Competitive and Fair Medium Access despite Reactive Jamming

ICDCS 2011

Andrea Richa (ASU)
Christian Scheideler (U of Paderborn)
Stefan Schmid (TU Berlin/T-Labs)
Jin Zhang (ASU)

Motivation

Channel availability hard to model:

- Background noise
- Temporary obstacles
- Mobility
- Co-existing networks
- Jammer

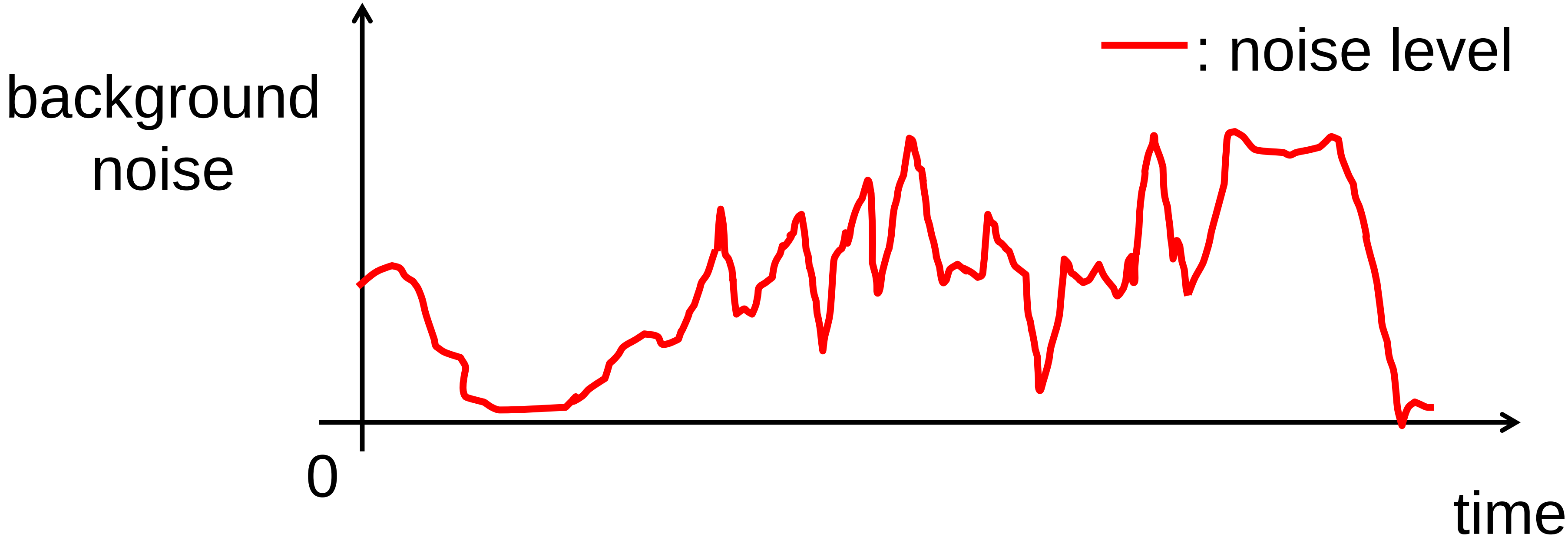
Motivation

Ideal world:

Usual approach adopted in theory.

Motivation

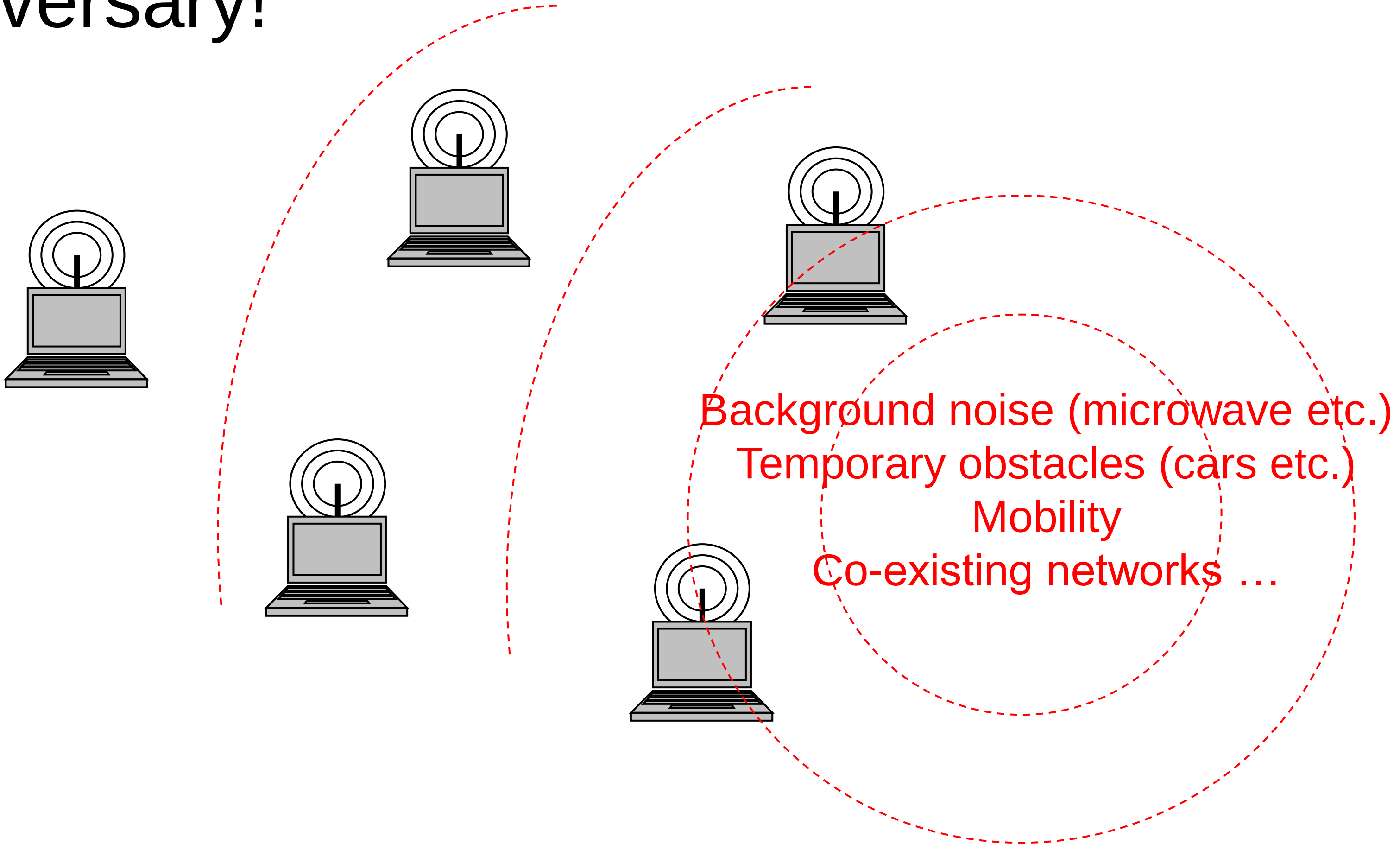
Real world:



How to model this???

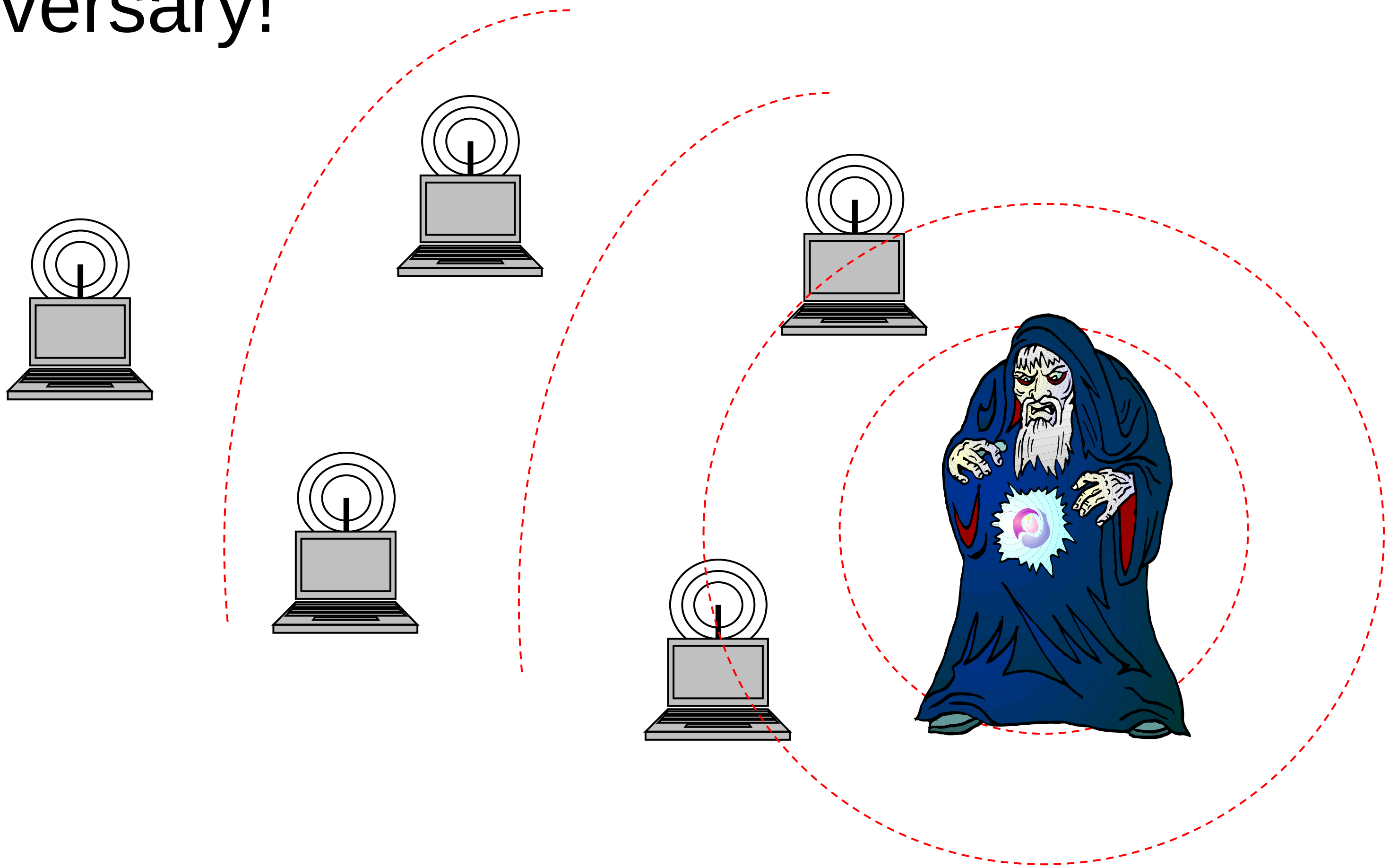
Our Approach: Adversarial Jamming

Idea: model unpredictable behaviors via adversary!



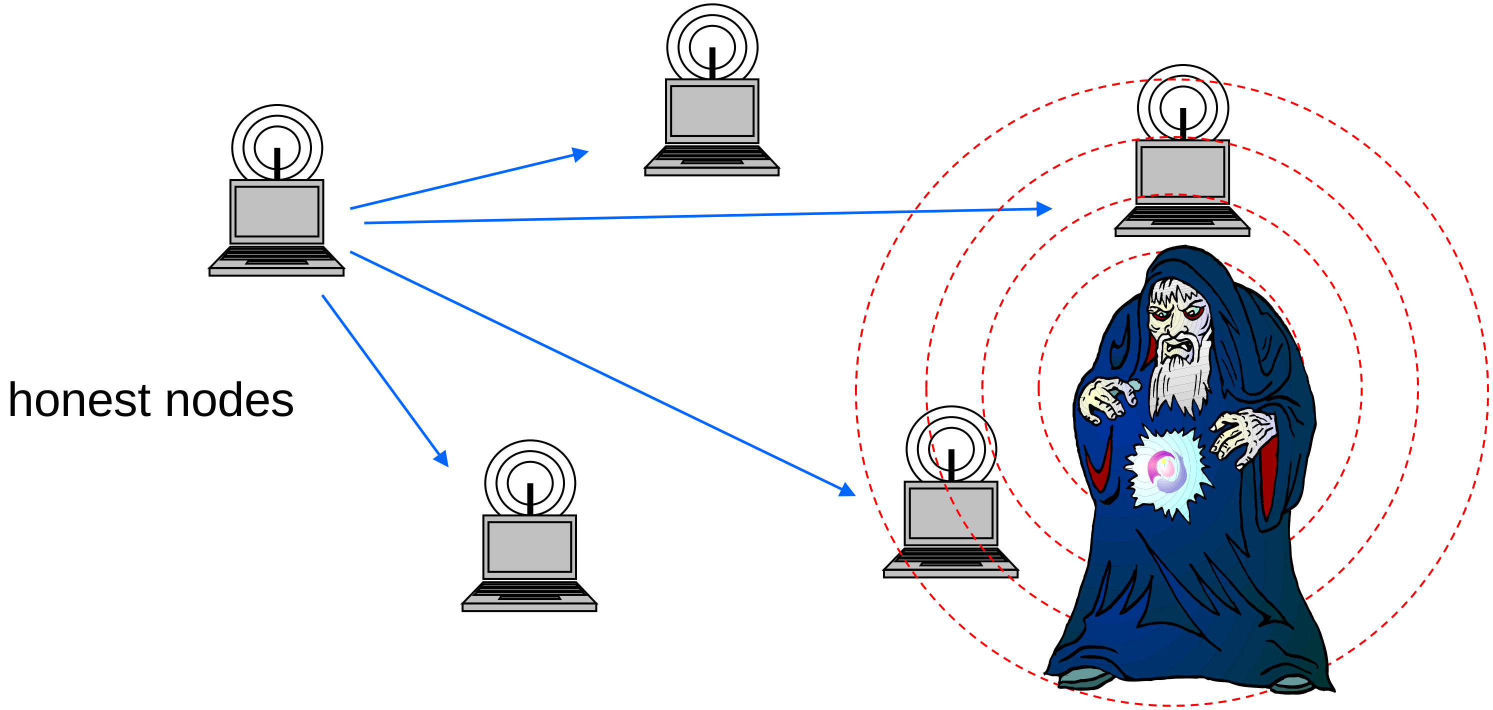
Our Approach: Adversarial Jamming

Idea: model unpredictable behaviors via adversary!



Adversarial physical layer jamming

- a jammer listens to the open medium and broadcasts in the same frequency band as the network
  - no special hardware required
  - can lead to significant disruption of communication at low cost

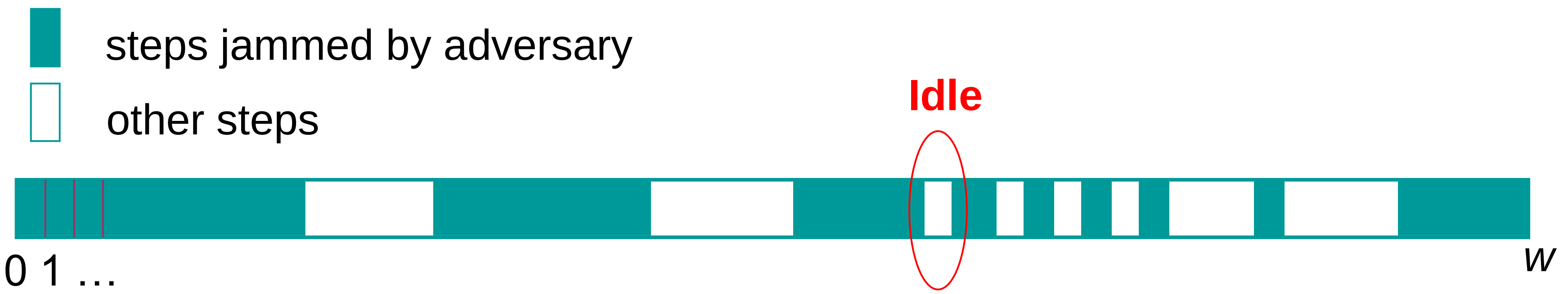


Reactive adversary

- $(T, 1-\varepsilon)$-bounded adversary, $0 < \varepsilon < 1$: in any time window of size $w \geq T$, the adversary can jam $\leq (1-\varepsilon)w$ time steps
- Adaptive: knows protocol and entire history
- Reactive: can use physical carrier sensing to make a jamming decision based on the actions of the nodes at the current step (much more powerful than non-reactive adversary!)

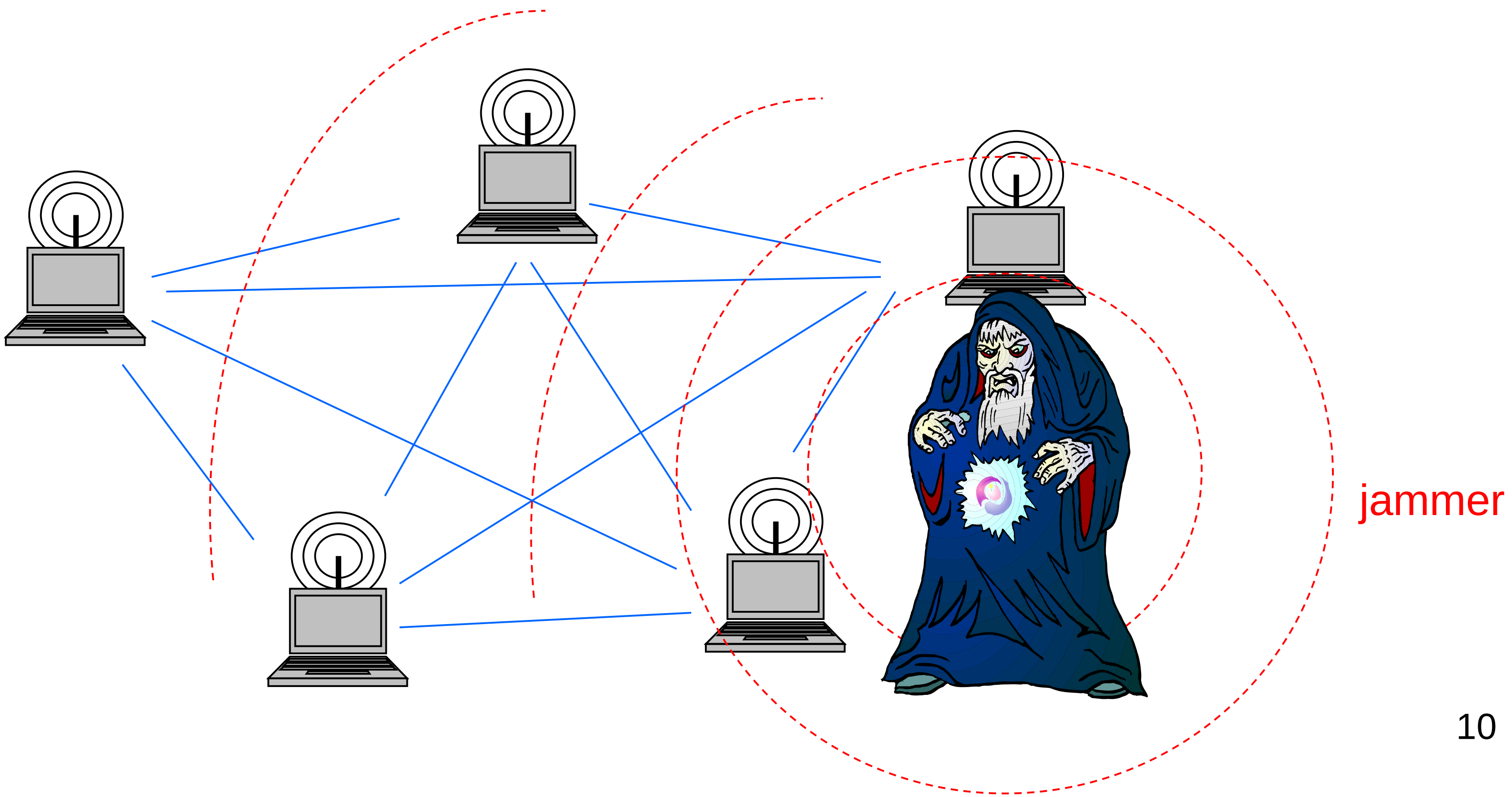
Reactive adversary

- (T,1-ε)-bounded adversary, $0 < \varepsilon < 1$: in any time window of size $w \geq T$, the adversary can jam $\leq (1-\varepsilon)w$ time steps
- Adaptive: knows protocol and entire history
- Reactive: can use physical carrier sensing to make a jamming decision based on the actions of the nodes at the current step (much more powerful than non-reactive adversary!)



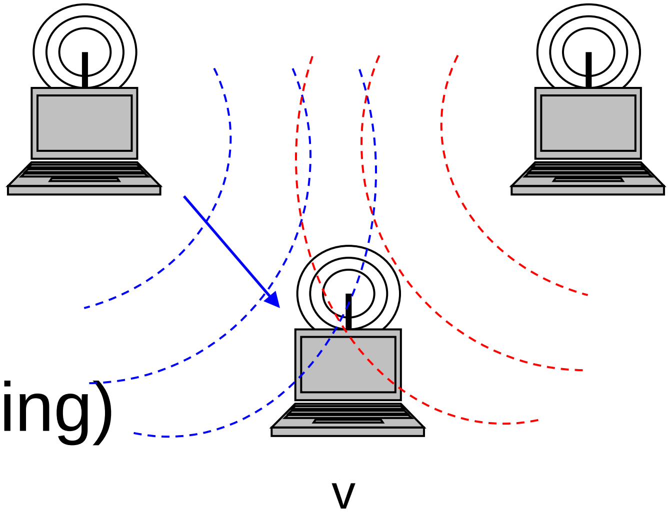
Single-hop wireless network

- *n* reliable honest nodes and one jammer; all nodes within transmission range of each other and of the jammer



Wireless communication model

- at each time step, a node may decide to transmit a packet (nodes continuously contend to send packets)
- a node may transmit *or* sense the channel at any time step (half-duplex)
- when sensing the channel a node *v* may
  - sense an idle channel
  - receive a packet
  - sense a busy channel (cannot distinguish between message collisions and adversarial jamming)

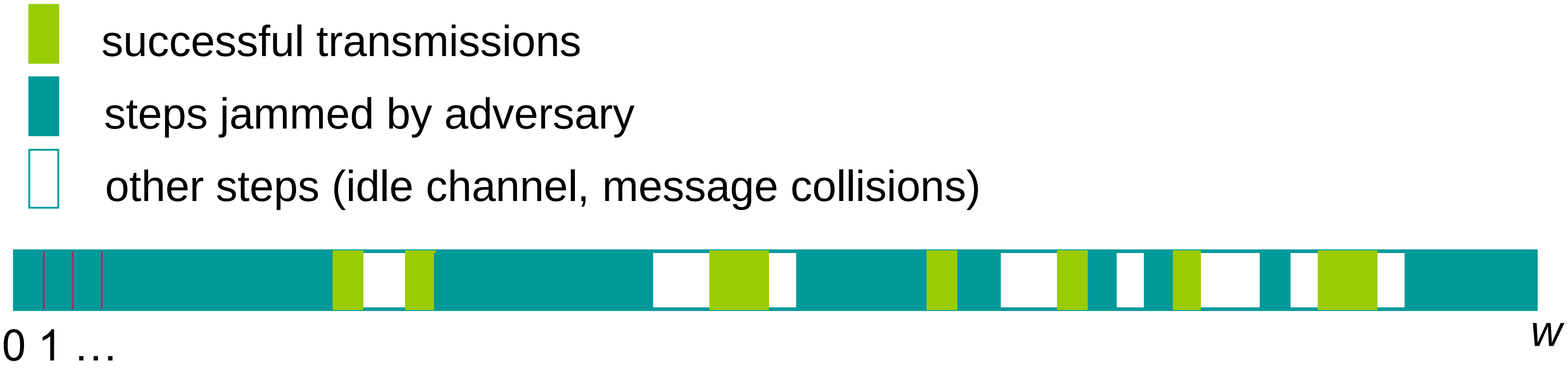


Fairness

- the channel access probabilities among nodes do not differ by more than a small factor after the first message was sent successfully.

Constant-competitive protocol

- a protocol is called constant-competitive against a (T,1-ε)-bounded adversary if the nodes manage to perform successful transmission in at least a constant fraction of the steps not jammed by the adversary, for any sufficiently large number of steps (w.h.p. or on expectation)



Our main contribution

- symmetric local-control MAC protocol, ANTIJAM, that is fair and constant competitive against any $(T, 1-\varepsilon)$-bounded reactive adversary after sufficiently large number of time steps w.h.p., for any constant $0 < \varepsilon < 1$, and any T.

Related Work

- spread spectrum & frequency hopping:
  - rely on broad spectrum. However, sensor nodes or common wireless devices based on 802.11 have very narrow bandwidths.
  - Our approach is orthogonal to broad spectrum techniques, and can be used in conjunction with those.
- random backoff:
  - reactive adversary too powerful for MAC protocols based on random backoff or tournaments (including the standard MAC protocol of 802.11 [BKLNRT'08])
- jamming-resistant MAC for single-hop [ARS'08]:
  - can achieve constant throughput in single-hop wireless networks, only under adaptive but non-reactive adversary model; leads to unfair access probabilities

Simple idea

- each node v sends a message at current time step with probability $p_v \leq p_{max}$, for constant $0 < p_{max} << 1$.
  $p = \sum p_v$ (cumulative probability)
  q_{idle} = probability the channel is idle
  $q_{success}$ = probability that only one node is transmitting (successful transmission)

- Claim. $q_{idle} \cdot p \leq q_{success} \leq (q_{idle} \cdot p) / (1 - p_{max})$

$\therefore$

if (number of times the channel is idle) $\cong$ (number of successful transmissions) $\longrightarrow$ $p = \theta(1)$!
(what we want!)

Basic approach

- a node v adapts p_v based only on steps when an idle channel or a successful message transmission are observed, ignoring all other steps (including all the blocked steps when the adversary transmits!)!

Basic approach

- a node v adapts p_v based only on steps when an idle channel or a successful message transmission are observed, ignoring all other steps (including all the blocked steps when the adversary transmits!)!

ANTIJAM Protocol

- each node v maintains
  - probability value p_v ,
  - time window threshold T_v
  - counter c_v, and
  - $\gamma = O(1/(\log T + \log\log n))$
- Initially, $T_v = c_v = 1$ and $p_v = p_{max}$ (< 1/24).
- synchronized time steps (for ease of explanation)

ANTIJAM Protocol

In each step:

- node v sends a message along with a tuple (p_v ,c_v ,T_v) with probability p_v . If v decides not to send a message then
  - if v senses an idle channel, then $p_v = \min\{(1+ \gamma)p_v , p_{max}\}$ and $T_v = \max\{T_v - 1, 1\}$
  - if v successfully receives a message along with the tuple of (p_{new} ,c_{new} ,T_{new}), then $p_v = p_{new}/(1+ \gamma)$, $c_v = c_{new}$, and $T_v = T_{new}$
- $c_v = c_v + 1$. If $c_v > T_v$ then
  - $c_v = 1$
  - if v did not sense an idle channel in the last T_v steps then $p_v = p_v/(1+ \gamma)$ and $T_v = T_v + 2$

ANTIJAM Protocol

In each step:

- node v sends a message along **<u>with a tuple (p_v ,c_v ,T_v)</u>** with probability p_v . If v decides not to send a message then
  - if v senses an idle channel, then $p_v = \min\{(1+\gamma)p_v , p_{max}\}$ and **<u>$T_v = \max\{T_v - 1, 1\}$</u>**
  - if v successfully receives a message along with the tuple of **<u>(p_{new} ,c_{new} ,T_{new}), then $p_v = p_{new} /(1+\gamma)$, $c_v = c_{new}$, and $T_v = T_{new}$</u>**

- $c_v = c_v + 1$. If $c_v > T_v$ then
  - $c_v = 1$
  - **<u>if v did not sense an idle channel in the last T_v steps then</u>**

    <u>$p_v = p_v /(1+\gamma)$ and $T_v = T_v + 2$</u>

Our results

- Let $N = \max\{T,n\}$
- Theorem. The ANTIJAM protocol can achieve:

1. fairness: the channel access probabilities among nodes do not differ by more than a factor of $(1+\gamma)$ after the first message was sent successfully.

2. $e^{-\theta(1/\epsilon^2)}$ - competitiveness w.h.p., under any $(T,1-\varepsilon)$-bounded reactive adversary if the protocol is executed for $\Theta(\frac{1}{\varepsilon}\log N \max\{T, (e^{\delta/\varepsilon^2}/\varepsilon\gamma^2)\log^3 N\})$ steps, where $\varepsilon \in (0,1)$ is a constant, $\gamma = O(1/(\log T + \log\log n))$, and δ is a sufficiently large constant.

Proof sketch: Fairness

- Fact:
  - Right after u sends a message successfully along with the tuple (p_u, c_u, T_u), $(p_v, c_v, T_v) = (p_u / (1+\gamma), c_u, T_u)$ for all receiving nodes v, while the sending node values stay the same. In particular, for any time step t after a successful transmission by node u, $(c_v, T_v) = (c_w, T_w)$ for all nodes v and $w \in V$

  - This implies that after a successful transmission, the access probabilities of any two nodes in the network will never differ by more than a factor $(1+\gamma)$ in the future.

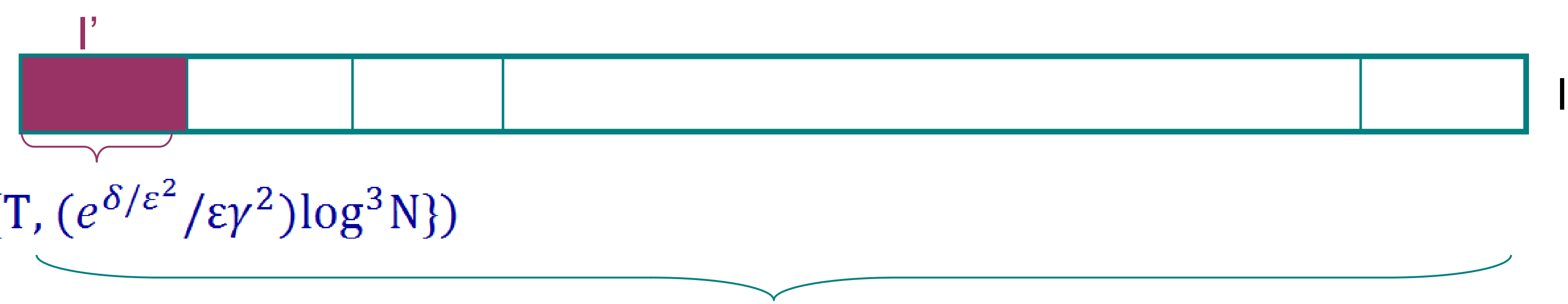
Proof sketch: Constant Competitiveness

- We study the competitiveness of the protocol for $F = \Theta(\frac{1}{\varepsilon} \log N \max\{T, (e^{\delta/\varepsilon^2}/\varepsilon\gamma^2)\log^3 N\})$ many steps

  $\downarrow$

  If we can show constant competitiveness for any such F, the theorem follows

- Use induction over sufficiently large time frames:



$f = \max\{T, (e^{\delta/\varepsilon^2}/\varepsilon\gamma^2)\log^3 N\})$

$F = \theta(\log N / \varepsilon) \cdot f$

Proof sketch: Constant Competitiveness

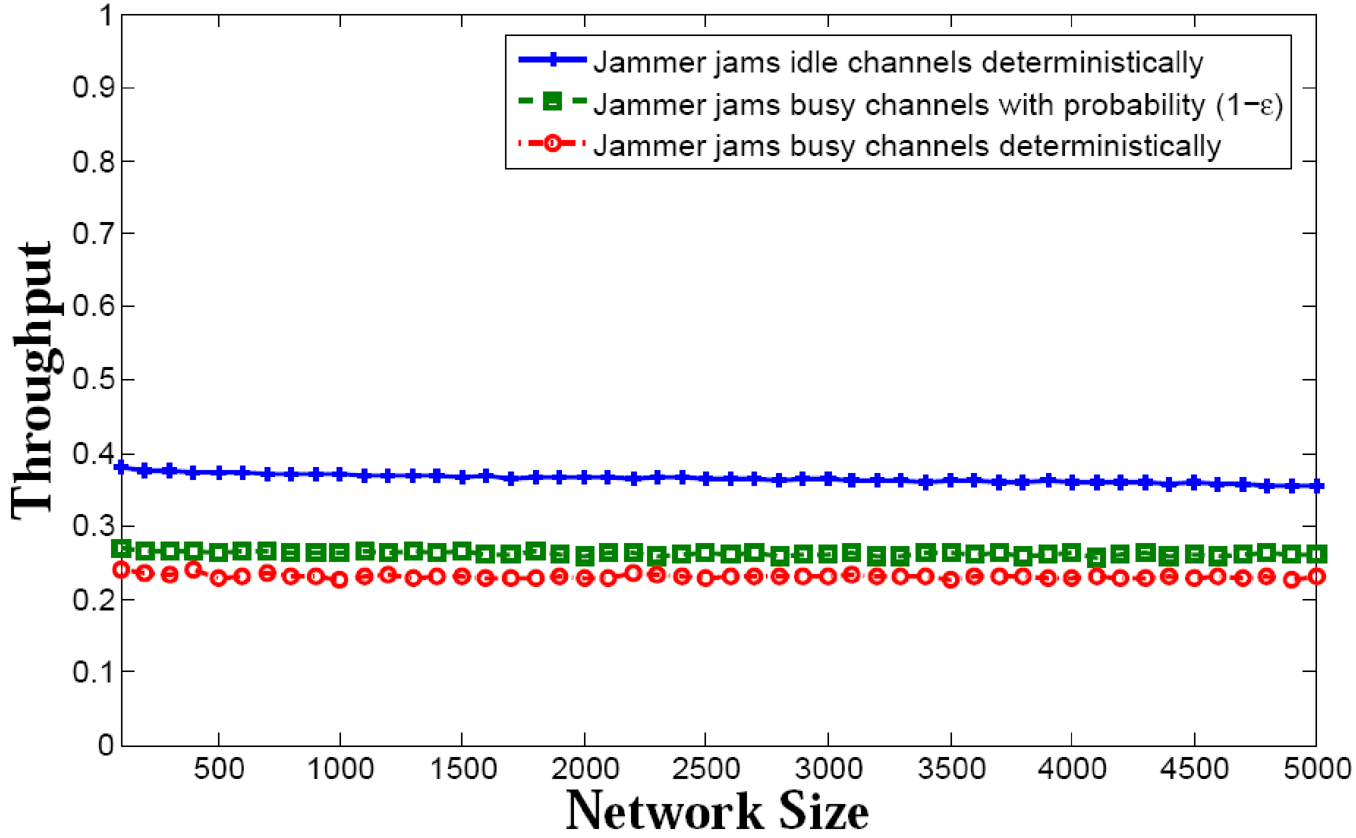
- First, show that constant competitive can be achieved w.h.p., when cumulative probability $p_t \leq \delta/\varepsilon^2$ for at least half of the non-jammed time steps t in a subframe I'.

- Second, show that at most half of the non-jammed time steps t in a subframe I' can have the property that $p_t > \delta/\varepsilon^2$, w.h.p.

- Then follow the same line as in [ARS'08], show that ANTIJAM is self-stabilizing.

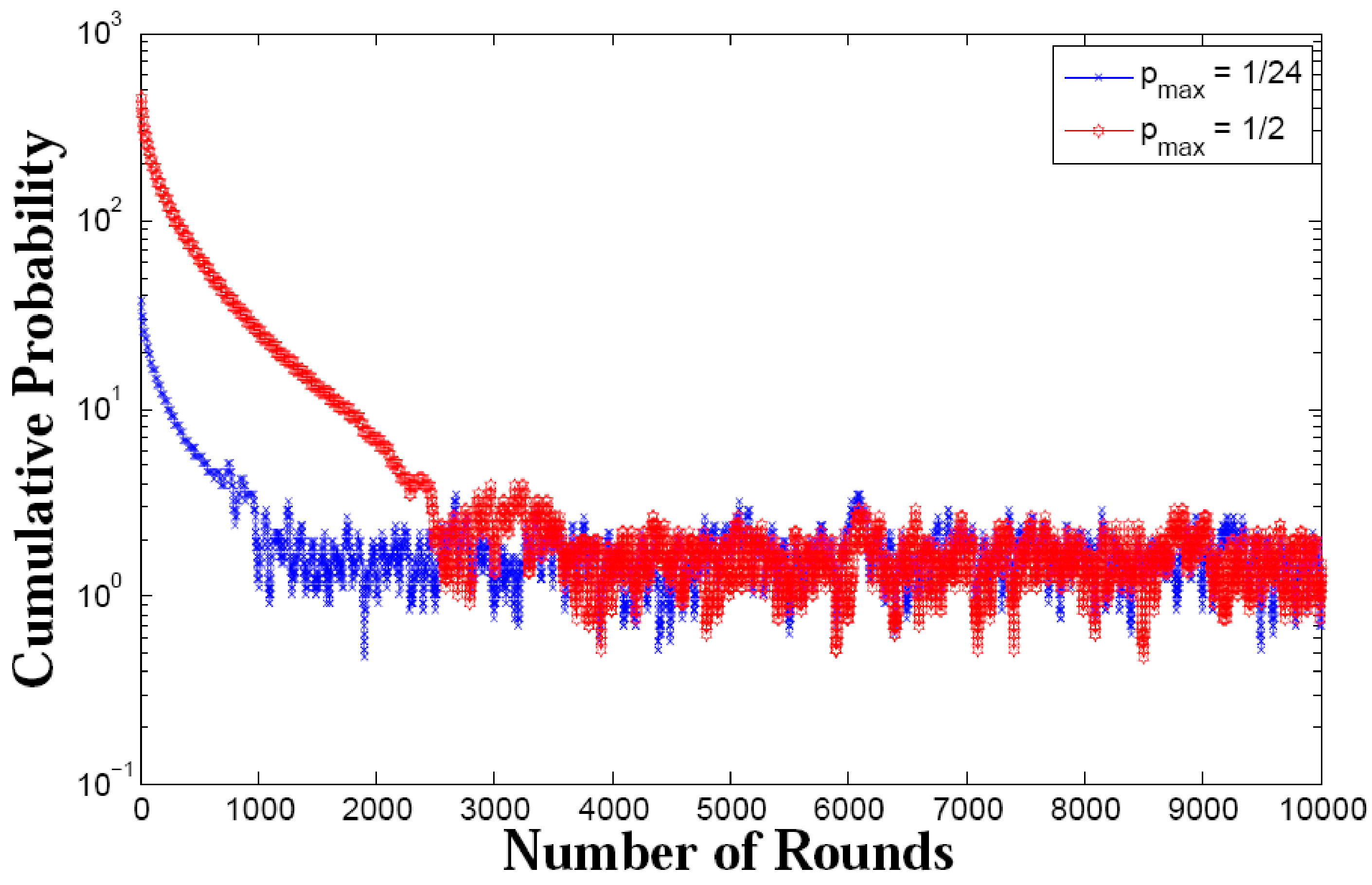
ANTIJAM Protocol

Experiment 1: Constant competitiviness



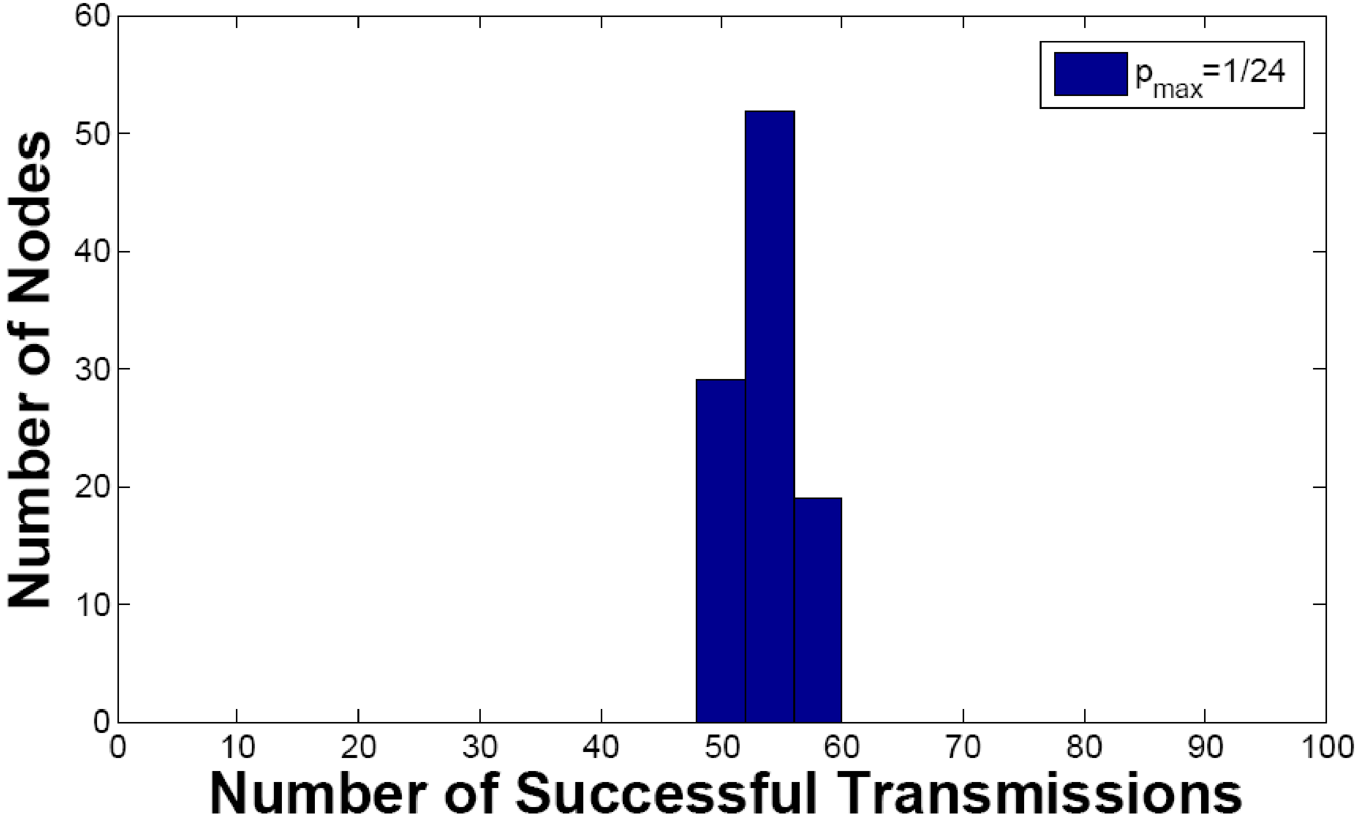
ANTIJAM Protocol

Experiment 2: Convergence time



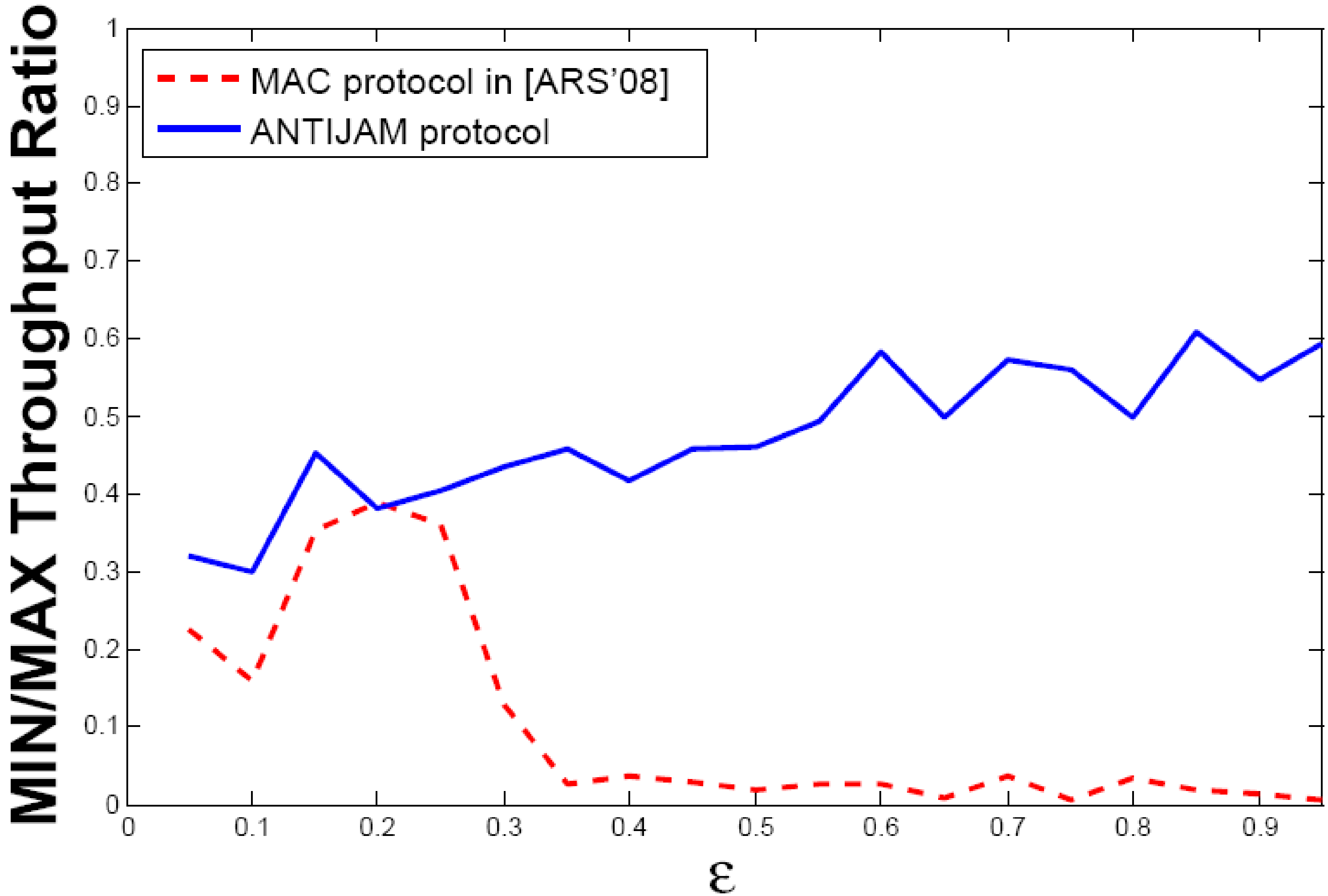
ANTIJAM Protocol

Experiment 3: Fairness



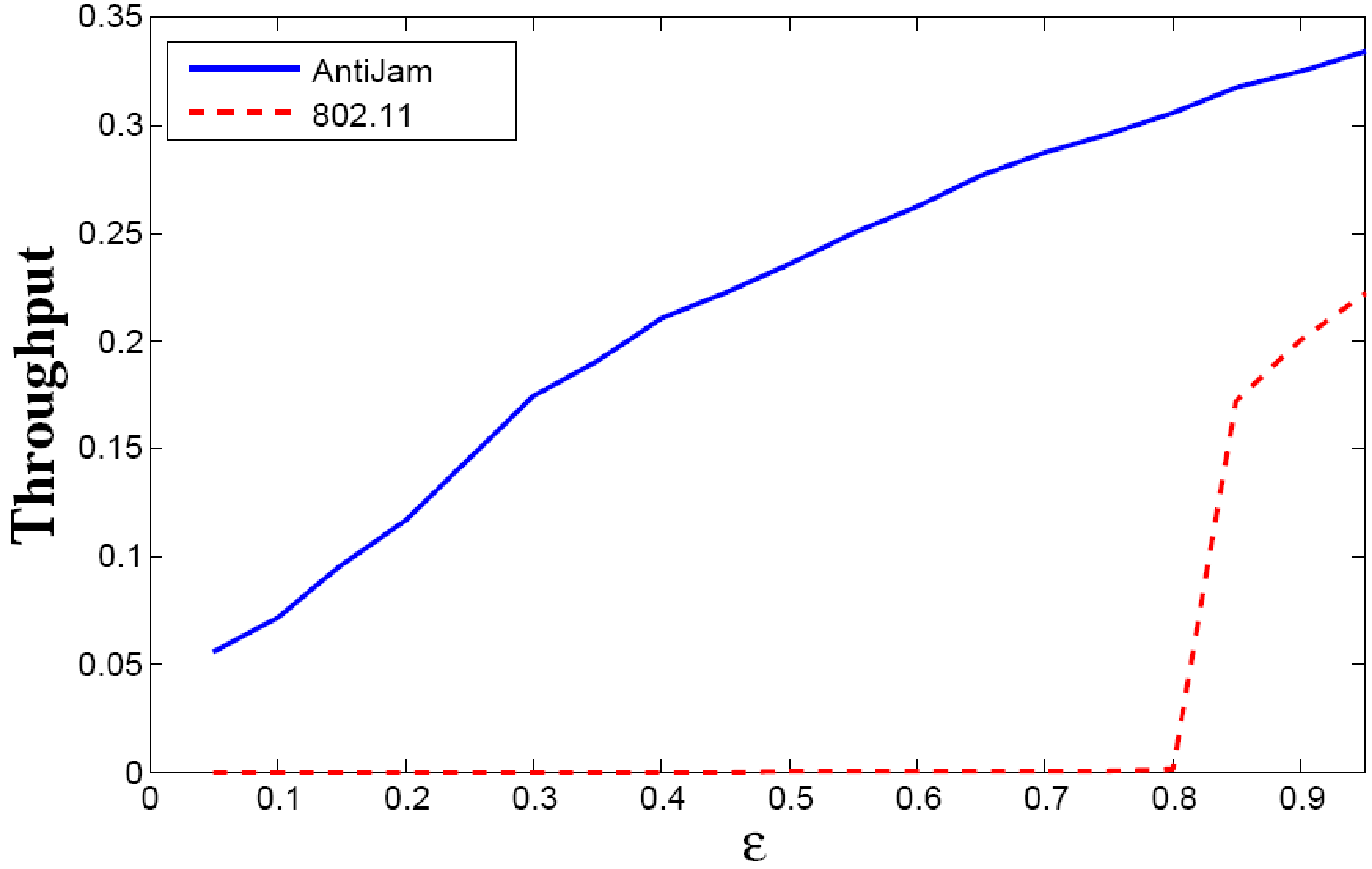
ANTIJAM Protocol

Experiment 4: Fairness (ANTIJAM vs. [ARS'08])



ANTIJAM Protocol

Experiment 5: ANTIJAM vs. 802.11

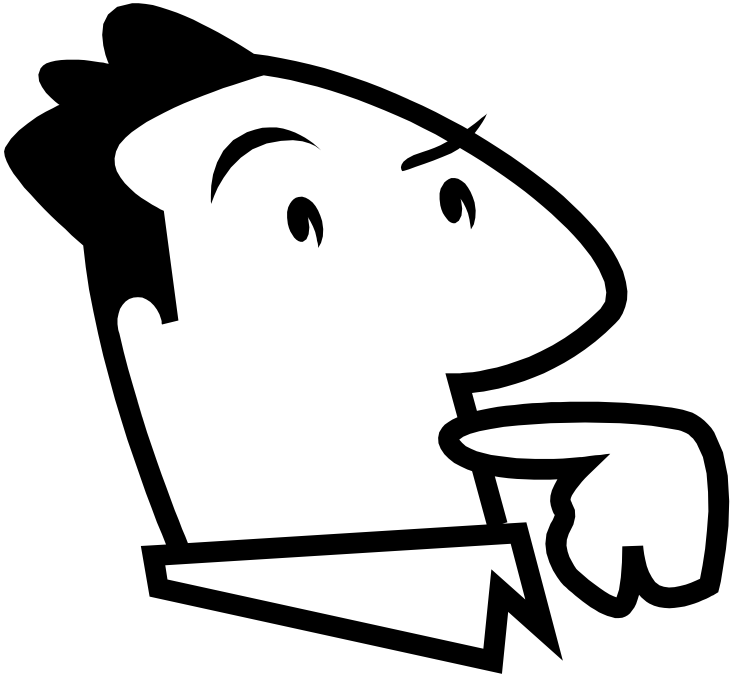


Future Work

- Can ANTIJAM perform well in physical interference model, i.e., SINR?

$$\frac{P_v(u)}{N + \sum_{w \in S} P_v(w)} \geq \beta$$

- Closing gaps in terms of ε.
  - $e^{-\theta(1/\varepsilon^2)}$ - competitiveness



Questions?