Repelling Sybil-type attacks in wireless ad hoc systems

Marek Klonowski
Michał Koza Mirosław Kutyłowski

Institute of Mathematics and Computer Science,
Wrocław University of Technology

ACISP 2010, Sydney

Outline

Outline

Network Model

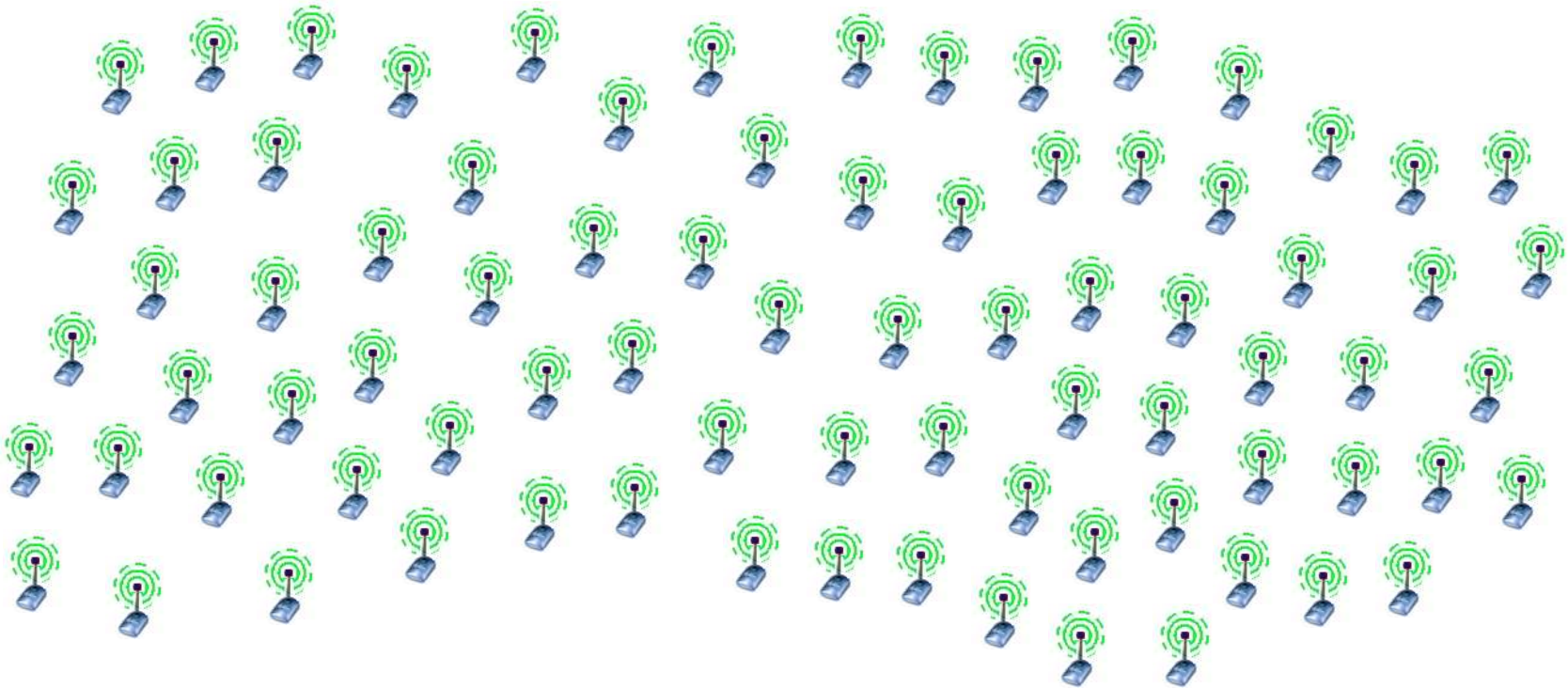
Network Model

- Wireless communication
- Single hop network
- Single communication channel
- Time divided into slots
- Synchronous clocks of all nodes
- Collision detection (single, silence, noise)
- A station cannot transmit and listen at the same time slot

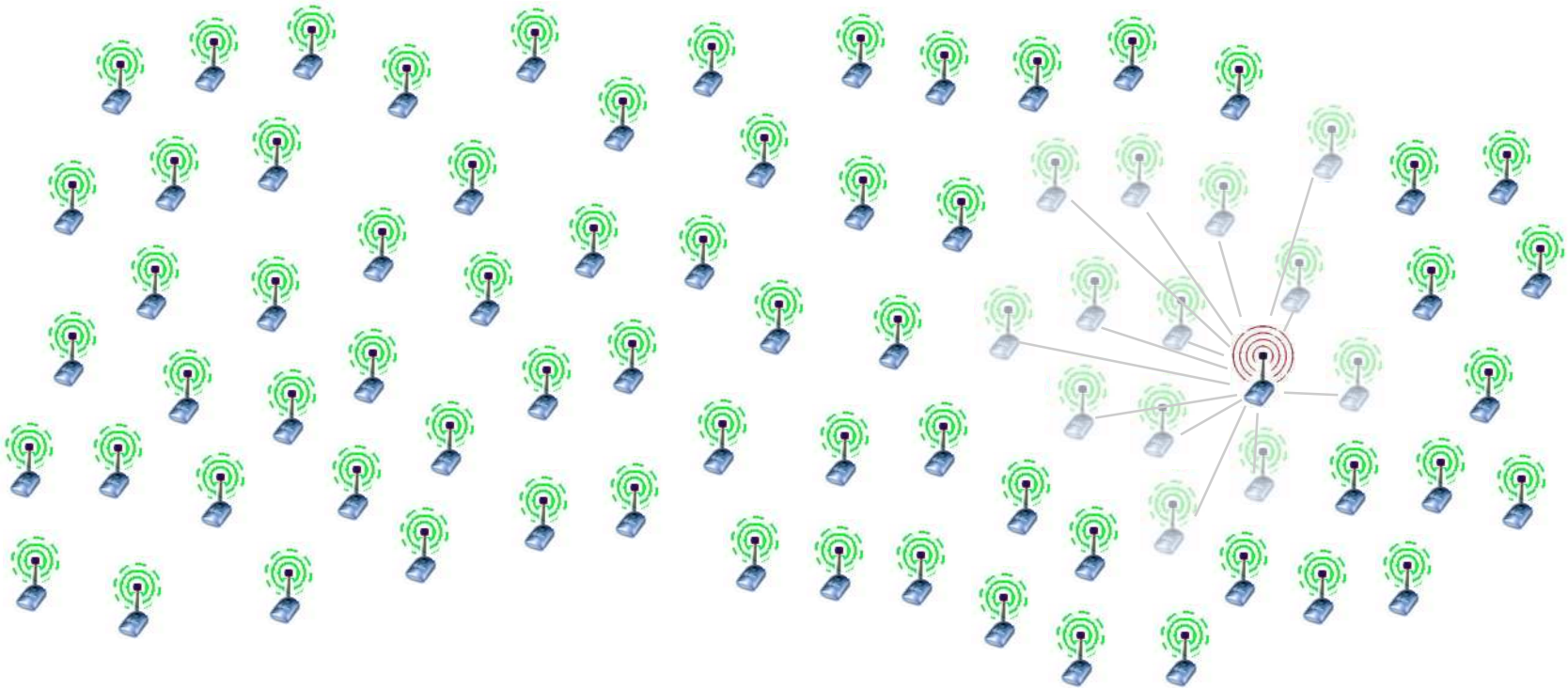
Outline

Network

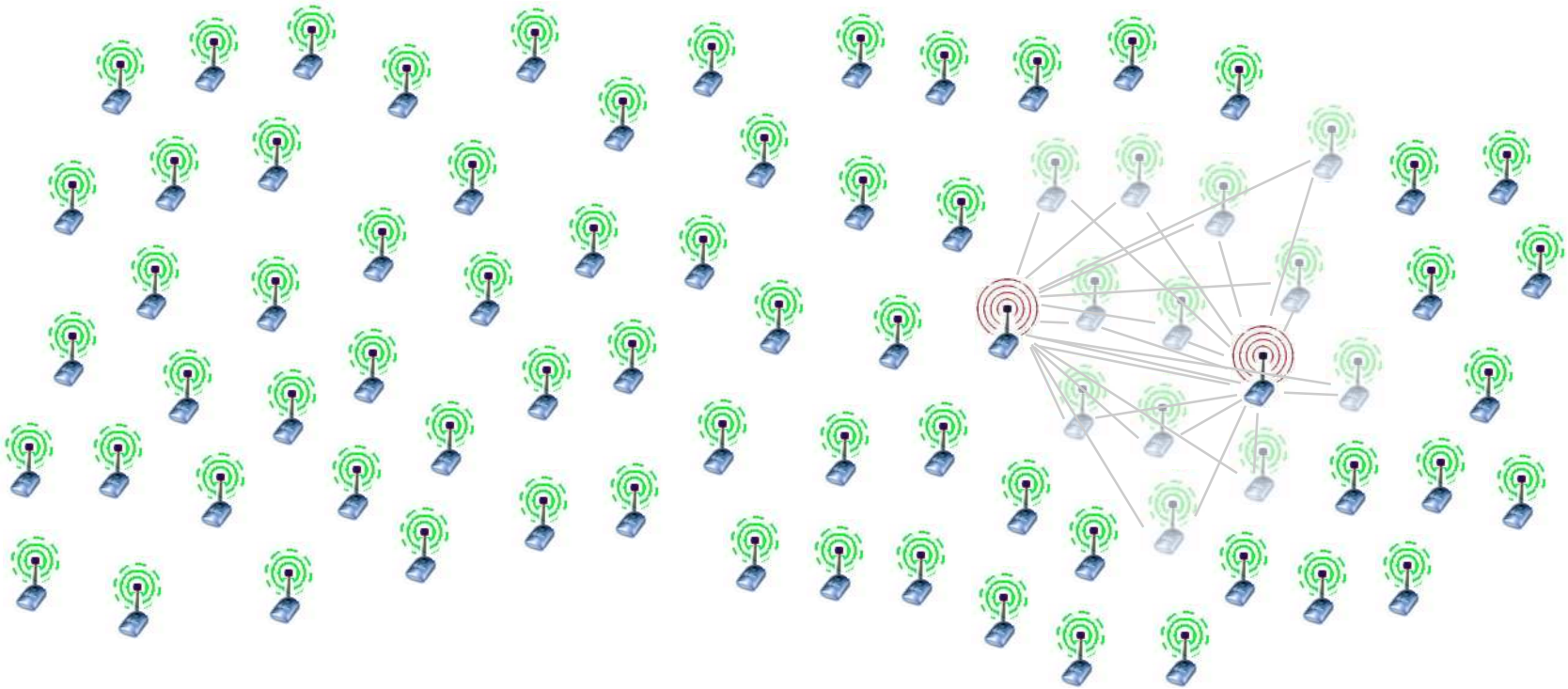
Network



Network with an adversary



Network with two adversaries



Outline

Goal

Initialization process

when initialization is completed, we get the following situation:

- each station has its ID registered
- no station has more than one ID registered

a basic procedure for self-organization of wireless ad hoc networks

Outline

Adversary Model

A malicious adversary:

- can capture some stations
- can have some preloaded strategy
- but cannot communicate outside the shared channel
- intends to emulate more stations to increase its chances in symmetric leader election and initialization protocols
- does not intend to block the network (and itself)

Outline

Assumptions

Two parameters

- N_{min} - the minimal number of honest stations in the network
- N_{max} - the maximal number of stations in the network (both adversarial and honest)

Computational power

Parameter a denotes that a station knowing $H(x)$ and not knowing a bits of x cannot guess x by a brute force attack with high probability.

Outline

Algorithm

ID's listing

All stations are supposed to declare their ID numbers. Adversarial stations can declare multiple identities. Phase lasts as long as there is no more station willing to declare its ID.
n - number of registered ID's

Verification phase

Verification whether there are no ID's being emulated by the same station (physical device).

Verification Phase

Verification Phase consists of $2n - 1$ trials, each dedicated to one identity.

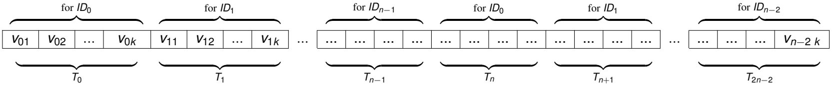
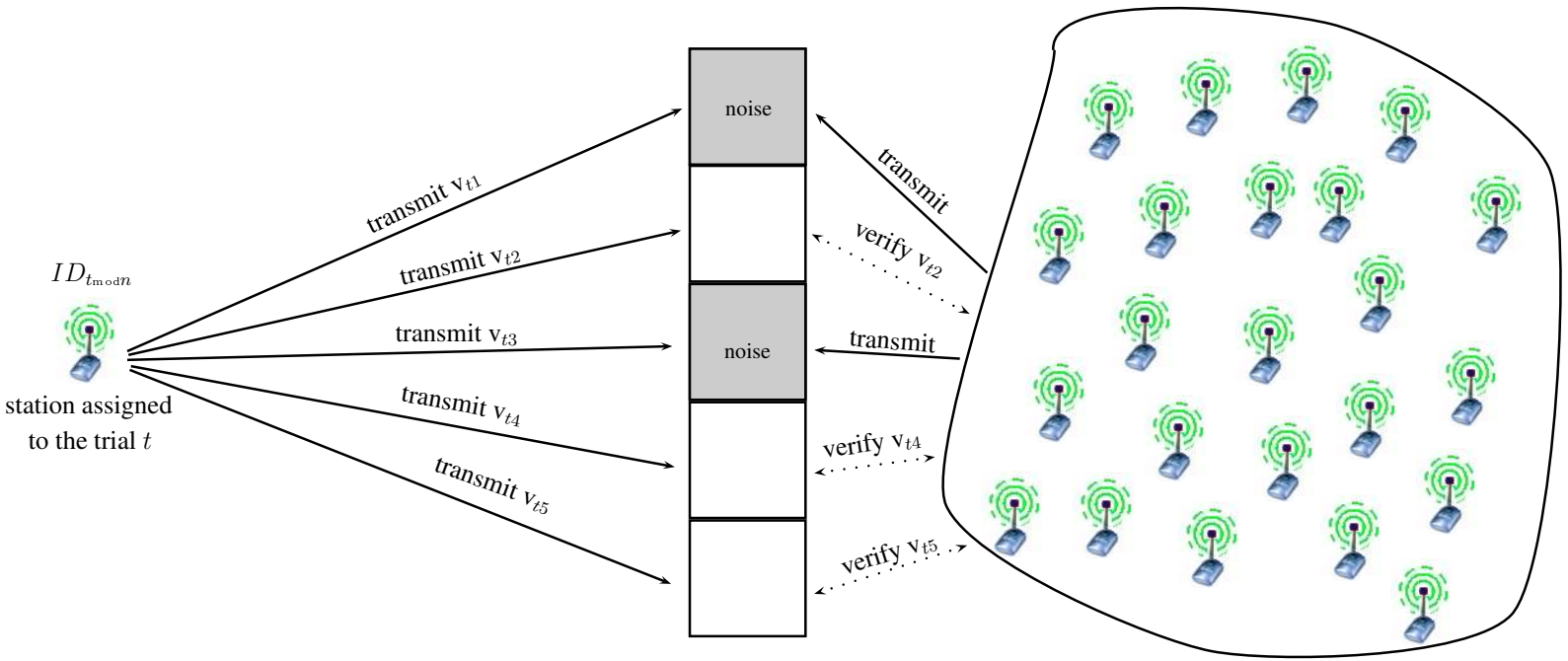


Figure: Trials assignment

Trial

Each trial consists of k slots.



Jamming pattern P_t: 10100

Verification message

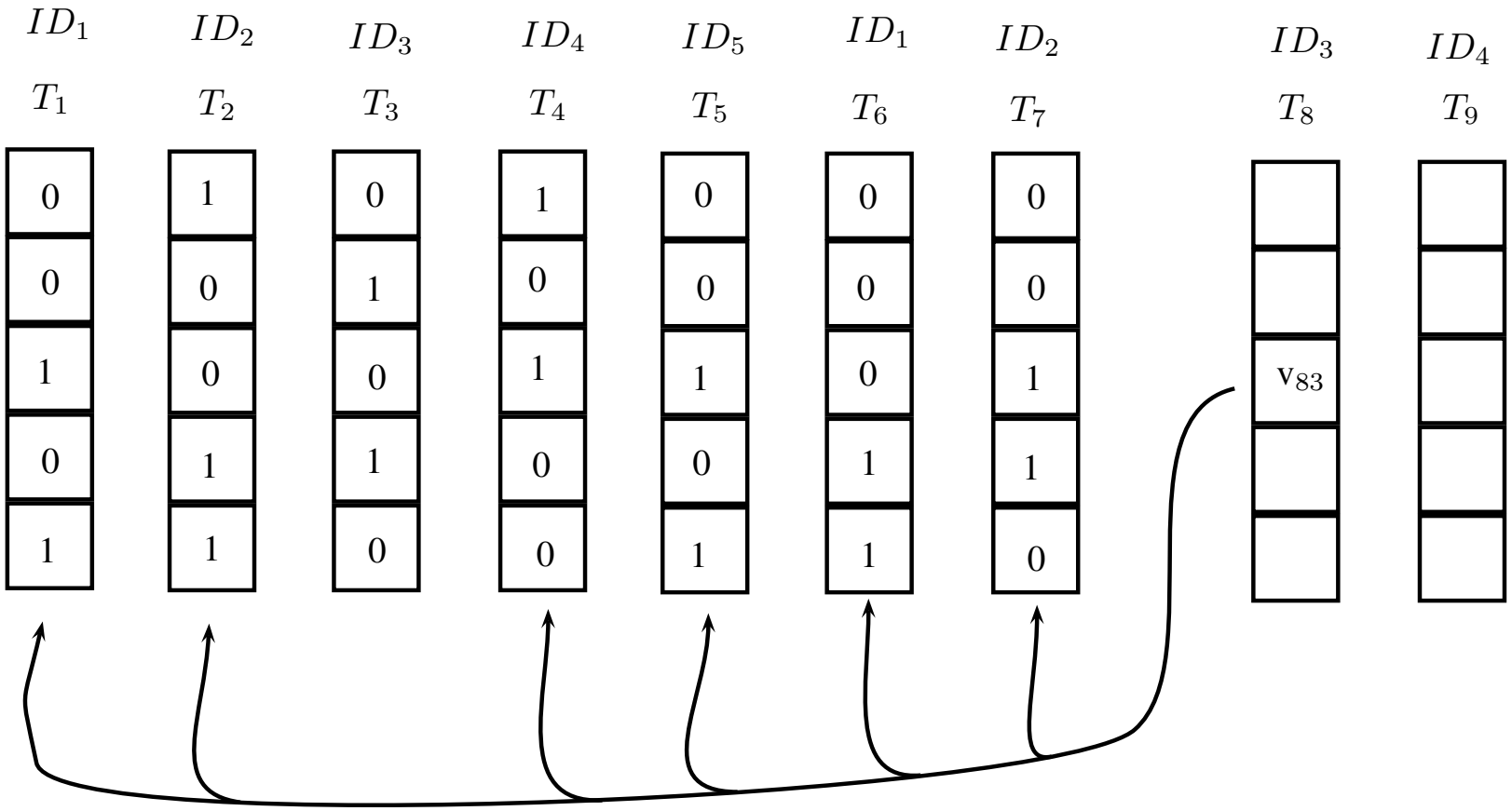
Function F

$F : \mathbb{N} \times \mathbb{N} \times (0,1)^k \mapsto \mathbb{N}$ (one-way)
$F_{ts}(P_i) = F(t, s, P_i)$

v_{ts}

$$v_{ts} = \begin{cases} 0 & \text{if } t = 0, \\ F_{ts}(P_0)||\ldots||F_{ts}(P_{t-1}) & \text{if } t < n, \\ F_{ts}(P_0)||\ldots||F_{ts}(P_{t-n-1})||F_{ts}(P_{t-n+1})||\ldots||F_{ts}(P_{t-1}) & \text{if } t \geq n. \end{cases} \quad (1)$$

Required jamming patterns



required jamming patterns

Result

Trial size

$$k > 2^{m/n} \cdot M \cdot a \cdot \log n \left(\frac{1}{\log n} + \frac{2}{Ma} + 2\sqrt{\frac{1}{(Ma)^2} + \frac{1}{Ma \log n}} \right)$$

Where:

- n - the number of declared ID's
- m - the number of ID's declared by adversary
- M - the number of adversarial devices
- a - the computational bound

Adversary risk

We show that it is optimal for the adversary to act according to protocol and:

- the probability of successful cheating is $\leq \frac{1}{n^2}$,
- cheating failures are punished.

Thank You!

Contact information:

- Marek.Klonowski@pwr.wroc.pl, Michal.Koza@pwr.wroc.pl, Miroslaw.Kutylowski@pwr.wroc.pl,
- +48 71 3202109, fax: +48 71 320 2105
- Wrocław University of Technology, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland