Optimizing Radio Channel Access

Mirosław Kutyłowski
Wrocław University of Technology

joint work with J. Cichoń, M. Zawada and the DATAX team

NeST, Liverpool, 26.6.2014

Talk agenda

1. wireless communication challenges
2. access to radio channel
3. algorithms
4. malicious stations

Wireless Communication Challenges

Common Beliefs

Myths

1. **communication bandwidth is unlimited**
   wrong! a limited range of frequencies, a limited amount of modulation possibilities
2. **the number of channels = the number of frequencies**
   wrong! trade-off between width of the frequency channel and capacity,
3. **low energy usage**
   wrong! wireless telecommunication is using huge amount of energy
4. **unlimited reachability**
   wrong! many problems due to signal propagation peculiarities, irregular signal attenuation, multipath propagation, ...

Energy

1. communication range depends on P_0 – the signal strength at the sender,

   $P_\Delta \approx P_0^{-d\cdot\Delta}$, while P_Δ should be above the noise level
2. strong signal ⇒ interference between different communication links

Solutions

1. use minimal energy level ⇒ less interference, less electromagnetic smog!
2. divide the network into small cells

Mobility

Challenges due to mobility

1. unpredictable who belongs to the network
2. unpredictable communication needs
3. dynamically changing network state
4. physical problems

   (e.g. limitations on frequencies used for communication with moving stations

Access to the Radio Channel

Problem

Shared communication channel

- many stations may need to transmit at the same time
- if two stations transmit at the same time then a collision occurs – transmission failed

Problem

how to organize leader election so that:

- the ratio between the transmission time and the global time is as close to 1 as possible
- i.e. minimize the time where:
  - channel silent
  - collision
  - messages devoted solely to leader election

Network dynamics

Highly dynamic networks

during the data transmission of the leader the other requests change
⇒ it does not make sense to find all nodes aiming to transmit

Static networks

the requests change slowly
⇒ collect the requests once and then transmit one by one

Technical conditions

Carrier detection

1. transmission of a single bits takes many periods of the carrier wave
2. carrier detection much faster than receiving any encoded message

Synchronization

1. delays to receive the signal non-negligible
2. no full synchronization possible

Time slots

1. execution time divided into time slots
2. necessary guard times between slots to compensate for (limited) asynchrony

Carrier Sensing Multiple Access

Steps of the protocol

Executed in a loop:

```
  if  there is a carrier signal, then stay idle time $\sigma$
else  start own transmission
```

Idea

somebody will be the first to try after the transmission end

Carrier Sensing Multiple Access

Steps of the protocol

in time interval $[0, T]$. Steps executed by a station:

1. choose $\eta < T$ at random
2. at time η sense the carrier

```
if    there is a carrier signal, then stay idle
else  send the carrier signal for the time [η, T].
```

Idea

the station that has chosen the smallest η is the winner

Problems

Delays

1. time between detecting the clear channel and starting to send the carrier signal
2. time between start of sending the carrier signal and receiving the signal by other station

Consequences

1. station *A* detects clear channel at time t_0
2. station *B* detects clear channel at time $t_1 = t_0 + \epsilon$
3. station *A* starts sending the carrier signal at time $t_0 + \lambda$ $(\lambda > \epsilon)$
4. station *A* starts sending the carrier signal at time $t_1 + \lambda$

Both *A* and *B* think they are the winners.

Error probability

Condition

- $\eta_1, \ldots, \eta_n$ time chosen by the stations A_1, ... A_n
- $\eta_{1:n}, \ldots, \eta_{n:n}$ - the same numbers after sorting
- error free if

$$\eta_{2:n} - \eta_{1:n} > \lambda$$

Probability

Let $T = 1$. If time moments are chosen according to the distribution f with a cumulative density function F, then

$$\Pr\left[\eta_{2:n} - \eta_{1:n} > \lambda\right] = n \int_0^{1-\lambda} f(x)(1 - F(x+\lambda))^{n-1} dx$$

Design choices

Uniform distribution ($f = 1$), T arbitrary

$$\Pr(X_{2:n} - X_{1:n} > \lambda) = (1 - \lambda/T)^n \quad .$$

Extending T:

- reduces error probability,
- increases transmission delay.

Unknowns

we do not know n, it could be anything between 0 and some reasonable upper bound

Design choices

Is the uniform distribution the right choice?

no!

1. better probabilities for $F(x) = x^{\alpha}$
2. even better for

$$F(x) = (e^{\alpha x^{\beta}} - 1)(e^{\alpha} - 1)$$

Optimum not known.

Practical issues:

there are limitations on F:
find the optimal F under the condition that choosing according to distribution F is very easy (small code, small computation time)

Variants

Large number of stations

A station willing to compete for the access to the radio channel:

- with probability p attempts to get the access
- with probability $1 - p$ waits back-off time σ and restarts the procedure

All problems due to the static value of p.

Continuous or discrete?

What is better?

1. choose probing points at random from continuous time distribution
2. or divide the time into slots and then block the slots?

Option 1 would be clearly better for delay $\lambda = 0$. But $\lambda \gg 0$.

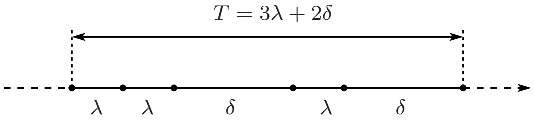
Slotted algorithms

Two slots

two independent slots where a station can compete for the channel:

- $T = 3\lambda + 2\delta$
- slot 1: carrier sent at time 0, transmission of length $\lambda + \delta$
- slot 2: is no carrier at time $[0, \lambda]$, start transmission at time λ, transmission of length $\lambda + \delta$,
- at time $2\lambda + \delta$ starting ACK of length δ

slot 1 chosen with pbb p, slot 2 chosen with pbb q



Two slotted

details

The probability of the success in one trial depends on parameters N (number of stations), p and q:

$$\Pr[\mathrm{Success}] = Np(1-p)^{N-1} + Nq(1-(p+q))^{N-1} \quad .$$

For $p = \frac{a}{N}$ and $q = \frac{b}{N}$,

$$\Pr[\mathrm{Success}] \approx f_2(a,b) \quad ,$$

where

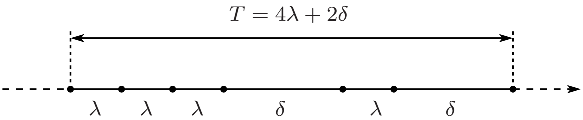
$$f_2(a,b) = ae^{-a} + be^{-(a+b)} \quad .$$

f_2 has a global maximum at point $(a,b) = (1-\frac{1}{e}, 1)$ and

$$f_2(1-\tfrac{1}{e}, 1) = e^{-1+\frac{1}{e}} \approx 0.531464 \quad .$$

Three slots

1. $T = 4\lambda + 2\delta$
2. p, q, r denote pbb of, respectively, starting to transmit at moment 0 λ, and 2λ.



The probability of the success depends on parameters N, p, q and r.

$$\Pr[\mathrm{Success}] = Np(1-p)^{N-1} + \\ Nq(1-(p+q))^{N-1} + Nr(1-(p+q+r))^{N-1} \quad .$$

For $p = \frac{a}{N}$, $q = \frac{b}{N}$ and $r = \frac{c}{N}$:

$$\Pr[\mathrm{Success}] \approx f_3(a,b,c) \quad ,$$

where $f_3(a,b,c) = ae^{-a} + be^{-(a+b)} + ce^{-(a+b+c)}$

The function f_3 has a maximum at the point

$$(a_0, b_0, c_0) = (1 - e^{-1+\frac{1}{e}}, 1 - \frac{1}{e}, 1)$$

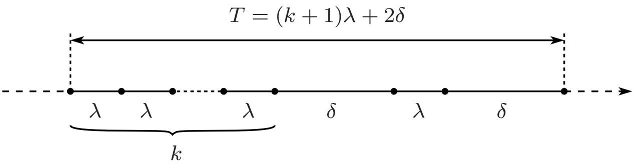
and

$$f_3(a_0, b_0, c_0) = e^{-1+e^{-1+\frac{1}{e}}} \approx 0.625918 \quad .$$

General case - k slots

for $i \leq k$: p_i is the probability of

- choosing by a station the transmission time $(i-1)\lambda$
- sending at this moment a message of length $(k-i)\cdot\lambda+\delta$ (if the channel was clear so far)



General case - k slots

details

Pbb of a successful transmission by a single station:

$$\Pr[\mathrm{Success}_{p_1,\ldots,p_k}] = \sum_{i=1}^{k} Np_i\,(1-(p_1+\ldots+p_i))^{N-1}$$

Let $p_i = a_i/N$ and

$$f_k(a_1,\ldots,a_k) = \sum_{i=1}^{k} a_i e^{-(a_1+\ldots+a_i)} \quad .$$

Then

$$\Pr[\mathrm{Success}_{a_1/N,\ldots,a_k/N}] \sim f_k(a_1,\ldots,a_k) \quad .$$

General case - k slots

details

Optimization

Let $(M_k)_{k\geq 1}$ be the sequence of reals defined by the following recurrence relation:

$$\begin{cases} M_1 & = & \frac{1}{e} \\ M_{k+1} & = & e^{-1+M_k} \quad \text{for } k \geq 1 \end{cases} \tag{1}$$

Theorem

The maximum value of the function f_k is M_k and the maximum occurs at the point $(b_k, \ldots, b_1)$ where

- $b_1 = 1$
- $b_a = 1 - M_{a-1}$ for $a = 2, \ldots, k$.

Comparison

Expected run-time to elect a leader for $N = 100$

Protocol	Expected run-time
1 slot	$5.464 \cdot \delta + 5.464 \cdot \lambda$
2 slots	$3.78662 \cdot \delta + 5.67993 \cdot \lambda$
3 slots	$3.19531 \cdot \delta + 6.43493 \cdot \lambda$
...	...
15 slots	$2.2539 \cdot \delta + 18.0312 \cdot \lambda$
...	...

Issues

Optimization for N versus a running protocol

1. we do not know the number of competitors
2. the competitor stations may appear with a certain pbb distribution

how do the protocols behave in this case?

Full Buffer

each of N stations has always something to send

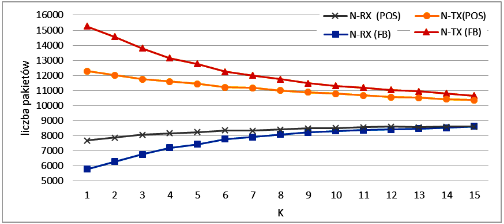
Poisson

requests to send appear with the Poisson distribution

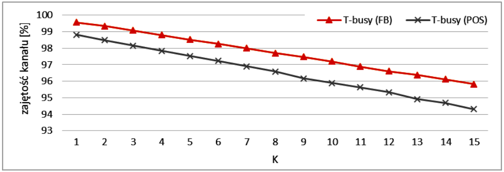
Some simulations results

parameters

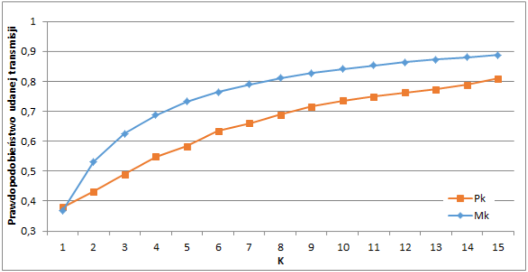
1. $N = 5$, $\delta = 100\lambda$
2. examined: number of slots k
3. total transmission time $10^6\lambda$



Number of sent versus the number of received messages



Channel usage



Probability of successful transmission

Dishonest stations

Cheating

simply choose early starting times

Sybil attacks

emulate many stations with different ID's, increased chances to get the access to the channel

Dishonest choice

Fair choice of the starting time

- pseudorandom choice of starting time (e.g. based on public key cryptography)
- problems: quite heavy computations, no time to check validity in real-time, only post-factum

Sybil attack

identity

Crypto countermeasures

ID’s based on public key cryptography, authentication
Problems: privacy, large scale, . . .

A little bit hopeless from the point of view of deployments problems/expected gain

Sybil attack

physical layer

Situation

A and *B* are the same station, it pretends two stations to increase chances

Test

testing whether *A* and *B* are really different:

1. *A* send some *k* messages,
2. other stations create collisions so that some of the messages are jammed
3. *B* has to answer which has not been jammed

Idea

if *A* is sending, then (for some devices) *A* cannot monitor the channel for collision. So if *A* and *B* are in reality the same device, then *B* does not know the answer.

Thanks for your attention!

Contact data

1. `Miroslaw.Kutylowski@pwr.edu.pl`
2. `http://kutylowski.im.pwr.wroc.pl`
3. +48 71 3202109