Competitive and Fair Throughput for Co-Existing Networks Under Adversarial Interference

PODC 2012

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

Co-existing wireless networks

- *$K>1$* different, independent networks that share the same wireless spectrum
  - *no collaboration* among different networks
  - transmission in one network is viewed as *noise by other networks*
    - E.g., networks use different encryption schemes

Possible scenarios

- Security Council, UN

- Ad-hoc Emergency Service Networks

Challenges

- How to *differentiate* successful transmissions in a different network from collisions (concurrent transmissions)?

- How to guarantee *fairness*, within a single network, and among different networks?

Our results

- *s(i):* number of successful transmissions for network *i*
- Throughput: $\sum_i s(i)$
- Fairness: differences $|s(i) - s(j)|$ are small
- Medium Access Control (MAC) protocol: local algorithm that decides which nodes transmit at any time step

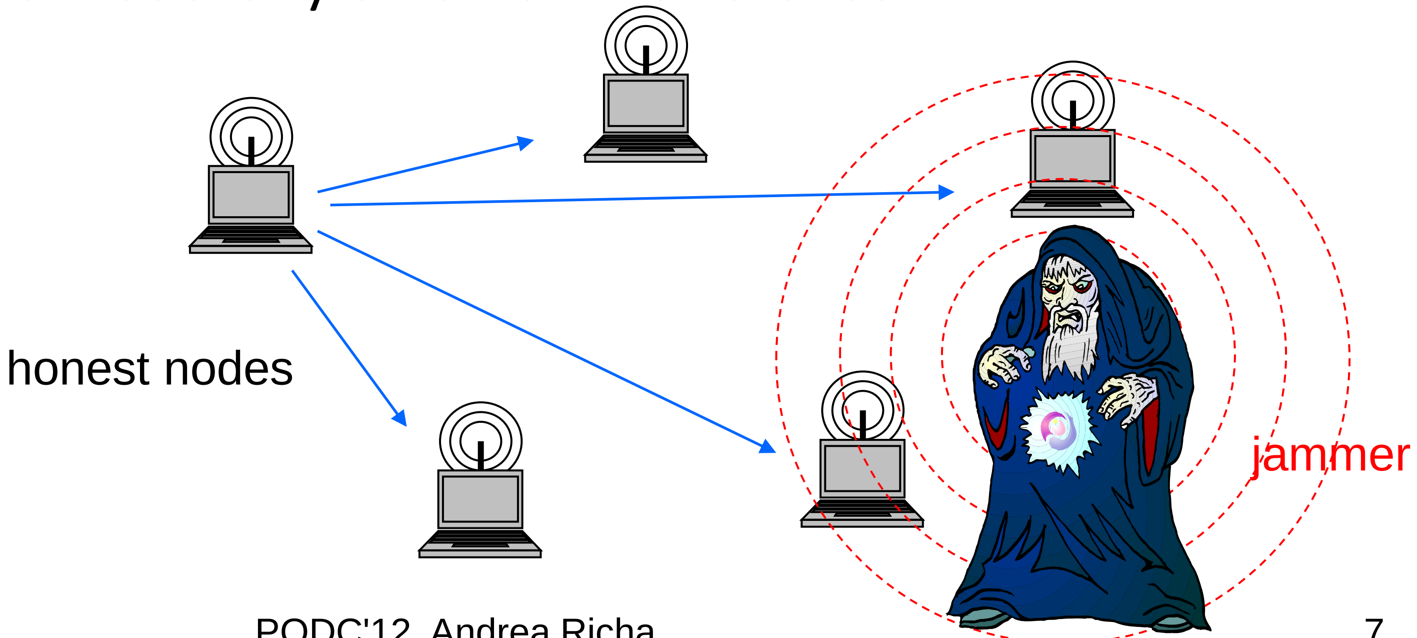
Our results: a jamming-resistant MAC protocol that can achieve *provably high throughput* and *fairness* in co-existing networks setting.

Why do we care?

- Spectrum resource is limited
- External interference
  - Unintentional: from other networks, collisions
  - Intentional: adversary
- Existing MAC protocols do *not* work well when co-existing networks are present

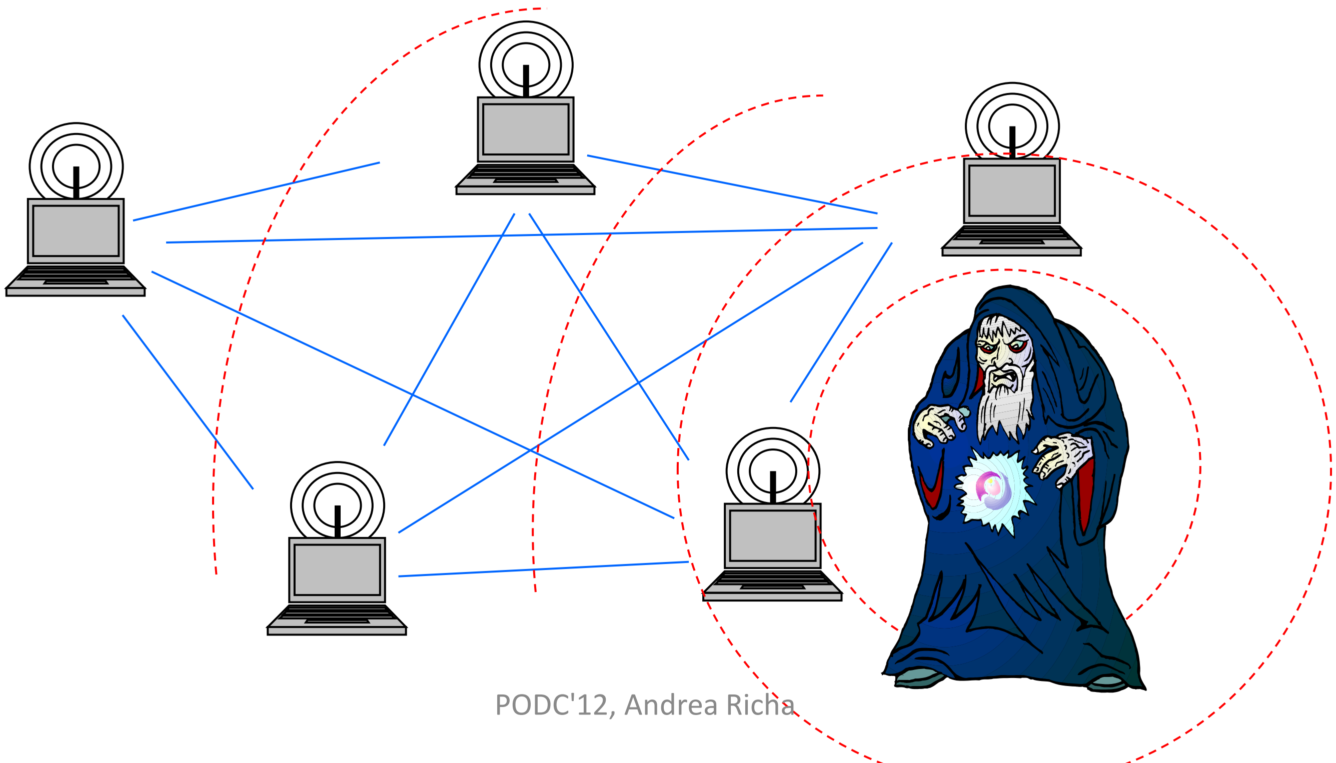
Adversarial physical layer jamming

- an adversary (jammer) listens to the open medium and broadcasts in the same frequency band as the networks
  - can lead to significant disruption of communication at low cost
  - used to model any external interference



Single-hop wireless network

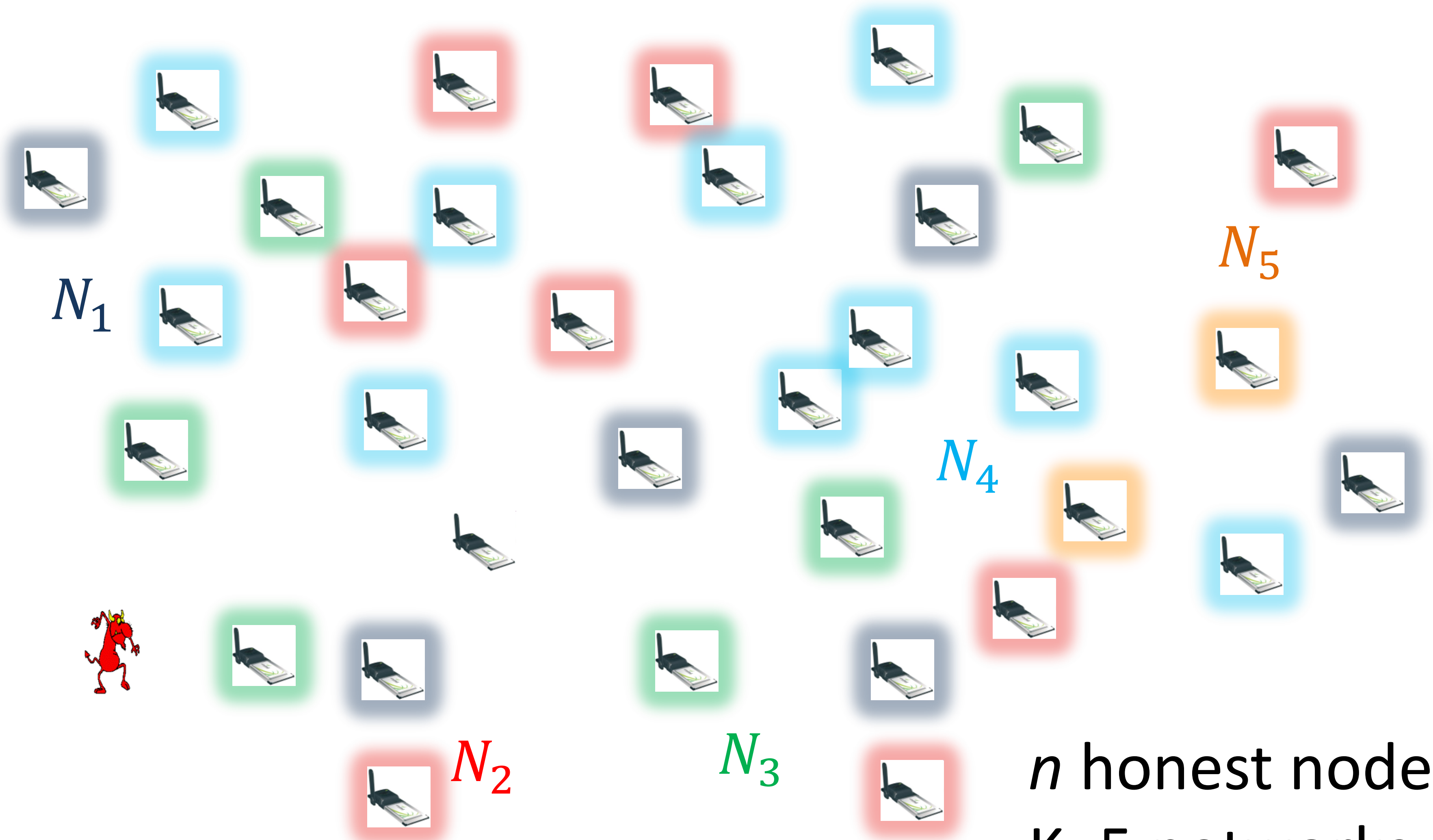
- *n* reliable honest nodes and a jammer; all nodes *within transmission range* of each other and of the jammer
- Nodes do *not* know *n*, nor the number of networks *K*



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)

Co-existing Networks

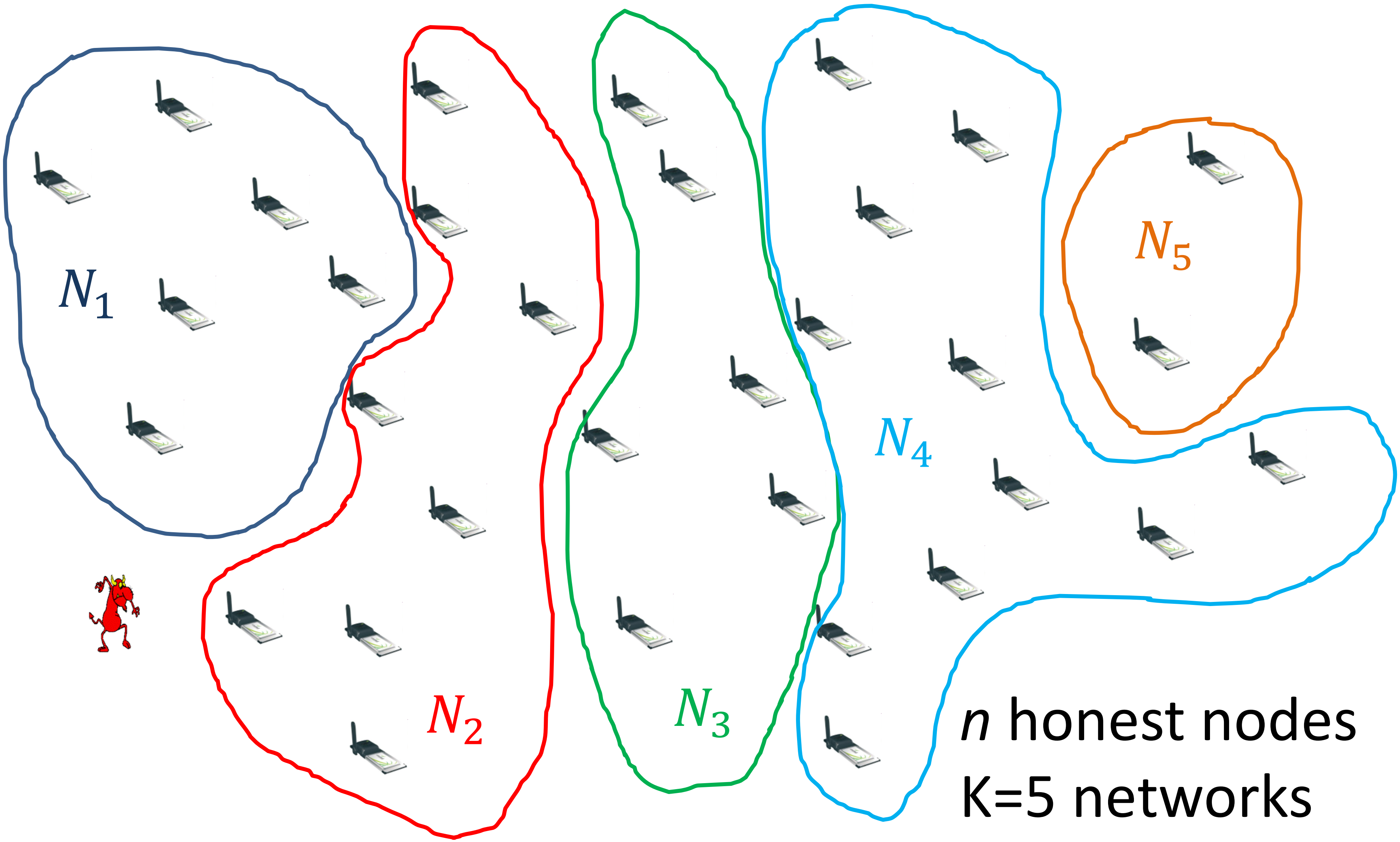


n honest nodes

K=5 networks

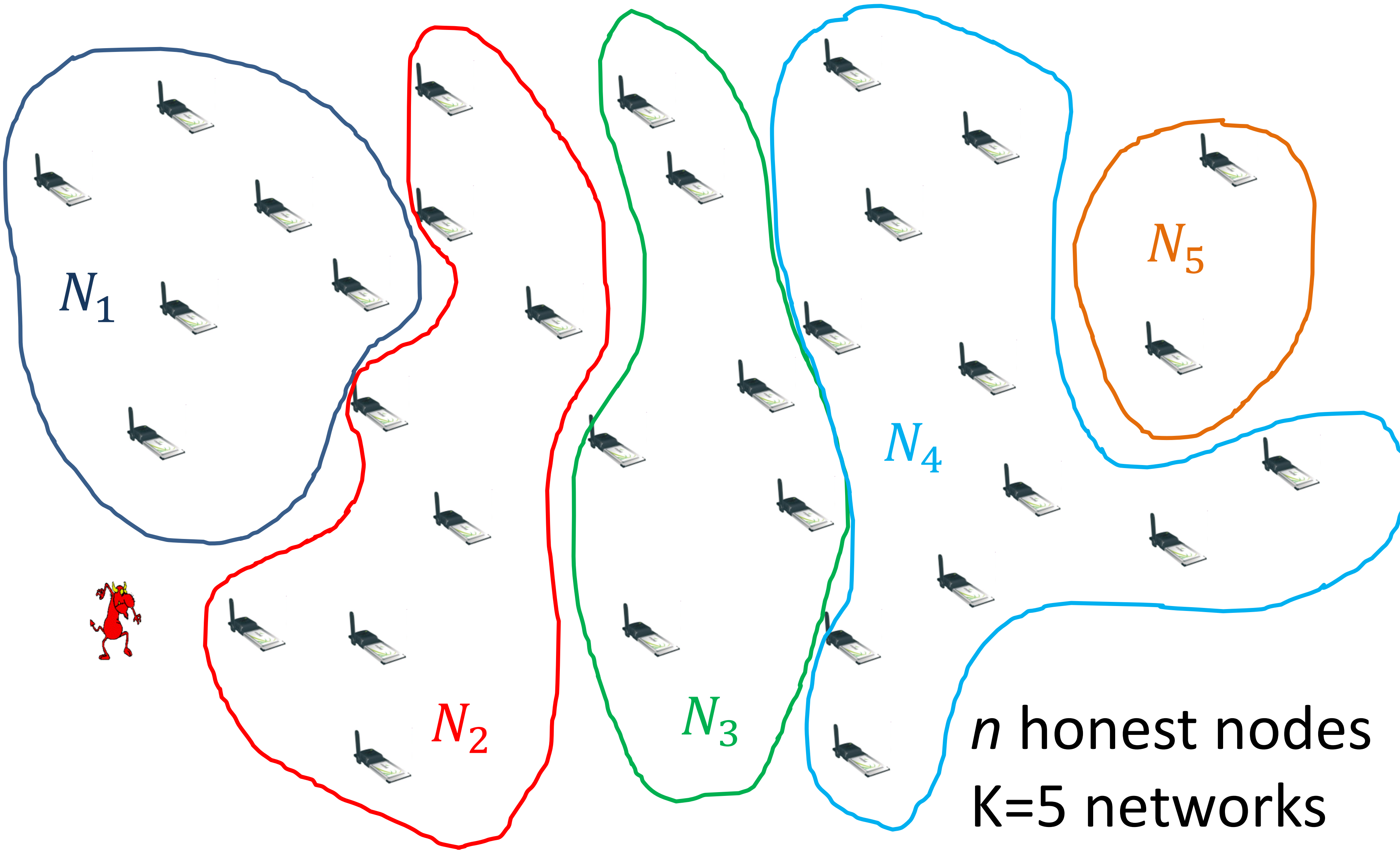
Single-hop

Co-existing Networks



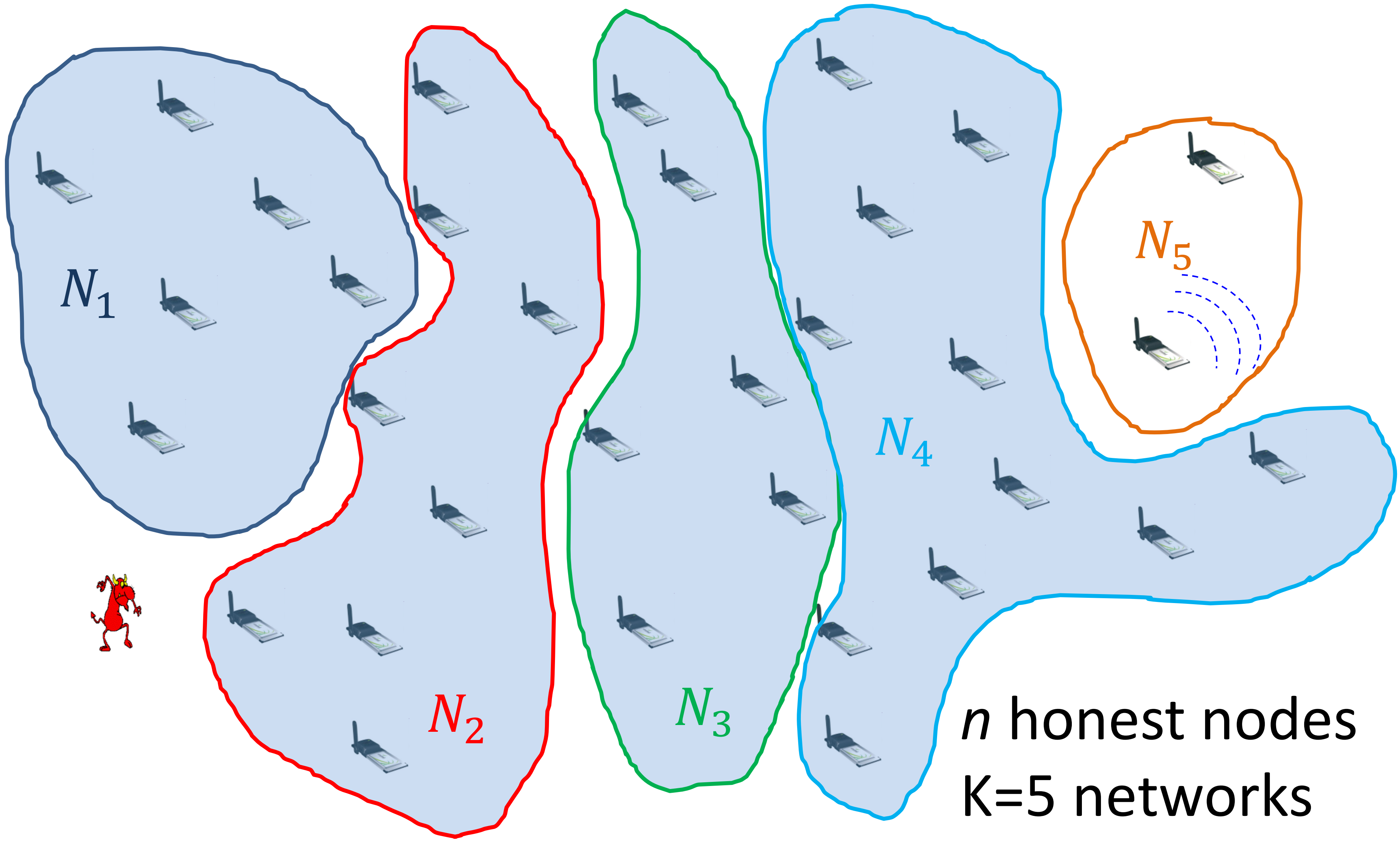
n honest nodes
K=5 networks
Single-hop

Idle Channel



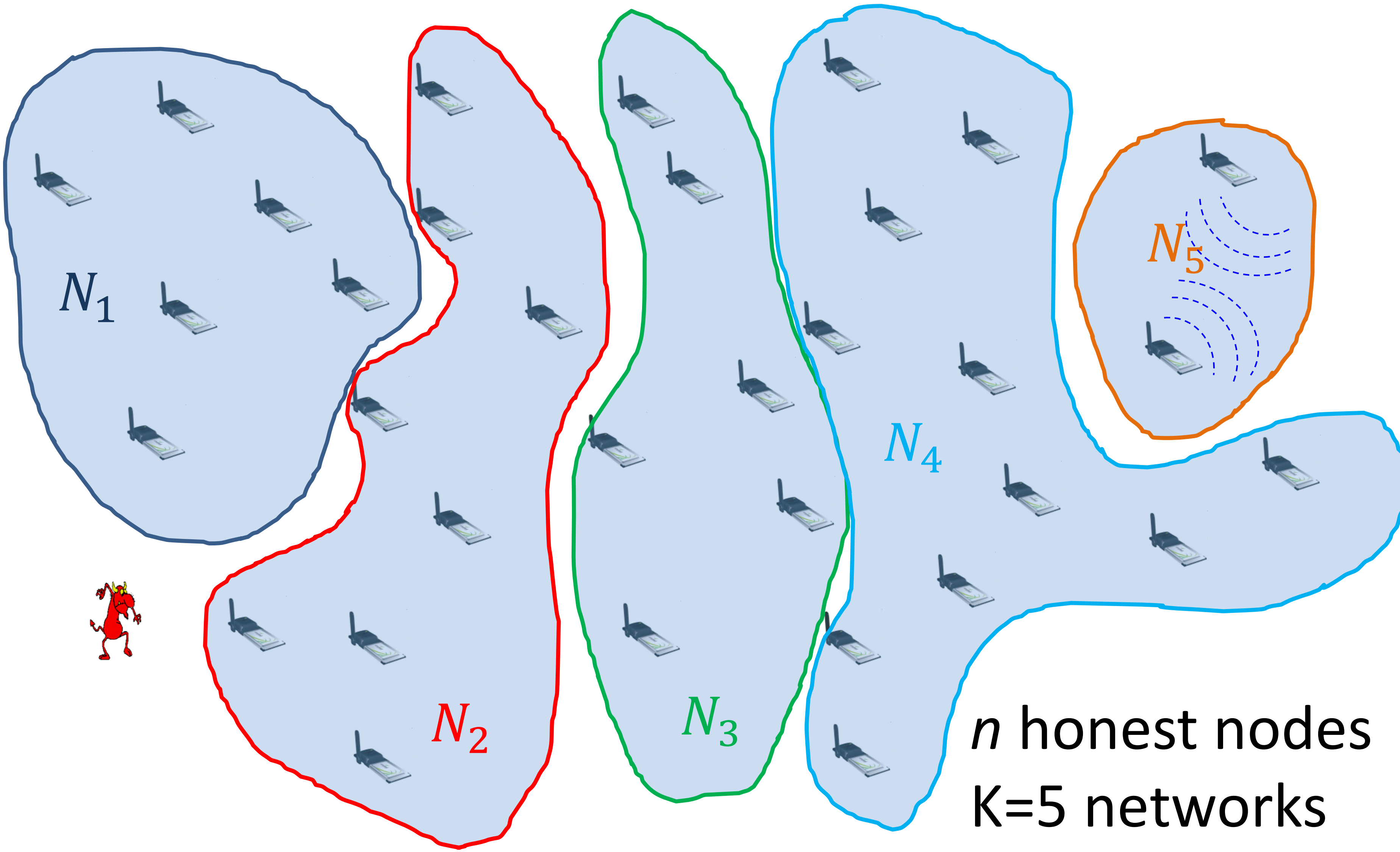
n honest nodes
K=5 networks
Single-hop

Successful Transmission in N_5



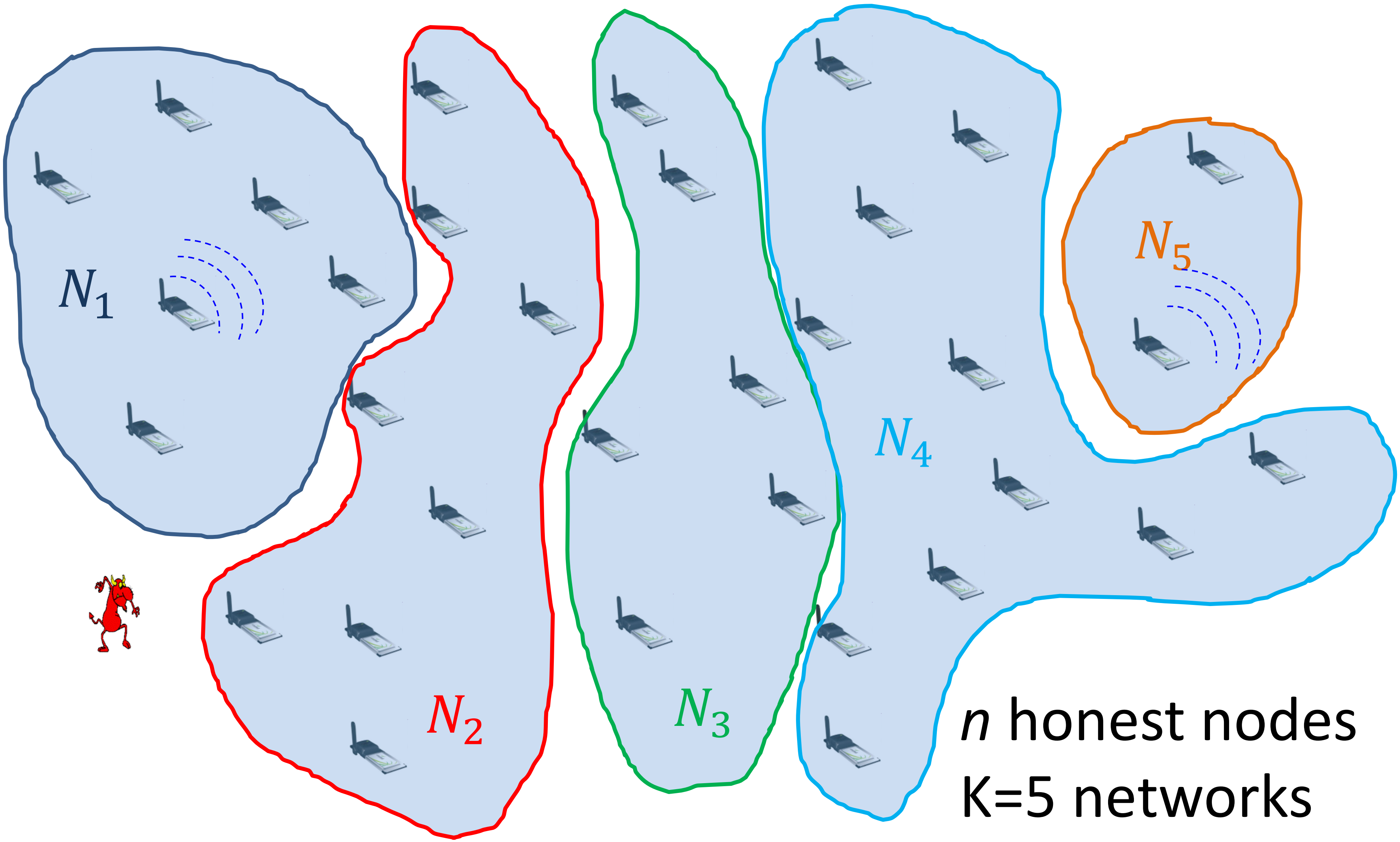
n honest nodes
K=5 networks
Single-hop

Busy Channel: Concurrent Transmissions



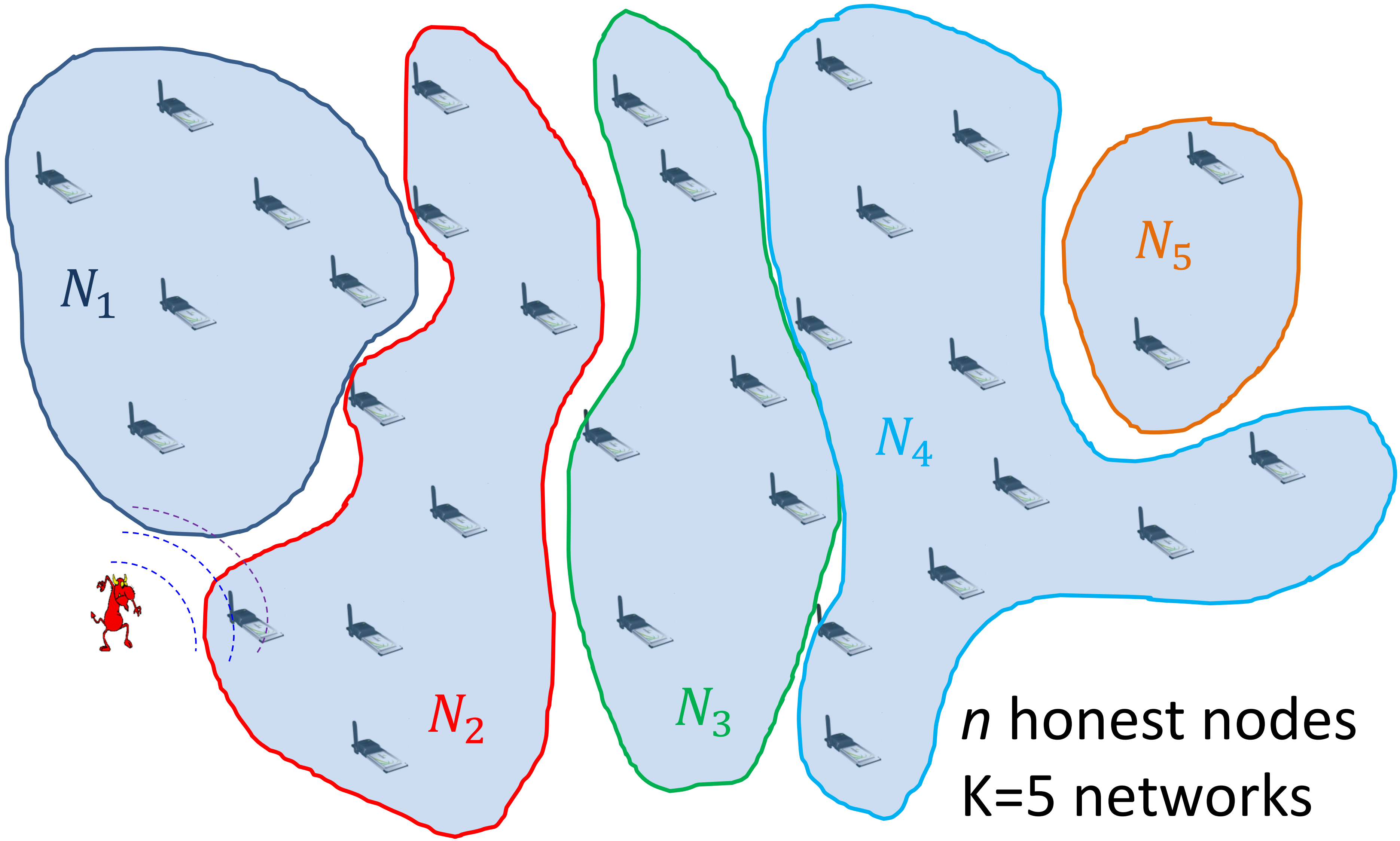
n honest nodes
K=5 networks
Single-hop

Busy Channel: Concurrent Transmissions



n honest nodes
K=5 networks
Single-hop

Busy Channel: Jamming

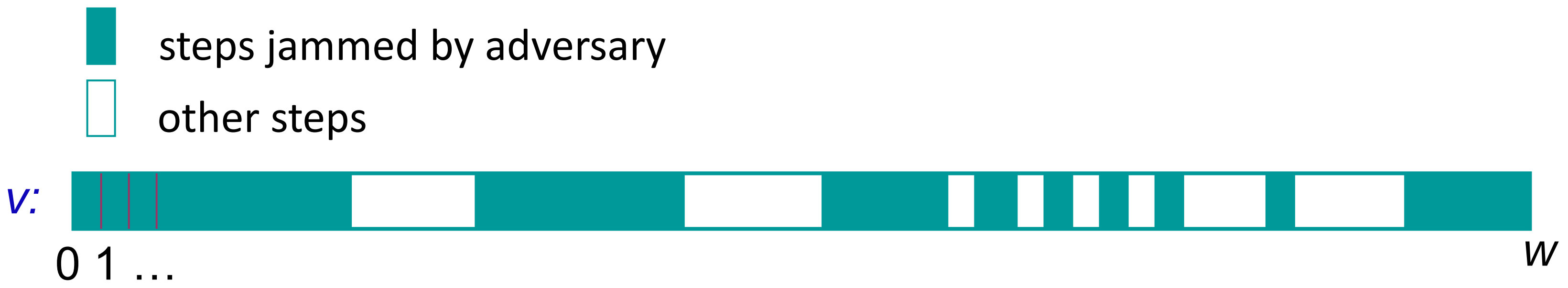


n honest nodes
K=5 networks
Single-hop

Adaptive adversary

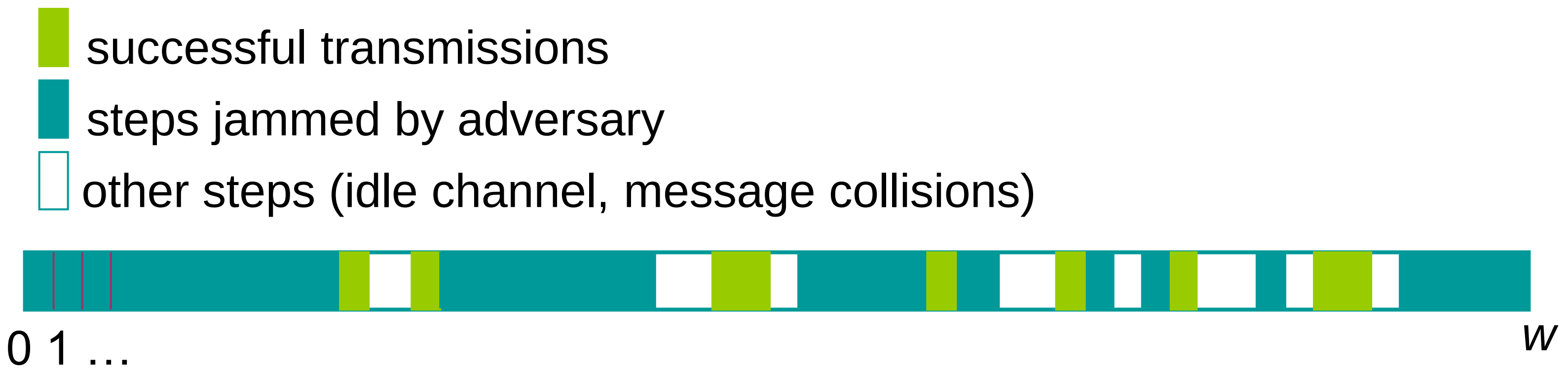
- knows *protocol and entire history*

- (T,1-ε)-bounded adversary: For every node v and every time window of size $w \geq T$, v experiences *$\leq (1-\varepsilon)w$ jammed time steps*, for some constants T and $0 < \varepsilon < 1$



Constant-competitive protocol

- a protocol is called *constant-competitive* against a (T,1-ε)-bounded adversary if the nodes manage to perform *successful* transmissions 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 contribution

- symmetric local-control MAC protocol, CoMAC, that is *constant-competitive* and *fair* against any $(T,1-\varepsilon)$-bounded adaptive adversary after $\tilde{\Omega}(T/\varepsilon)$ steps w.h.p., for any constant $0<\varepsilon<1$ and any T.

(The adversary considered here is adaptive but non-reactive.)

Related Work

Medium Access in Co-existing Networks:

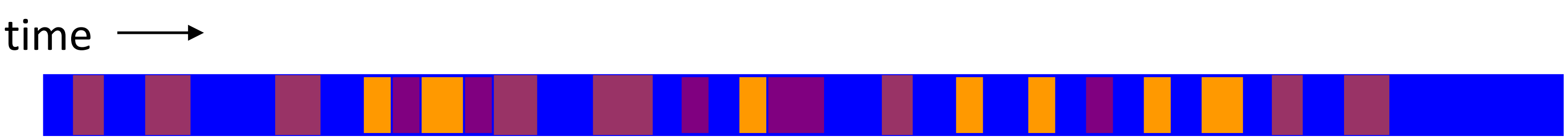
- Interference cancellation [Santoso, Tang, Vucetic, Jamalipour, Li, SICCS 2006]
- White spaces [Nychis, Chandra, Moscibroda, Tashev, Steenkiste, CoNEXT 2011]
  - No formal throughput nor fairness guarantees

Jamming model:

- [Awerbuch, R, Scheideler, PODC 2008]
- [R, Scheideler, Schmid, Zhang, DISC 2010, ICDCS 2011, MOBIHOC 2011]
  - Single network scenario

Basic approach: single network

- [ARS, PODC'08]
- a node *v* adapts its *probability of transmission* p_v based only on steps when an *idle channel (multiplicative increase)* or a *successful transmission (multiplicative decrease)* are observed



idle steps

successful transmissions

steps jammed by adversary

steps where collision occurred but no jamming

Basic approach: single network

- [ARS, PODC'08]
- a node *v* adapts its *probability of transmission* p_v based only on steps when an *idle channel (multiplicative increase)* or a *successful transmission (multiplicative decrease)* are observed
- Goal: achieve *constant cumulative probability* $p = \sum p_v$, which in turn implies *constant probability of successful transmission*

Why not previous jamming-resistant MAC protocols?

- Does not work in co-existing network settings
  - Individual networks aim to achieve constant cumulative probabilities, hence overall $p = \Theta(K)$.
  - Throughput degrades exponentially with the number of networks, i.e., $q_{success} \cong pe^{-p} = \Theta(K)e^{-\Theta(K)}$

- What is the problem?

  Since successful transmissions are viewed as busy channels by other networks, p_v is *not decreased often enough* to balance the increases due to idle time steps

Basic Idea for co-existing networks

- A *less aggressive* approach to increase p_v when idle.
  - p_v is increased at an idle time step with a probability q_v that is *inversely proportional* to the *time elapsed since last idle time step*
  - Hard to analyze
  - Solution: transform into a deterministic rule.

CoMAC Protocol

- each node v maintains
  - p_v : transmission probability
  - L_v : the *time elapsed since last idle time step*
  - q_v : used to determine *whether to increase p_v in an idle step*
  - T_v : time window estimate
  - c_v : counter
  - $\gamma = O(1/(\log T + \log\log n))$
- Initially, $T_v = c_v = 1$, $q_v = 0$, $L_v = +\infty$ and $p_v = p_{max}$ (< 1).
- synchronized time steps (for ease of explanation)
- Nodes do not know n, K, ε or T

CoMAC 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

    $$p_v = \min\{(1+\gamma)p_v,\ p_{max}\},$$
    $$T_v = \max\{T_v - 1,\ 1\},$$

  - If v successfully receives a message along with the tuple $(p_{new}, c_{new}, T_{new})$, then $(p_v\ c_v, T_v) = (p_{new}/(1+\gamma),\ c_{new},\ T_{new})$
- $c_v = c_v + 1$. If $c_v > T_v$ then
  - $c_v = 1$
  - if v did not sense an idle channel in the past T_v steps then

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

CoMAC 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
    - **$q_v = q_v + 1/L_v$. If $q_v >= 1$, then**

      $p_v = \min\{(1+\gamma)p_v, p_{max}\}$,

      $T_v = \max\{T_v - 1, 1\}$,

      $q_v = q_v - 1$, and update L_v (time since last idle step)
  - If v successfully receives a message along with the tuple $(p_{new}, c_{new}, T_{new})$, then $(p_v\ c_v, T_v) = (p_{new}/(1+\gamma), c_{new}, T_{new})$
- $c_v = c_v + 1$. If $c_v > T_v$ then
  - $c_v = 1$
  - if v did not sense an idle channel in the past T_v steps then

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

Our results

- Let $N = \max\{T, n\}$

- Theorem. For any $(T, 1-\varepsilon)$-bounded adaptive adversary, if executed for $\Omega(\log N \cdot \max\{T, \log^3 N/(\varepsilon \gamma^2)\}/\varepsilon)$ many time steps, CoMAC achieves, w.h.p.
  - Throughput: A constant-competitive throughput of $\Omega(\varepsilon^2 \min\{\varepsilon, 1/poly(K)\})$
  - Fairness: The difference between the minimum and the maximum cumulative probabilities of the individual co-existing networks is $O(K^2)$.

Proof sketch: Competitive Throughput

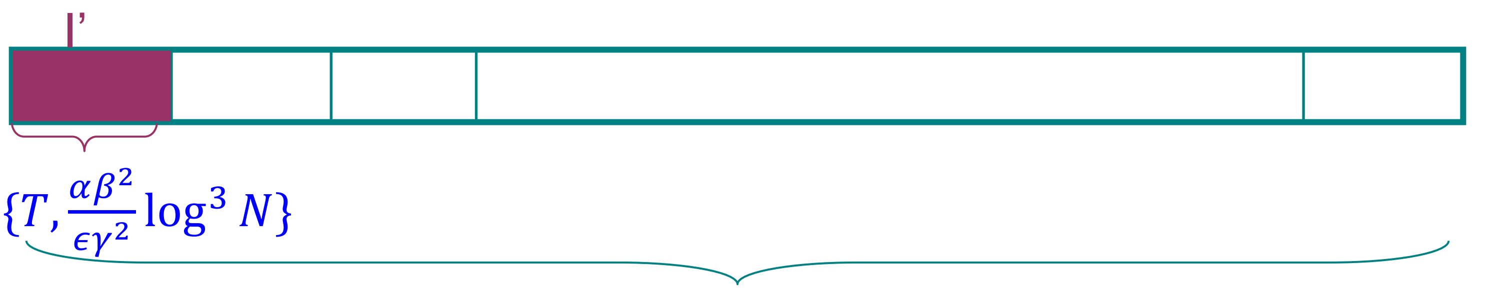
- We study the competitiveness of the protocol for

  $F = \Omega(\frac{1}{\epsilon} \log N \, max\{T, \frac{1}{\epsilon\gamma^2} \log^3 N\})$ many steps

  ↓

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

- Use induction over sufficiently large time frames:



$f = max\{T, \frac{\alpha\beta^2}{\epsilon\gamma^2} \log^3 N\}$

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

Proof sketch: Competitive Throughput

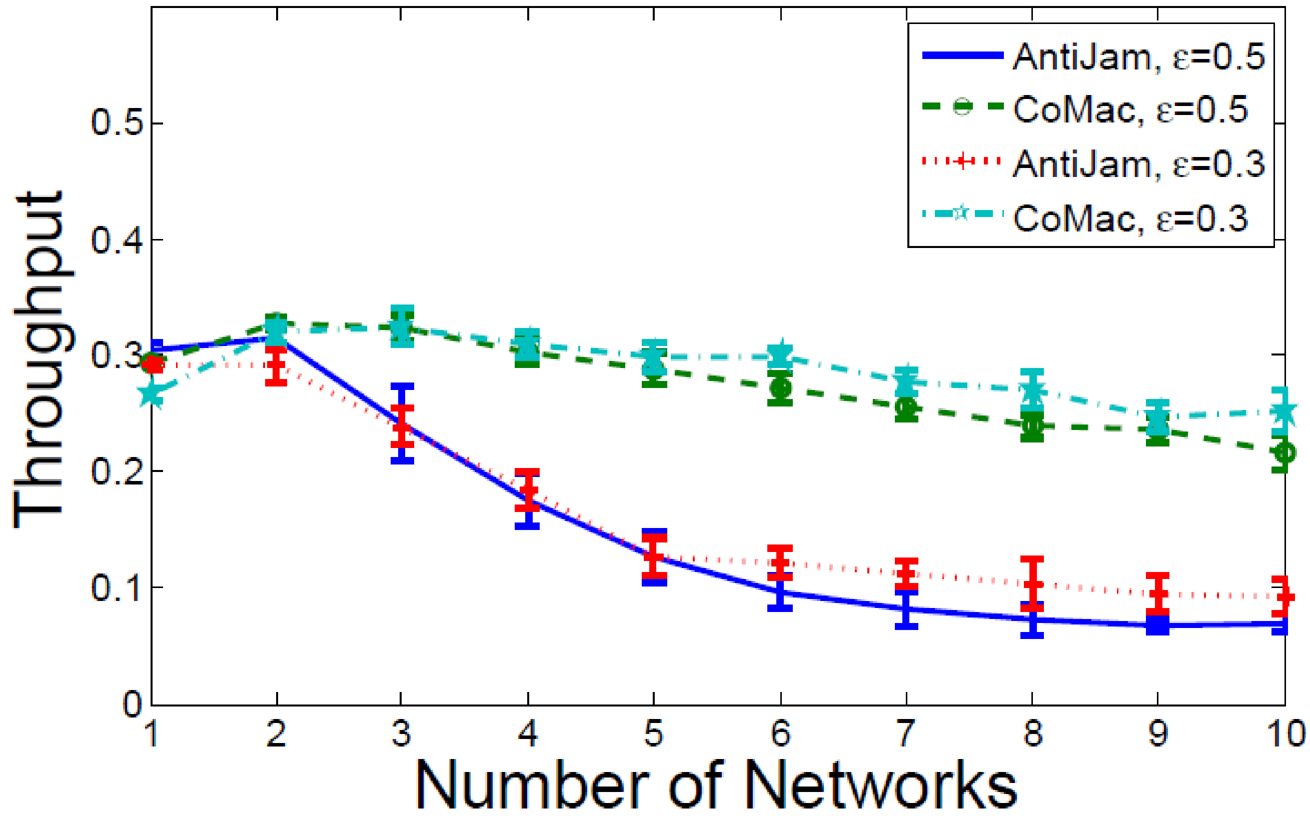
- $p \in [\frac{\epsilon\hat{p}}{4}, 36 \ln K]$ with moderate probability for at least a constant fraction of subframe I'
- $p \in [\frac{\epsilon\hat{p}}{4}, 36 \ln K]$ w.h.p., for at least a constant fraction of I (I contains logarithmic number of I')
- Hence, CoMAC achieves a competitive throughput of $\Omega(\epsilon^2 \min\{\epsilon, 1/poly(K)\})$ w.h.p., for any (T,1-ε)-bounded *adaptive* adversary.

Proof sketch: Fairness

- Potential Function: $\Phi = \sum_i |x_i - x_{min}|$
  - where $x_i = log_{1+\gamma} P_i$, and $x_{min} = \min_{\mathrm{i}} x_i$
  - P_i is the cumulative probability of network N_i
  - Only successful transmissions change the value of Φ
  - It takes at most $F = \Omega(\frac{1}{\epsilon} \log N \, max\{T, \frac{1}{\epsilon\gamma^2} \log^3 N\})$ many steps w.h.p. until the difference between minimum and maximum cumulative probability of a network is at most $\mathrm{O}(K^2)$

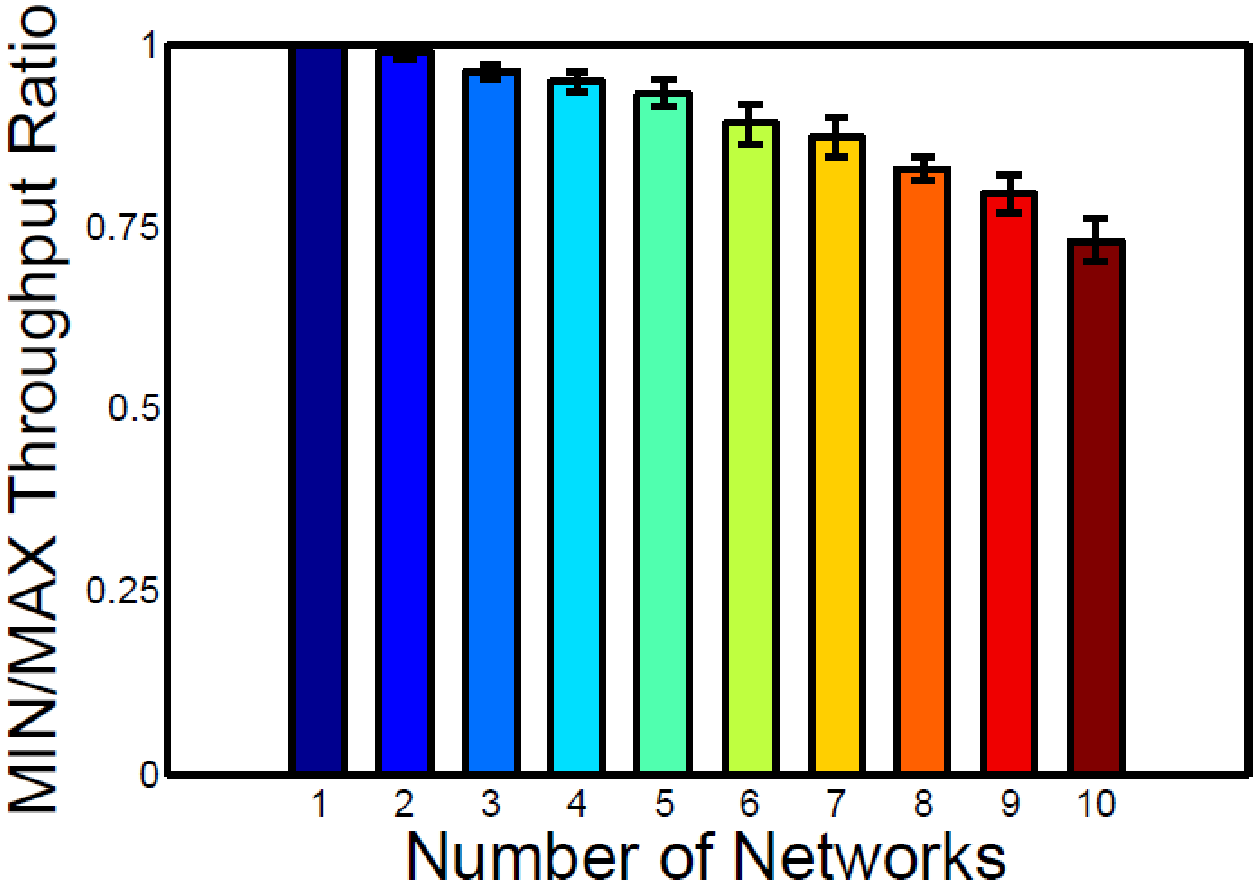
Simulations: CoMAC

Experiment 1: competitive throughput, compared to ANTIJAM



Simulations: CoMAC

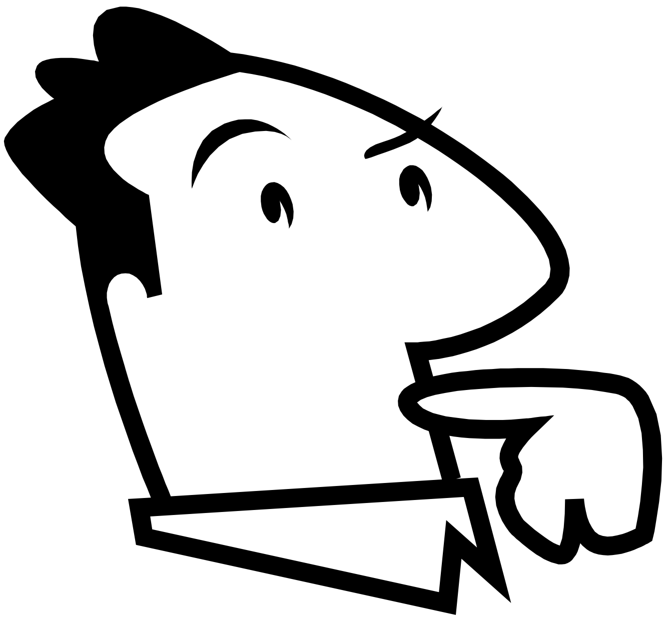
Experiment 2: fairness



Future Work

- Can we have a MAC protocol in the presence of co-existing networks that is provably robust against an adaptive (and reactive) adversary under
  - SINR model?
  - Multihop networks?

- Can the protocol be modified so that no bound on loglog n and log$T$ are required?



Questions?

Related Work

Defenses against jamming:

- spread spectrum (FHSS & DSSS):
  - Our approach is orthogonal to broad spectrum techniques, and can be used in conjunction with those.
- random backoff:
  - adaptive adversary too powerful for MAC protocols based on random backoff or tournaments (including the standard MAC protocol of 802.11 [Bayraktaroglu, King, Liu, ... INFOCOM 2008])

Preliminaries

- 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

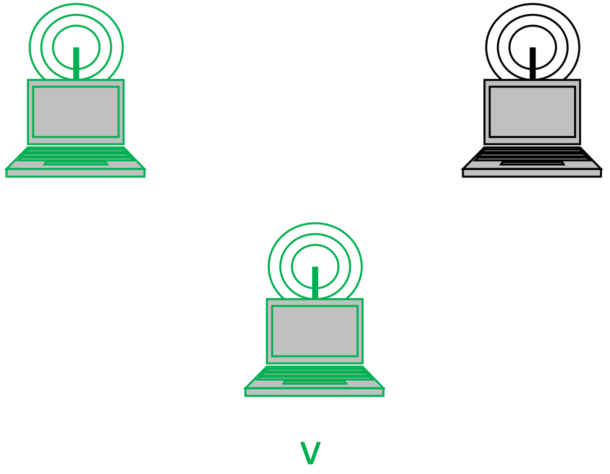
In each step:

- 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 past T_v steps then $p_v = p_v/(1+\gamma)$ and $T_v = T_v + 2$

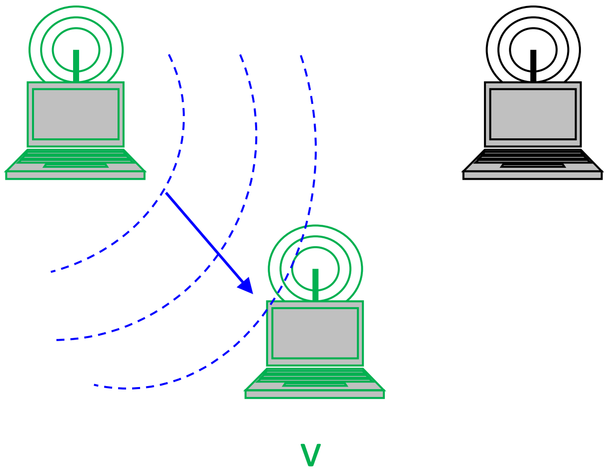
Wireless communication model

- when sensing the channel a node *v* may
  - sense an idle channel



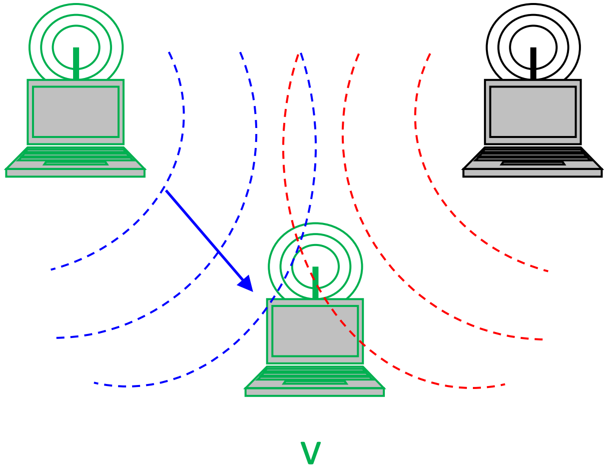
Wireless communication model

- when sensing the channel a node *v* may
  - – sense an idle channel
  - – receive a packet
    - Exactly one node in *v* ‘s network transmits



Wireless communication model

- when sensing the channel a node *v* may
  - sense an idle channel
  - receive a packet
  - sense a busy channel
    - When more than one node transmit, or a node outside *v*'s network transmits



Simple (yet powerful) idea

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

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

$\therefore$

if (number of times the channel is idle) $\tilde{=}$ (number of successful transmissions) → $p = \theta(1)$ → $q_{succ} = \theta(1)$!
(what we want!)