authenticated single-frequency communication channel.

The papers mentioned above assume that the n devices are labelled 1 through n and start during the same round. In work currently under submission, we relax these assumptions, assuming that devices are activated during arbitrary rounds by the adversary and know only an upper bound on the total number of participants. We show how its possible for these devices to *discover* each other and agree on a common labelling of the rounds—a foundation for adapting the above gossip solutions to this more difficult environment. Specifically, we describe a protocol that guarantees that a device synchronizes to a shared round number within $O\left(\frac{\mathcal{F}}{\mathcal{F}-t} \log^2 n + \frac{\mathcal{F}t}{\mathcal{F}-t} \log n\right)$ rounds of being activated.

5. FUTURE WORK

A variety of interesting theoretical questions remain regarding the DRN model. Arguably, the most pressing is the generalization of the model to multiple hops. Also of interest, however, is the question of whether we can develop basic communication primitives that mask much of the complexity of adversarial interference, therefore simplifying the design of higher-level applications such as gossip, agreement, or point-to-point communication. In addition, though we have some results for the model variant that allows the adversary to spoof messages [4], it remains open as to what other problems are solvable under these harsher conditions. Finally, from the systems perspective, important future work includes the identification of real world scenarios where a safety-critical, interference-resilient protocol would prove useful, with the eventual goal of using the DRN model to design strong solutions. For example, could our gossip protocols be used to resynchronize the nodes of a mesh network in the face of unexpected interference? Or could we use our ad hoc leader election protocol to remove the need for manual pairing in a bluetooth piconet?

The challenge of obtaining reliability in this unreliable setting is non-trivial, but the DRN model, among other efforts, can help move us closer to this goal.

6. REFERENCES

[1] B. Awerbuch, A. Richa, and C. Scheideler. A jamming-resistant mac protocol for single-hop wireless networks. In *The Proceedings of the International Symposium on Principles of Distributed Computing*, 2008.

[2] V. Bhandari and N. H. Vaidya. On reliable broadcast in a radio network. In *The Proceedings of the International Symposium on Principles of Distributed Computing*, pages 138–147, 2005.

[3] S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport. Gossiping in a multi-channel radio network: An oblivious approach to coping with malicious interference. In *The Proceedings of the International Symposium on Distributed Computing*, 2007.

[4] S. Dolev, S. Gilbert, R. Guerraoui, and C. Newport. Secure communication over radio channels. In *The Proceedings of the International Symposium on Principles of Distributed Computing*, 2008.

[5] V. Drabkin, R. Friedman, and M. Segal. Efficient byzantine broadcast in wireless ad hoc networks. In *Dependable Systems and Networks*, pages 160–169, 2005.

[6] S. Gilbert, R. Guerraoui, D. Kowalski, and C. Newport. Interference-resilient information exchange. In *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2009 (To Appear.).

[7] S. Gilbert, R. Guerraoui, and C. Newport. Of malicious motes and suspicious sensors: On the efficiency of malicious interference in wireless networks. In *The Proceedings of the International Conference on Principles of Distributed Systems*, December 2006.

[8] S. Gilbert, R. Guerraoui, and C. Newport. Of malicious motes and suspicious sensors: On the efficiency of malicious interference in wireless networks. *Theoretical Computer Science*, 410(6-7):546–569, 2009.

[9] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan. Understanding and mitigating the impact of rf interference on 802.11 networks. In *SIGCOMM*, pages 385–396. ACM New York, NY, USA, 2007.

[10] C.-Y. Koo. Broadcast in radio networks tolerating byzantine adversarial behavior. In *The Proceedings of the International Symposium on Principles of Distributed Computing*, pages 275–282, 2004.

[11] C.-Y. Koo, V. Bhandari, J. Katz, and N. H. Vaidya. Reliable broadcast in radio networks: The bounded collision case. In *The Proceedings of the International Symposium on Principles of Distributed Computing*, 2006.

[12] A. Pelc and D. Peleg. Broadcasting with locally bounded byzantine faults. *Information Processing Letters*, 93(3):109–115, 2005.

[13] P. Turán. On an extremal problem in graph theory. *Matematicko Fizicki Lapok*, 48, 1941.