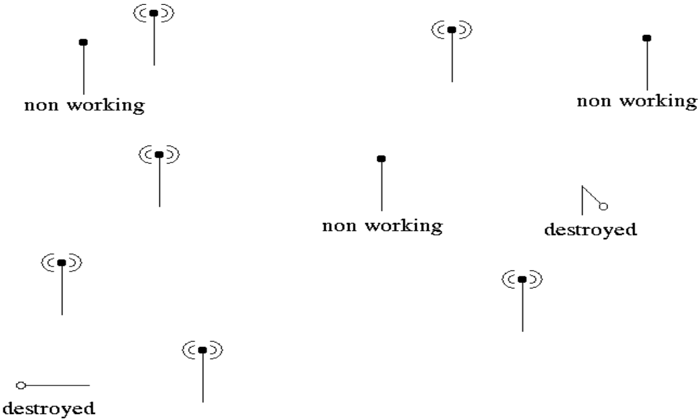
Adversary Immune Size Approximation of Single-Hop Radio Networks

Jędrzej Kabarowski, Mirek Kutyłowski, Wojtek Rutkowski

Institute of Mathematics and Computer Science,
Wrocław University of Technology

TAMC'2006
Beijing

Single-Hop Radio Network



A network consists of a number of stations communicating via a radio channel.

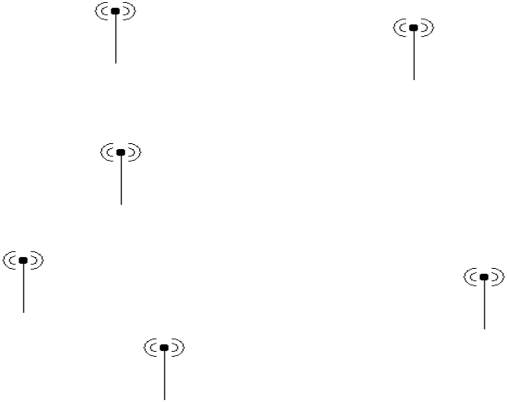
Single-hop Network

- possible status of a station:

dead	
inactive	its transmitter and receiver are switched off, internal work only
active	sending xor monitoring the channel *(not necessarily getting a message)*

- number of stations, status of a station – unpredictable

Single-hop Radio Network



State of a network from an algorithmic point of view.

Single-hop Network

- communication via a **shared broadcast channel**
- a signal from a station can reach everybody -**single-hop**
- one cannot simultaneously transmit and listen

Single-hop Network

- communication via a **shared broadcast channel**
- a signal from a station can reach everybody -**single-hop**
- one cannot simultaneously transmit and listen
- if two stations send then **collision** - no message comes through
- common clock, **synchronous** communication, discrete time steps

Ad hoc nature of the network

- no central control,
- initially - a station knows only about itself, no knowledge on existance of other stations,
- the stations may have some preloaded shared knowledge (secret keys ...)

Motivations

often said:

- no central control, so resistant against failures and attacks
- dynamically adopting

but the truth is:

we are used to work with algorithms for:

- low dynamic systems
- reliable communication
- not many “bad guys” in the system
- unproblematic initialization

here the situation is completely different

Self-organization of a Network

Start situation::

- each station knows only about itself and the algorithm executed

Goal:

- build a logical infrastructure so that we can run algorithms on this basis.

It is like "booting" ad hoc networks.

Size Approximation

One of the very basic problems to solve:

find a number N such that

$$n/c \leq N \leq c \cdot n$$

where n is the (unknown) number of the stations

Performance Measures

time - the number of time slots used by the algorithm

Performance Measures

time - the number of time slots used by the algorithm

energy cost - the maximal k such that some station transmits/listens k times during algorithm execution

- communication consumes almost all energy used (processor and sensors usage - negligible)
- energy required for transmitting and listening of the same magnitude

Adversary Model

- random transmission errors,
- or burst errors,
- or even a malicious adversary knowing the algorithm

Adversary Model

- legitimate stations share a secret that is not known by the adversary
  $\Rightarrow$ keyed MAC can be used to prevent faking messages by an adversary
- an adversary may attempt to cause collisions so that the algorithm fails
- the adversary cannot use much higher communication resources than the other stations

Basic Algorithm

Suppose we have K stations.

A step:

- a station decides to transmit a message with probability p, then probability that exactly one station transmits equals

$$K \cdot p \cdot (1-p)^{K-1}$$

- the probability maximized for $p = 1/K$, the value achieved is $\approx 1/e$
- the probability ≈ 0, if p is not close to $1/K$.

Basic Algorithm

Steps executed:

- for probabilities

$$p = \ldots, 2^{-i}, 2^{-(i+1)}, 2^{-(i+2)}, \ldots$$

  until a single message sent
  (for each probability some number of trials takes place)
- then $1/p$ taken as an approximation of the number of stations

Basic Algorithm is Vulnerable

Attack
the adversary sends junk messages when probability p is close to $1/K$

then the algorithm will never terminate

Main Result

- energy cost – $O(\log\log N \cdot \sqrt{\log N})$
- time complexity – $O(\log^{2.5} N \cdot \log\log N)$
- outcome correct with probability $\geq 1 - 2^{-z}$ where $z = \Omega(\sqrt{\log N})$ for an adversary with energy cost $O(\log N)$
- the same (correct) answer known to all stations except $o(N/2^{\sqrt{\log N}})$ of them.

Main Result

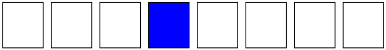
- energy cost – $O(\log\log N \cdot \sqrt{\log N})$
- time complexity – $O(\log^{2.5} N \cdot \log\log N)$
- outcome correct with probability $\geq 1 - 2^{-z}$ where $z = \Omega(\sqrt{\log N})$ for an adversary with energy cost $O(\log N)$
- the same (correct) answer known to all stations except $o(N/2^{\sqrt{\log N}})$ of them.

Best fragile algorithm (Jurdziński, K., Zatopiański, COCOON'2002): runtime $O(\log^{2+\varepsilon} n)$, energy cost $O((\log\log n)^{\varepsilon})$ for any $\varepsilon > 0$

Tricks: Time Window

- within a group of k time slots only one really used by the algorithm
- which slot is used depends on a secret unknown to the adversary

- For an adversary it is difficult to make a collision at the right moment!
- but waste of communication time



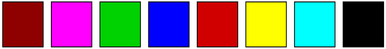
Interleaving Time Windows

A technique used when groups of stations perform independent computations in parallel:

- a time window of length k used simultaneously by k groups
- for communication in window t, group i uses slot

$$f(\text{secret}, t; i)$$

$f(\text{secret}, t; -)$ - a cryptographic pseudorandom permutation



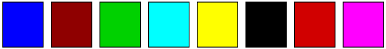
Interleaving Time Windows

A technique used when groups of stations perform independent computations in parallel:

- a time window of length k used simultaneously by k groups
- for communication in window t, group i uses slot

$$f(\mathrm{secret}, t; i)$$

$f(\mathrm{secret}, t; -)$ - a cryptographic pseudorandom permutation



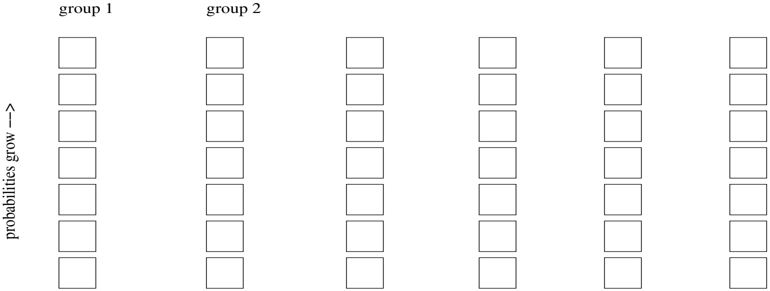
Advantages:

- each time slot used
- behaviour from a point of view of a group – the same as for time windows
- an adversary cannot attack a single group – the attack goes against all groups with less collisions for each group

Algorithm Idea

General strategy:

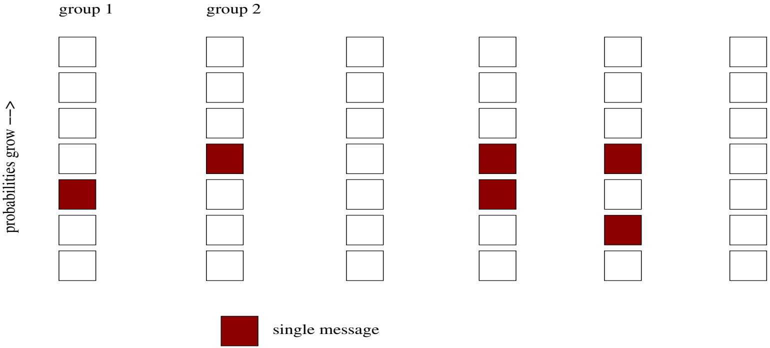
- perform the basic algorithm in many groups independently
- in a group try different probabilities
- the number of groups is too large to allow an adversary disturb all of them



Algorithm Idea -

Sucesses:

- single transmissions for about the same probabilities
- take some median
- one cannot listen all the time due to energy cost

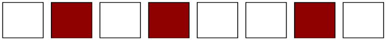


Algorithm Idea

Experiment for a single group and a single probability:

- 8 trials
- success if a message exactly 3 times came through

success in a single experiment



Algorithm Idea

Dissemination of information:

- gossiping
- even if two stations do not have the same view, it is likely that the median probability is the same

Thanks for your attention