Brief Announcement: Towards Robust Medium Access in Multi-Hop Networks

Andrea Richa[1], Christian Scheideler[2], Stefan Schmid[3], Jin Zhang[1]
[1] Arizona State University, [2] University of Paderborn, [3] T-Labs / TU Berlin

1 Introduction

Coordinating the access to a shared medium is a central challenge in wireless networks. Ideally, a Medium Access Control (MAC) protocol should not only be able to use the wireless medium as effectively as possible, but it should also be robust against attacks. Unfortunately, most of today's MAC protocols can be easily attacked. A particularly critical class of attacks are *jamming attacks* (i.e., denial-of-service attacks on the broadcast medium). Jamming attacks are typically easy to implement as the attacker does not need any special hardware. Attacks of this kind usually aim at the physical layer and are realized by means of a high transmission power signal that corrupts a communication link or an area, but they may also occur at the MAC layer, where an adversary may either corrupt control packets or reserve the channel for the maximum allowable number of slots so that other nodes experience low throughput by not being able to access the channel. In this paper we focus on jamming attacks on the physical layer, that is, the interference caused by the jammer will not allow the nodes to receive messages. The fundamental question that we are investigating is: *Is there a MAC protocol so that for any physical-layer jamming strategy, the protocol will still be able to achieve an asymptotically optimal throughput for the non-jammed time steps?* Such a protocol would *force* the jammer to jam all the time in order to prevent any successful message transmissions. Finding such a MAC protocol is not a trivial problem. In fact, the widely used IEEE 802.11 MAC protocol already fails to deliver any messages for very simple oblivious jammers that jam only a small fraction of the time steps [2]. On the positive side, Awerbuch et al. [1] have demonstrated that there are MAC protocols which are provably robust against even powerful, adaptive jamming, but their results only hold for single-hop wireless networks with a single jammer, that is, all nodes experience the same jamming pattern.

In this paper, we significantly extend the results in [1]. We present a MAC protocol called JADE (a short form of "jamming defense") that can achieve a constant fraction of the best possible throughput for a large class of jamming strategies in a large class of multi-hop networks where transmissions and interference can be modeled using unit-disk graphs.

2 Model

We consider the problem of designing a robust MAC protocol for multi-hop wireless networks with a single wireless channel. The wireless network is modeled as a *unit disk graph* (UDG) $G = (V, E)$ where V represents a set of $n = |V|$ honest and reliable nodes and two nodes $u, v \in V$ are within each other's transmission range, i.e., $\{u, v\} \in E$, if and only if their (normalized) distance is at most 1. We assume that time proceeds in synchronous time steps called *rounds*.

In each round, a node may either transmit a message or sense the channel, but it cannot do both. A node which is sensing the channel may either (*i*) sense an *idle* channel (if no other node in its transmission range is transmitting at that round and its channel is not jammed), (*ii*) sense a *busy* channel (if two or more nodes in its transmission range transmit at that round or its channel is jammed), or (*iii*) *receive* a packet (if exactly one node in its transmission range transmits at that round and its channel is not jammed).

In addition to these nodes there is an adversary (who may control any number of jamming devices). We allow the adversary to know the protocol and its entire history and to use this knowledge in order to jam the wireless channel at will at any round (i.e, the adversary is *adaptive*). However, like in [1], the adversary has to make a jamming decision *before* it knows the actions of the nodes at the current round. The adversary can jam the nodes individually at will, as long as for every node v, at most a $(1-\epsilon)$-fraction of its rounds is jammed, where $\epsilon > 0$ can be an arbitrarily small constant. That is, v has the chance to receive a message in at least an ϵ-fraction of the rounds. More formally, an adversary is called $(T, 1-\epsilon)$-*bounded* for some $T \in \mathbb{N}$ and $0 < \epsilon < 1$, if for any time window of size $w \geq T$ and at any node v, the adversary can jam at most $(1-\epsilon)w$ of the w rounds at v.

In order to investigate the issue of multiple jammers in more detail, we also introduce the notion of a k-uniform adversary. An adversary is *k-uniform* if the node set V can be partitioned into k subsets so that the jamming pattern is the same within each subset.

Given a node v and a time interval I, we define $f_v(I)$ as the number of time steps in I that are non-jammed at v and $s_v(I)$ as the number of time steps in I in which v successfully receives a message. A MAC protocol is called *c-competitive* against some $(T, 1-\epsilon)$-bounded adversary if, for any time interval I with $|I| \geq K$ for a sufficiently large K (that may depend on T and n),

$$\sum_{v \in V} s_v(I) \geq c \cdot \sum_{v \in V} f_v(I).$$

In other words, a c-competitive MAC protocol can achieve at least a c-fraction of the best possible throughput.

Our goal is to design a *symmetric local-control* MAC protocol (i.e., there is no central authority controlling the nodes, and all the nodes are executing the same protocol) that has a constant-competitive throughput against any $(T, 1-\epsilon)$-bounded adversary in any multi-hop network that can be modeled as a UDG.

In this paper, we will say that a claim holds *with high probability (w.h.p.)* iff it holds with probability at least $1 - 1/n^c$ for any constant $c \geq 1$

3 The JADE Protocol

JADE is a fairly simple protocol: it is based on a very small set of rules and has a minimal storage overhead. We believe that these properties make our protocol interesting for a real deployment. In contrast to the algorithm, our stochastic analysis is rather involved as it requires to shed light onto the complex interplay between the nodes all following their randomized protocol in a highly dependent manner and an adversary.

In JADE, each node v maintains a probability value p_v, a threshold T_v and a counter c_v. The parameter $\gamma < 1$ is the same for every node and is set to some sufficiently small value (that will be specified below). Let $\hat{p}$ be any constant so that $0 < \hat{p} \leq 1/24$.

Initially, every node v sets $T_v := 1$, $c_v := 1$ and $p_v := \hat{p}$. Afterwards, the protocol works in synchronized rounds. In every round, each node v decides with probability p_v to send a message. If it decides not to send a message, it checks the following two conditions:

- If v senses an idle channel, then $p_v := \min\{(1+\gamma)p_v, \hat{p}\}$.
- If v successfully receives a message, then $p_v := (1+\gamma)^{-1}p_v$ and $T_v := \max\{T_v - 1, 1\}$.

Afterwards, v sets $c_v := c_v + 1$. If $c_v > T_v$ then it does the following: v sets $c_v := 1$, and if there was no round among the past T_v rounds in which v sensed a successful message transmission *or an idle channel*, then $p_v := (1+\gamma)^{-1}p_v$ and $T_v := T_v + 1$.

The concept of using a multiplicative-increase-multiplicative-decrease mechanism for p_v and an additive-increase-additive-decrease mechanism for T_v, as well as the slight addition to the protocol in [1], marked in italic above, are crucial for JADE to work.

4 Results

JADE has the following properties.

Theorem 4.1. *When considering a time interval of $\Omega((T\log n)/\epsilon + poly(\log n, 1/\epsilon))$ length,* JADE *has a constant competitive throughput for any $(T, 1-\epsilon)$-bounded adversary and any UDG w.h.p. as long as $\gamma = O(1/(\log T + \log\log n))$ and (a) the adversary is 1-uniform and the UDG is connected, or (b) there are at least $2/\epsilon$ nodes within the transmission range of every node.*

Note that in reality, $\log T$ and $\log\log n$ should be rather small so that our condition on γ is not too restrictive. On the other hand, we can also show the following result demonstrating that Theorem 4.1 essentially captures all the scenarios (within our notation) under which JADE can have a constant competitive throughput.

Theorem 4.2. *If (a) the UDG is not connected, or (b) the adversary is allowed to be 2-uniform and there are nodes with $o(1/\epsilon)$ nodes within their transmission range, then there are cases in which* JADE *is not constant competitive for a constant c independent of ϵ.*

Certainly, no MAC protocol can guarantee a constant competitive throughput if the UDG is not connected. However, it is still open whether there are simple MAC protocols that are constant competitive under non-uniform jamming strategies even if there are $o(1/\epsilon)$ nodes within the transmission range of a node.

References

[1] B. Awerbuch, A. Richa, and C. Scheideler. A jamming-resistant mac protocol for single-hop wireless networks. In *Proc. of PODC '08*, pages 45–54, 2008.

[2] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa. On the performance of IEEE 802.11 under jamming. In *Proc. of IEEE Infocom '08*, pages 1265–1273, 2008.

[3] E. Lebhar and Z. Lotker. Unit disk graph and physical interference model: Putting pieces together. In *23rd IEEE Intl. Symp. on Parallel and Distributed Processing (IPDPS)*, pages 1–8, 2009.