Tracing pirate cards as part of the satellite video broadcasting

Ulrich AIVODJI, Alexandre GONZALVEZ,
Pascal LEFEVRE, Brandon DRAVIE

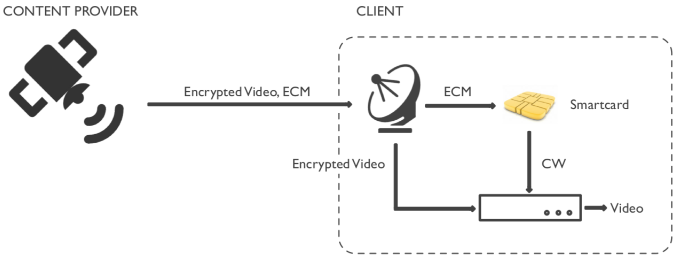
Supervisors: Cécile DELERABLÉE, Thomas BAIGNÈRES

REDOCS'16 Report

28^{th} *October* 2016

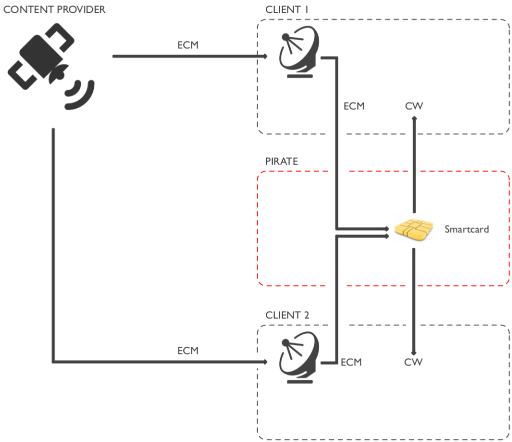
Table of contents

Problem



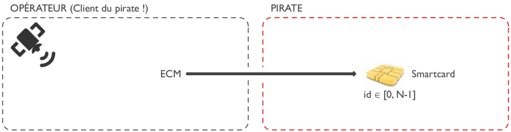
Satellite broadcasting

Problem



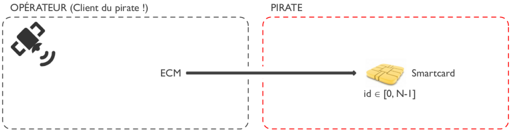
Hacking

Problem

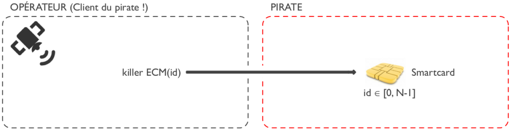


Provider:
Pirate client

Problem

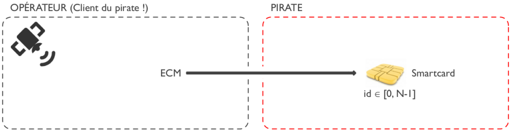


Provider:
Pirate client

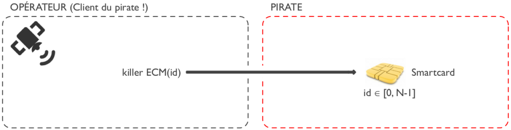


Killer ECM

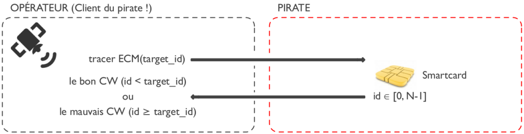
Problem



Provider:
Pirate client



Killer ECM



Id target

Pirate Strategies

1. $\text{strategy1}(r, CW_0, \ldots, CW_{n-1}) \rightarrow CW_0$

2. $\text{strategy2}(r, CW_0, \ldots, CW_{n-1}) \rightarrow \begin{cases} \text{majority}(CW_0, \ldots, CW_{n-1}) & \text{if } n \text{ is odd} \\ CW_0 & \text{else} \end{cases}$

3. $\text{strategy3}(r, CW_0, \ldots, CW_{n-1}) \rightarrow CW_{r \bmod n}$

Table of contents

Metrics

- CPU Time (s)
- Collateral damage *ColD* (Avg, stddev): $\sum(1 - \frac{id_i}{N})$
- QoS of the pirate (Avg): $100 * \frac{t}{T}$ (T: number of normal *ECMs*, t: number of correct *cw*)

Table of contents

General principle

- Hypothesis: The traitor always uses the same card.
- Goal: Locate the card by using a minimum number of tracking ECM. Killing the card will
- Solution: Binary search (average number of iterations $log(n)$)

Benchmark

	CPU Time (s)	Collateral damage		QoS
		Avg	Stddev	Avg
Binary Search	54.37	14.11	8.14	0
Ternary Search	54.18	17.52	10.78	0

Table: Benchmark for 100 runs and nbCard = 10

Table of contents

Strategy 2

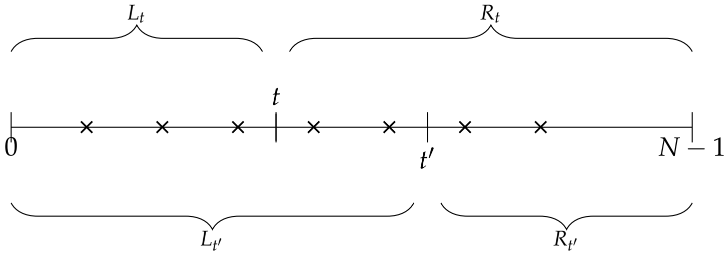
Notations

- M_t : pirate response to ECM tracer t
- $M_t \in L$: majority of pirate cards identifiers are $< t$ (on the left side)
- $M_t \in R$: majority of pirate cards identifiers are $\geq t$ (on the right side)

Strategy 2: Why binary search works.

Proposition

Let $p = 2k + 1$ cards (majority vote) and $t' < t$ two tracers ECM.
$M_t \in L$ and $M_{t'} \in R \implies \exists\, \mathbf{Id}_P \in [t', t[$.



Algorithm

Pivots

- $p \leftarrow 0$
- $p' \leftarrow N - 1$

Details

- Stops when $|p - p'| = 1$
- ECM tracer $t_m \leftarrow \lfloor (p + p')/2 \rfloor$
  if $M_{t_m} \in L$, $p' \leftarrow t_m$
  else $p \leftarrow t_m$

Benchmark Strategy II

	CPU Time (s)	Collateral damage		QoS
		Avg	Stddev	Avg
Optimal approach	249.82	50.35	17.24	0
Paper approach [Tas05]	94.69	50.55	15.10	0

Table: Benchmark for 100 runs and nbCard = 10

Tamir Tassa, *Low bandwidth dynamic traitor tracing schemes*, J. Cryptol. **18** (2005), no. 2, 167–183.

Table of contents

Strategy 3

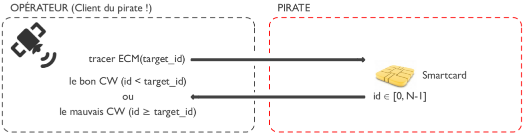
Description

Strategy 3

Description

Pirate Strategy

Own a number n of cards, and generates randomly and uniformly an number r larger than n.

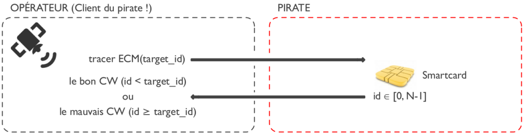


Strategy 3

Description

Pirate Strategy

Own a number n of cards, and generates randomly and uniformly an number r larger than n.



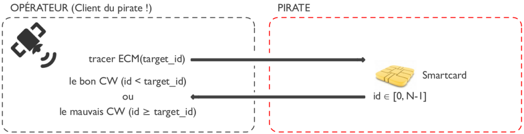
- made only of correct values **cw**

Strategy 3

Description

Pirate Strategy

Own a number n of cards, and generates randomly and uniformly an number r larger than n.



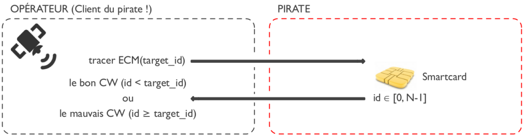
- made only of correct values **cw**
- made only of incorrect values of **cw**

Strategy 3

Description

Pirate Strategy

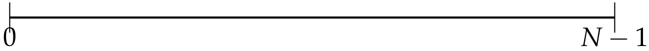
Own a number n of cards, and generates randomly and uniformly an number r larger than n.



- made only of correct values **cw**
- made only of incorrect values of **cw**
- made both of correct and incorrect values of **cw**

Strategy 3

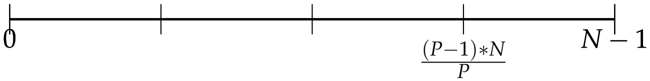
Algorithm



Population : N-1 cards

Strategy 3

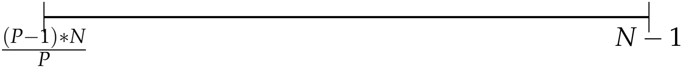
Algorithm



P pirates cards $\rightarrow$ P - 1 intervals

Strategy 3

Algorithm

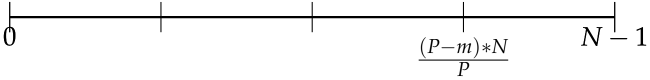


Condition for dichotomy

In [A;B], if $NbrCardsFalse > 0$, then at least a pirate card is present.

Strategy 3

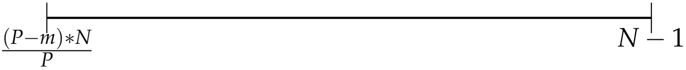
Algorithm



With m intervals.

Strategy 3

Algorithm



Condition for dichotomy

In [A;B], if *NbreCardsFalse* - (nbCardsMute+0.6)*Cst >0 ,
then at least a pirate card is present.

Benchmark Strategy III

	CPU Time (s)	Collateral damage		QoS
		Avg	Stddev	Avg
Heuristic approach	631.29	68865	35630	57

Table: Benchmark for 100 runs and nbCard = 10

General principle for Strategy III version II

- Return a set of small intervals that have a good probability to contain id of the traitor's cards
- Let $S = \{0, 1, 2, \ldots, n-1\}$ be the set of all the cards (regular user and traitors).
- Divide S in 100 subsets and select subsets S_j that pass the test.
- The test take a subset $Sj = [a, b]$, uses a and b as input for a tracking ECM send *nbSample* times.
- Let *ProbA* be the chance to have negative response with tracking ECM a and *ProbB* be the chance to have positive response with tracking ECM b.
- Reject S_j if $abs(ProbA - ProbB) > epsilon$ and accept S_j otherwise.
- Repeat until $|S_j| \leq 1000$.

Table of contents

Bilan

- Optimal counter attack against strategy I and II
- 2 heuristic approaches for strategy III

Perspectives

- Find theoretical bound for strategy III
- Explore game theory alternative (Bilevel optimization)

$$\begin{aligned} \min_{id_i} \quad & \sum_i (1 - \frac{id_i}{N}) \\ \text{s.t.} \quad & QoS(pirate) \leq \epsilon \\ & id_i \in \{0, 1\} \end{aligned}$$

Bonus

Content

- Challenges
- Knowlegde

Interesting tools and methods

- Teamwork with efficiency (AGILE method)
- Tools: GitHub, CollabEdit

Social

- Contacts, colleagues, friends, fun...