Towards Fair Leader Election in Wireless Networks

Zbigniew Gołębiewski[1,2], Marek Klonowski, Michał Koza, Mirosław Kutyłowski[1]

Wrocław University of Technology[2], Wrocław University[1]

AD HOC NOW 2009, Murcia

FRONTS, 7th Framework Programme, contract 215270

Problem
unfair behavior of users

Ad hoc groups

An ad hoc group of devices forms a local network and has to self-organize itself.

For instance

- scheduling the transmission requests,
- assigning auxiliary tasks,
- ...

basics of any reasonable, self-running system that has to work well
despite of heterogeneous devices, evolving overlay systems, ...

Basic assumptions

Assumptions

- questions are to be resolved locally (devices come from diverse providers...)
- no pre-knowledge on the group
- no external authentication, trust evaluation,...

Communication assumptions

Assumptions

- wireless communication, a single hop network
- denial of service is a failure for the adversary *(blocking the network can be achieved by just jamming)*
- a station can either transmit or receive but not both
- transmission successful iff only one device broadcasts, collisions can be recognized.

Leader election

Problem statement

Given a group of n devices, each holding a unique ID. The goal is to choose a member of a group so that

1. each group member has the same chance to become the leader
2. there is a consensus who is the leader

Leader election

Problem statement

Given a group of n devices, each holding a unique ID. The goal is to choose a member of a group so that

1. each group member has the same chance to become the leader
2. there is a consensus who is the leader

Network assumptions - recalled

- wireless communication
- single hop
- small group size
  we are not looking for asymptotic solutions for n stations with $n \to \infty$

Trust model
selfish behavior

Society of devices

1. devices might be selfish and may try to cheat
2. each device tries to hide that it is behaving badly
3. no device oriented on blocking the network
   this can be achieved easily by jamming the radio channel

the protocol itself has to force the devices to behave well

Basic scheme and misbehavior

Basic leader election scheme

Network

(approximately) n stations willing to become the leader, station synchronized

The following steps repeated until success:

- **time 0** each station decides at random to be either *active* or *passive* or *idle*
- **time slot 1** each active station transmits its identifier with probability $\frac{2}{n}$, each passive station listens with probability $\frac{2}{n}$,
- **time slot 2** each passive station retransmits the identifier it has heard in slot 1, each active station listens,
- **time slot 3** the active station that has received its identifier at step 2 retransmits

Basic scheme

The following steps repeated until success:

- **time 0** each station decides at random to be either *active* or *passive* or *idle*
- **time slot 1** each active station transmits its identifier with probability p, each passive station listens with probability p,
- **time slot 2** each passive station retransmits the identifier it has heard in slot 1, each active station listens,
- **time slot 3** the active station that has received its identifier at step 2 retransmits

The best success probability $\frac{1}{e^2}$ achieved if $p = \frac{2}{n}$.

Basic scheme - simplified

with a confirmer (the previous leader)

The following steps repeated until success:

- **time slot 1** each station transmits its identifier with probability p, the confirmer listens,
- **time slot 2** the confirmer retransmits the identifier it has heard in slot 1, each station listens,

The best success probability $\frac{1}{e}$ achieved if $p = \frac{1}{n}$.

Misbehavior for Basic Scheme

Change probability

Just transmit with probability 1.
Nobody else can become the leader.

Effect on trial success probability

- each honest station transmits with pbb $\frac{1}{n}$,
- the dishonest station transmits with pbb p_z

Success probability:

$$p_z \left(1 - \frac{1}{n}\right)^{n-1} + (1-p_z)(n-1)\frac{1}{n}\left(1 - \frac{1}{n}\right)^{n-2} = \left(1 - \frac{1}{n}\right)^{n-1}$$

Misbehavior for Basic Scheme

corollaries

1. measuring the time to success does not give any information of nasty behavior
2. analyzing sequence of silence and collision states is necessary

Non-aggressive station case

Assumptions

1. sending probability of the misbehaving station less than $\frac{1}{2}$
2. the number of stations n relatively high

Result

probability distribution of patterns states of the channel until success is close to the case with no misbehaving station.

Malicious stations emulating many stations

Attack

Attack strategy

- a single malicious station can mimic many stations with different identities,
  if any of these "virtual stations" gets elected, the adversary wins.
- fair elections $\Rightarrow$ each candidate gets the same chance $\Rightarrow$ the adversary creates many virtual stations in order to improve his chances

Problem

eliminating fake stations is hard, if no strong identity verification and certification is implemented.

A hopeless situation?

Algorithm overview

Phases

1. creating the list of candidates
2. random choice
3. checking for duplicates:
   if duplicates detected, remove and `goto 2`

List of candidates

Algorithm

1. basic method,
   each station which is still not on the list may transmit its identifier
2. all identifiers that are transmitted without collision are added to the list
3. all stations which identifiers are <u>not</u> on the list transmit in the check slot, if anybody transmits (single or collision), `goto 1`

Random choice

Algorithm for k participants

1. each station s_i chooses a random number r_i and broadcasts a (cryptographic) commitment to r_i in time slot i
2. in time slot $k + i$ station s_i opens the commitment,
3. after all commitments opened, then $r := ((\sum r_i) \bmod k) + 1$ and s_r is the station chosen

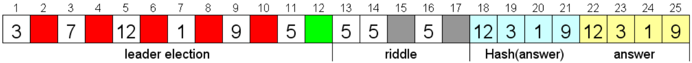
It suffices that a single station chooses r_i at random

Riddle procedure
eliminating cheaters

Algorithm for a t -way check

1. the leader sends its ID in each of t slots,
2. for $i \leq t$, each other station at slot i:
   - with probability $\sqrt[n-1]{0.5}$ listens,
   - otherwise it creates a collision in this slot.
3. each station (except the leader) should be able to say when collisions has occurred:
   - at slot i such that it has transmitted,
   - at slot i such that it has not transmitted and has not heard the leader's ID
4. in the next $n-1$ slots each station transmits its commitment to what the station has heard
5. ... then the commitments are opened.
6. all stations that have failed to say when the collisions have occurred are removed from the list.

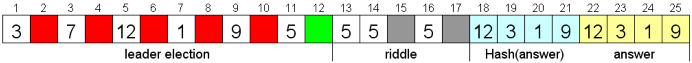
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3		7		12		1		9		5		5	5		5		12	3	1	9	12	3	1	9
leader election												riddle					Hash(answer)				answer			



In steps $1, 3, 5, 7, 9, 11$ the stations are listed (by means of a standard leader election algorithm).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3		7		12		1		9		5		5	5		5		12	3	1	9	12	3	1	9
leader election												riddle					Hash(answer)				answer			

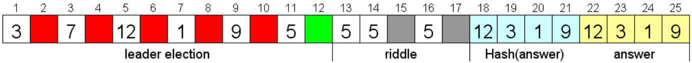
In steps $1, 3, 5, 7, 9, 11$ the stations are listed (by means of a standard leader election algorithm). In steps $2, 4, 6, 8, 10, 12$ checks are performed to see, if there are still stations in the system not present on the list.



In steps $1, 3, 5, 7, 9, 11$ the stations are listed (by means of a standard leader election algorithm). In steps $2, 4, 6, 8, 10, 12$ checks are performed to see, if there are still stations in the system not present on the list. After step 12, the list is randomly sorted and first station becomes the candidate (here $ID = 5$).

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3		7		12		1		9		5		5	5		5		12	3	1	9	12	3	1	9
leader election												riddle					Hash(answer)				answer			

In steps $1, 3, 5, 7, 9, 11$ the stations are listed (by means of a standard leader election algorithm). In steps $2, 4, 6, 8, 10, 12$ checks are performed to see, if there are still stations in the system not present on the list. After step 12, the list is randomly sorted and first station becomes the candidate (here $ID = 5$). In steps $13 - 17$ the riddle is posed, the answer commitments are gathered in steps $18 - 21$.



In steps $1, 3, 5, 7, 9, 11$ the stations are listed (by means of a standard leader election algorithm). In steps $2, 4, 6, 8, 10, 12$ checks are performed to see, if there are still stations in the system not present on the list. After step 12, the list is randomly sorted and first station becomes the candidate (here $ID = 5$). In steps $13 - 17$ the riddle is posed, the answer commitments are gathered in steps $18 - 21$. Stations' answers are revealed in steps $22 - 25$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3		7		12		1		9		5		5	5		5		12	3	1	9	12	3	1	9
leader election												riddle					Hash(answer)				answer			

In steps $1, 3, 5, 7, 9, 11$ the stations are listed (by means of a standard leader election algorithm). In steps $2, 4, 6, 8, 10, 12$ checks are performed to see, if there are still stations in the system not present on the list. After step 12, the list is randomly sorted and first station becomes the candidate (here $ID = 5$). In steps $13 - 17$ the riddle is posed, the answer commitments are gathered in steps $18 - 21$. Stations' answers are revealed in steps $22 - 25$. If all answers are correct, the leader candidate becomes the Leader; if any station answered wrongly it is removed from the list and algorithm jumps to step 13.

Cheaters and the riddle

Assume a candidate j and the leader are the same station

1. the leader must transmit its ID (otherwise silence occurs with probability $\frac{1}{2}$ and the leader is declared as a cheater,
2. if leader sends, then candidate j does not know the state of the channel (as it is served by the same station) $\Rightarrow$ so candidate j will fail the test with high probability

Cheaters and the riddle

Assume a candidate j and the leader are the same station

1. the leader must transmit its ID (otherwise silence occurs with probability $\frac{1}{2}$ and the leader is declared as a cheater,
2. if leader sends, then candidate j does not know the state of the channel (as it is served by the same station) $\Rightarrow$ so candidate j will fail the test with high probability

why the leader is not removed from the list?

Cheaters and the riddle

Assume a candidate j and the leader are the same station

1. the leader must transmit its ID (otherwise silence occurs with probability $\frac{1}{2}$ and the leader is declared as a cheater,
2. if leader sends, then candidate j does not know the state of the channel (as it is served by the same station) $\Rightarrow$ so candidate j will fail the test with high probability

why the leader is not removed from the list?

the leader is not necessarily a cheater: some candidate may pretend to be served by the same station as the leader

Fine tuning

If the number of non-collisions is to low the check is repeated
(otherwise dishonest leader might send junk all the time)

Probabilities, a single dishonest station with k virtual copies

- each honest station gets the same chance to become the leader:

$$\frac{1}{n} + \frac{k}{n} \cdot \frac{1}{n-k+1} = \frac{n+1}{n} \cdot \frac{1}{n-k+1}$$

- the dishonest station gets elected with probability

$$\frac{k}{n} \cdot \frac{1}{n-k+1}$$

Final remarks

1. presented technique works only if the adversary has a single device
2. ... but similar tricks are possible also if there are collusions of users
(to be included in a journal version)

Thank you for your attention!

miroslaw.kutylowski@pwr.wroc.pl