Detecting and Excluding Misbehaving Nodes in a P2P Network

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong
firstname.lastname@supelec.fr

Supélec, SSIR Group (EA 4039)

I²CS, June 2008
Schoelcher, Martinique

Main Line of Our Work

Aim

Guarantee Confidentiality, Integrity and Availability in P2P

Specificities of P2P Networks

Dynamic and *Collaborative* networks without *Central Authority*

Approach

1. Membership Control
2. Security Protocols tolerating a bounded number of attackers

Usage

Membership Control through Distributed Certification

1. Genuine members obtain a membership certificate [COPS '08]
2. Misbehaving nodes are excluded

Exclusion

1. Detection of misbehaving nodes
2. Revocation of their certificates

Related Work

Admission Control to a Peer Group [Kim *et al.*]

- Admission based on a *Group Charter*
- But people don't know each other...

Reputation Systems

- Reaction to some types of misbehaviors
- But lack of reactivity...

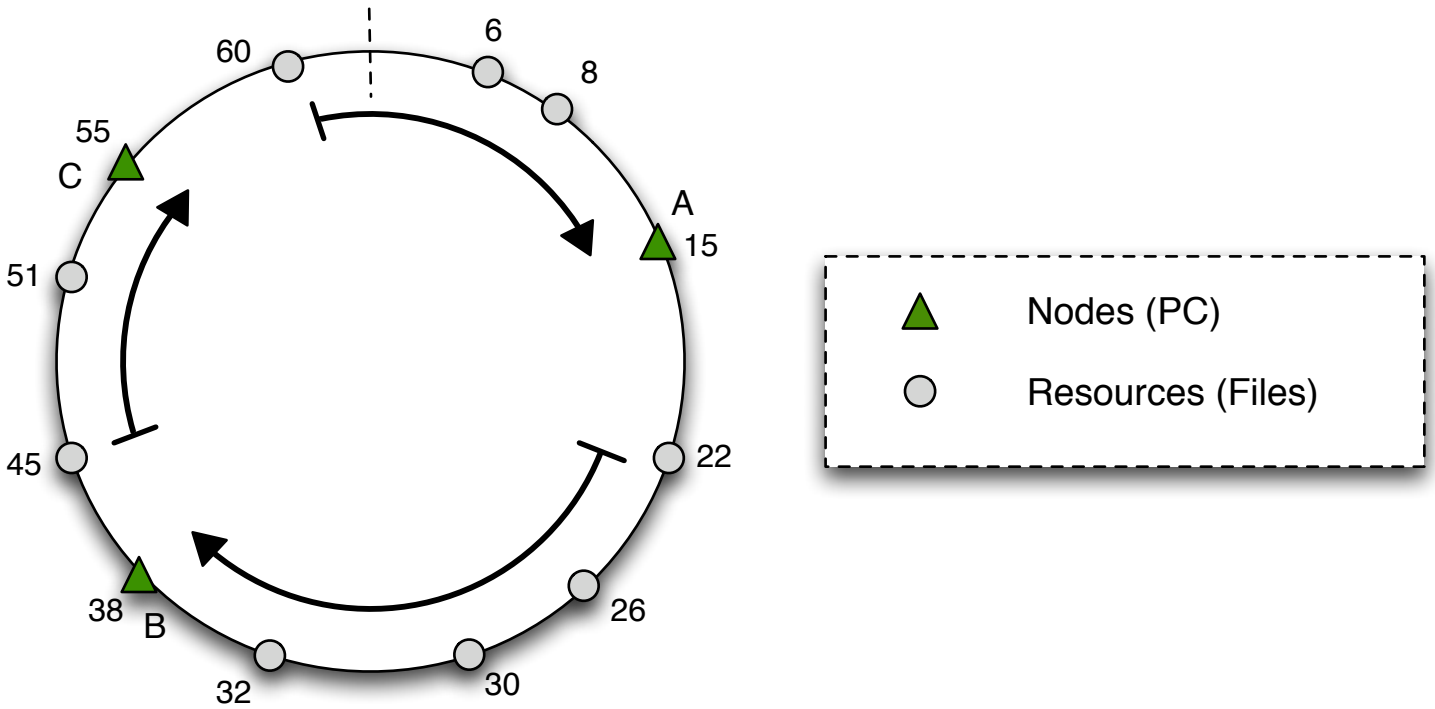
Proposed Detection and Exclusion

- Complementary reaction to some types of misbehaviors
- Attackers are immediately and globally excluded

Outline

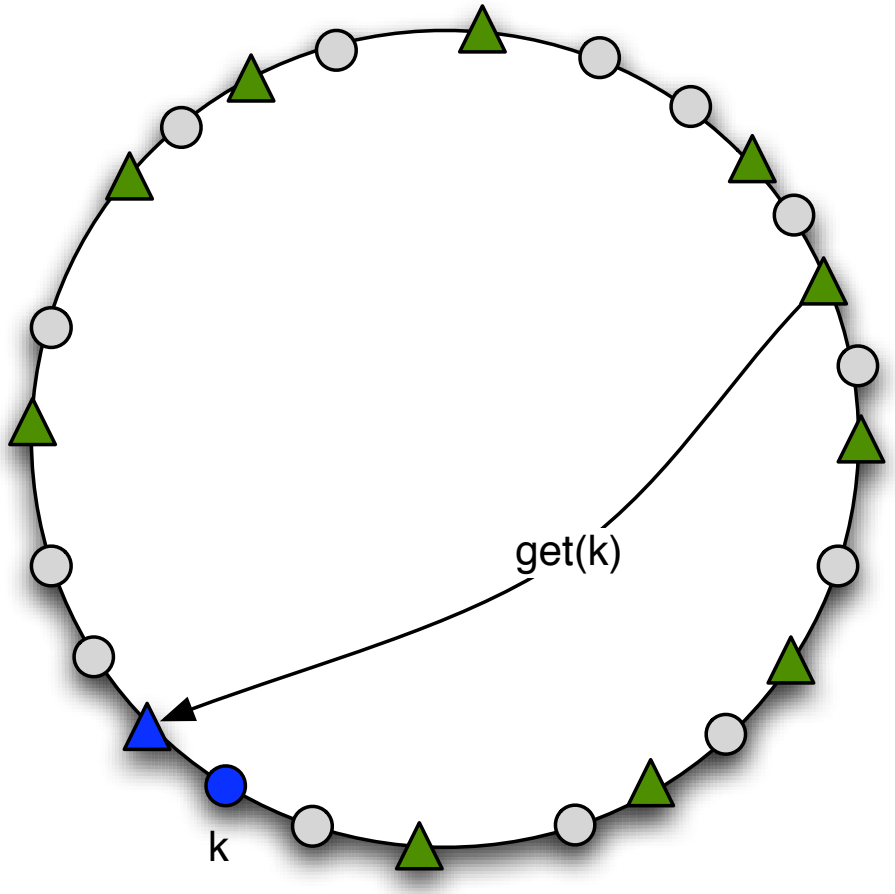
Use-case

Structured P2P Networks: Chord

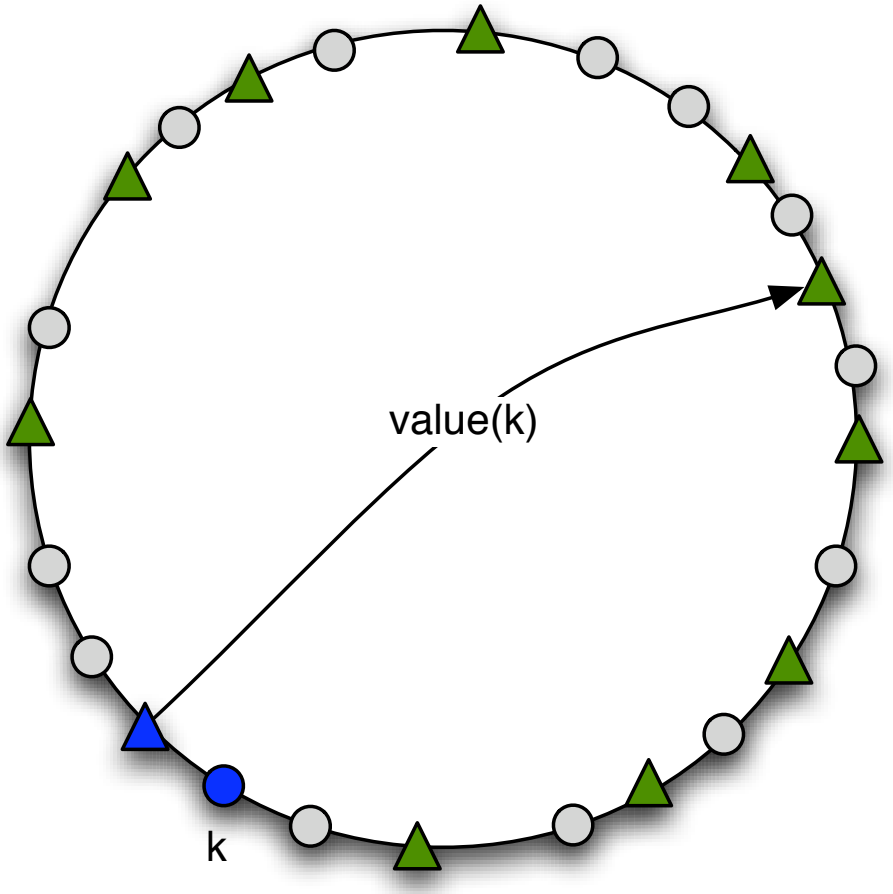


DHT : $key \mapsto value$

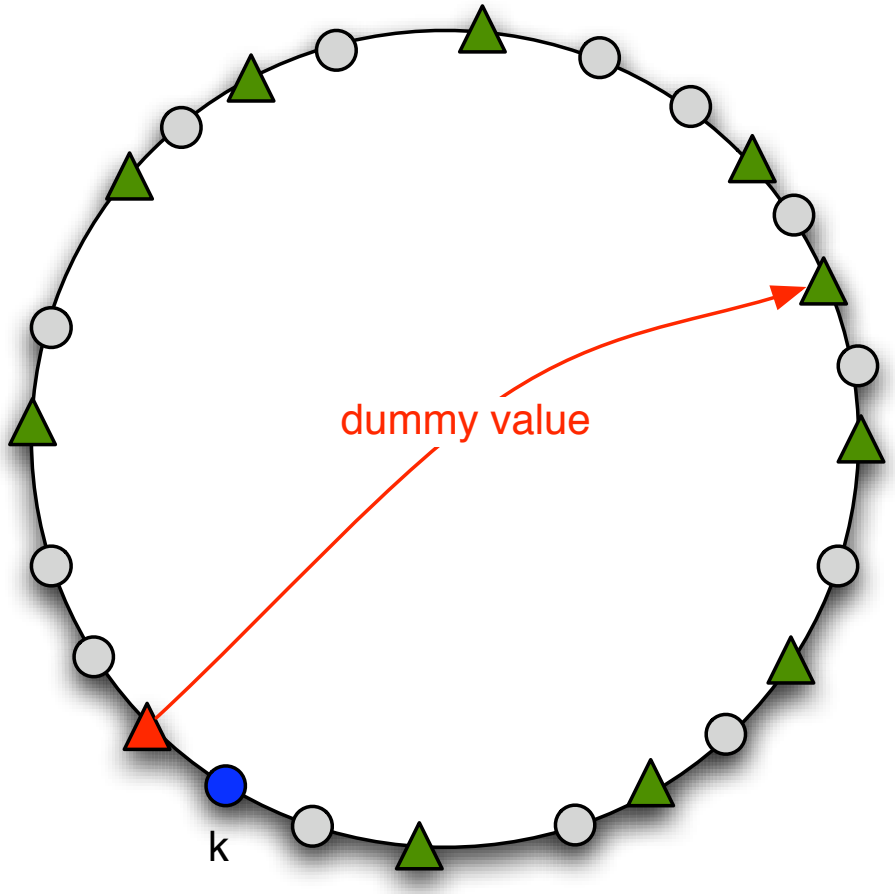
Sample Attack



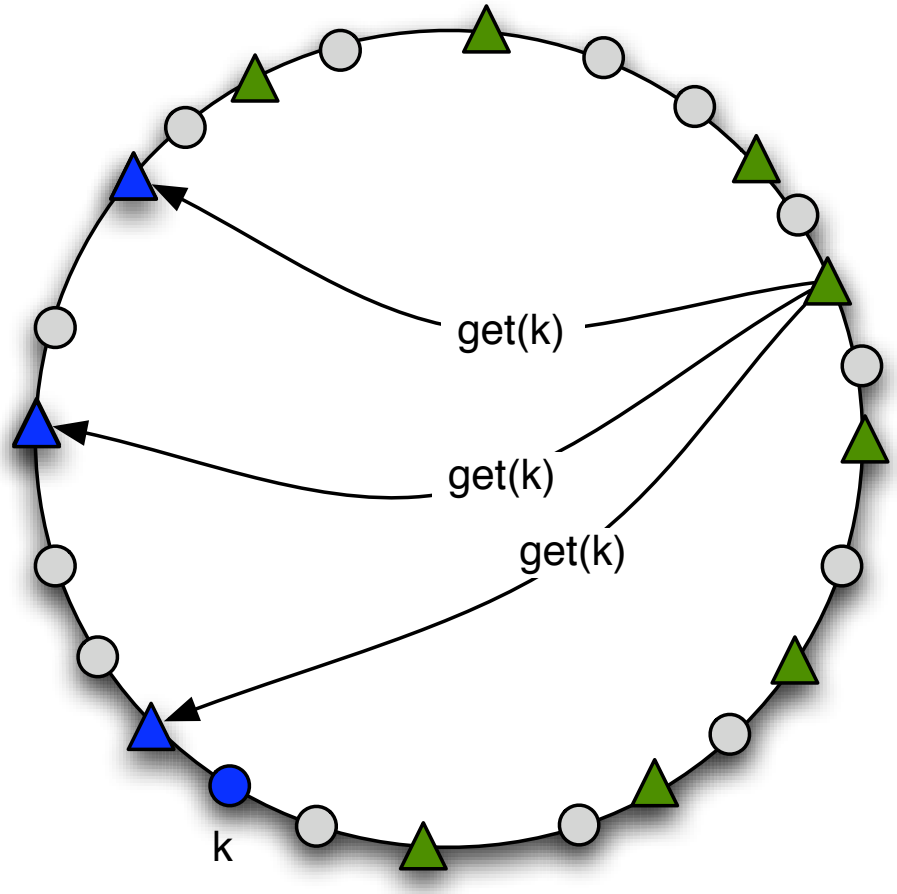
Sample Attack



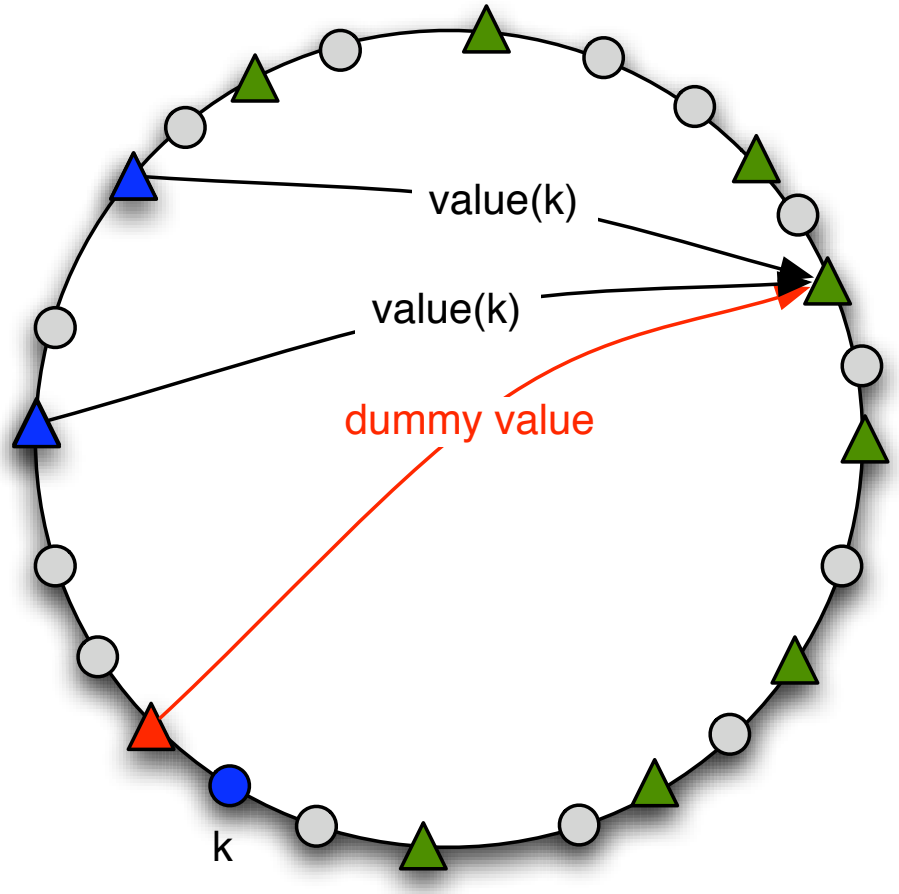
Sample Attack



Sample Attack



Sample Attack



Why Excluding these Attackers ?

Our strategy

- Exclude liars
- Make lying an inefficient strategy
- Reduce the number of redundant requests

Detecting Misbehaving Nodes

Detection

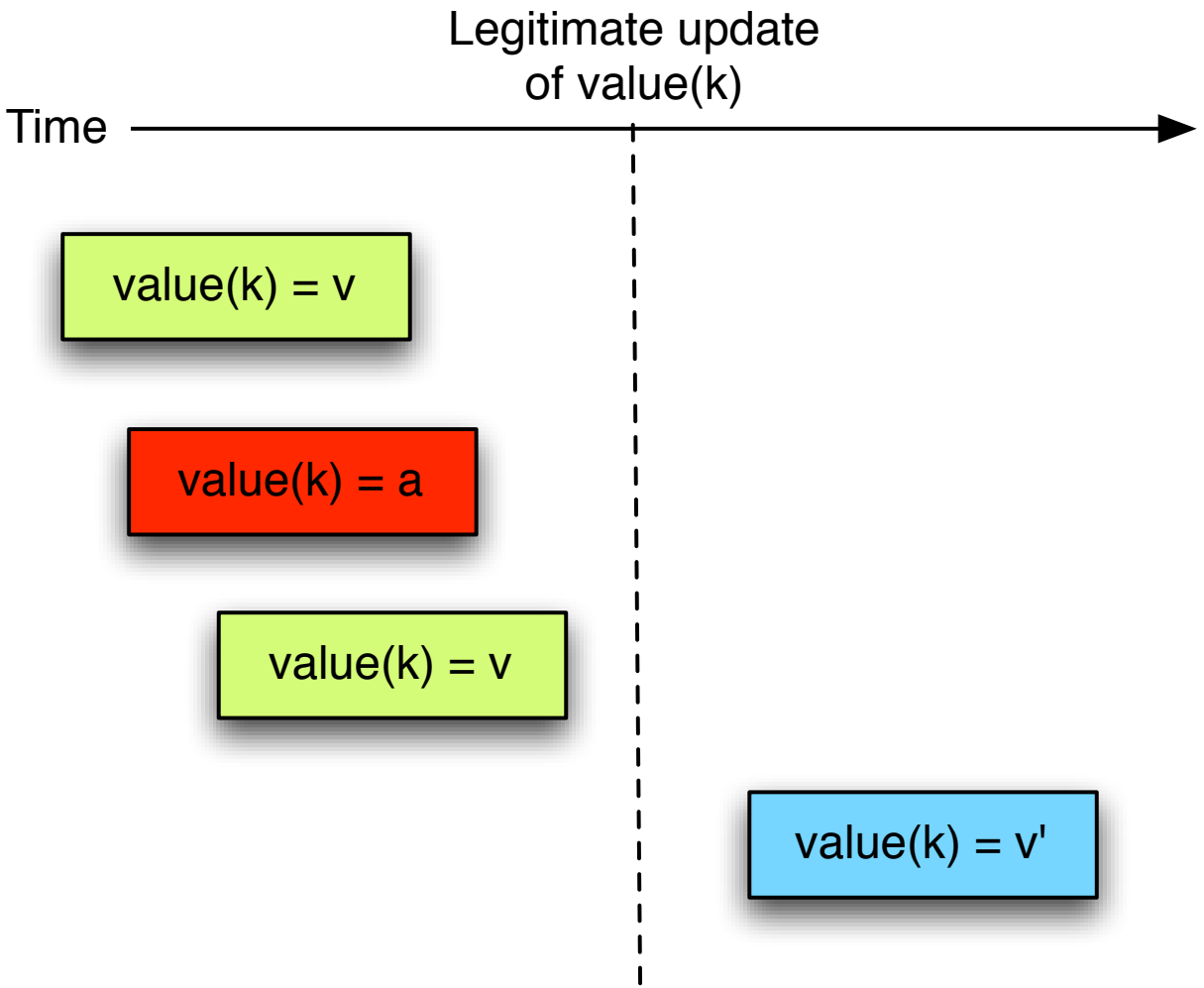
Hypothesis

Most of the nodes are well-behaving

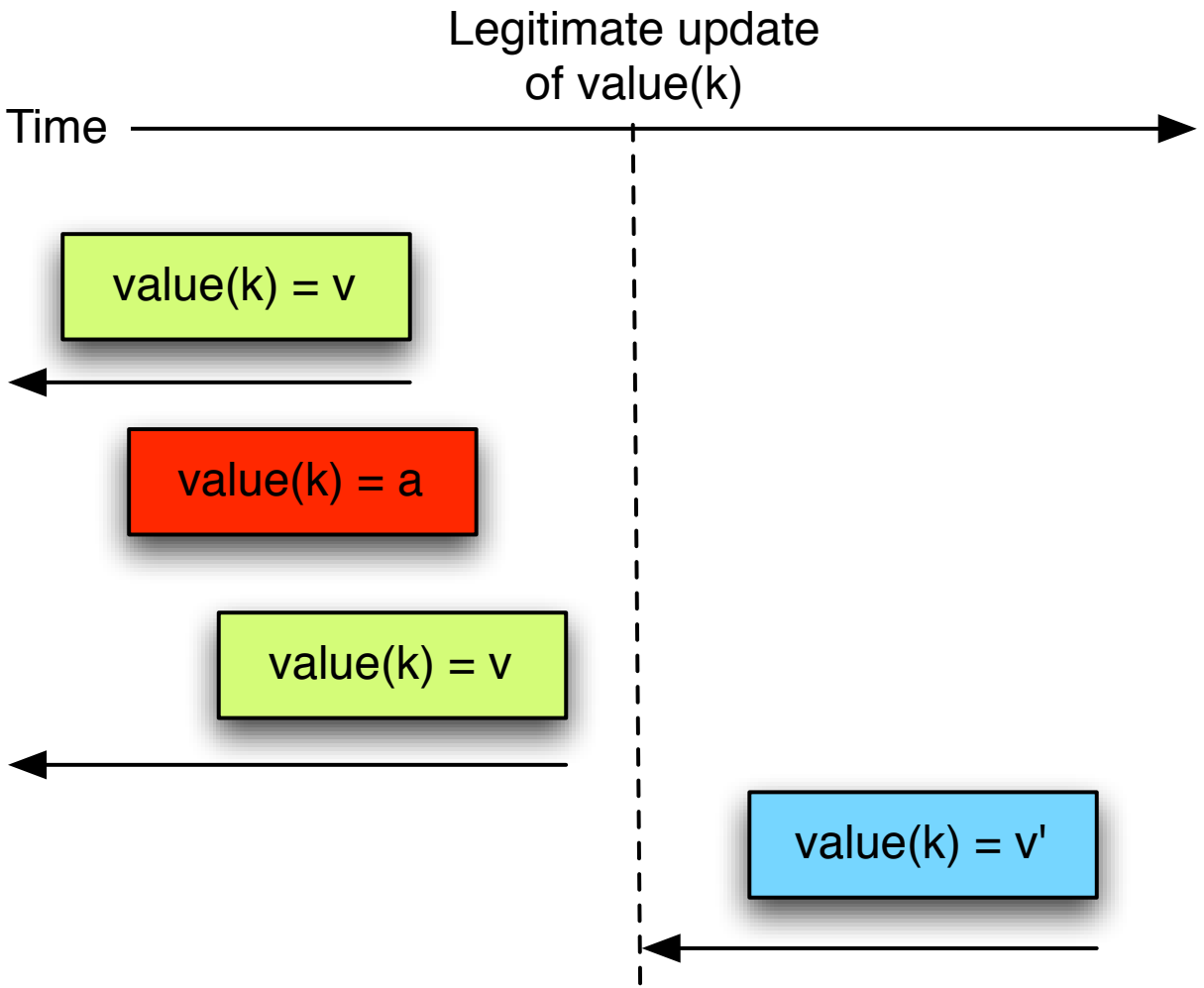
Principle

- Define Observable Behavior Specifications
- Compare nodes behaviors
- Generate misbehavior proofs

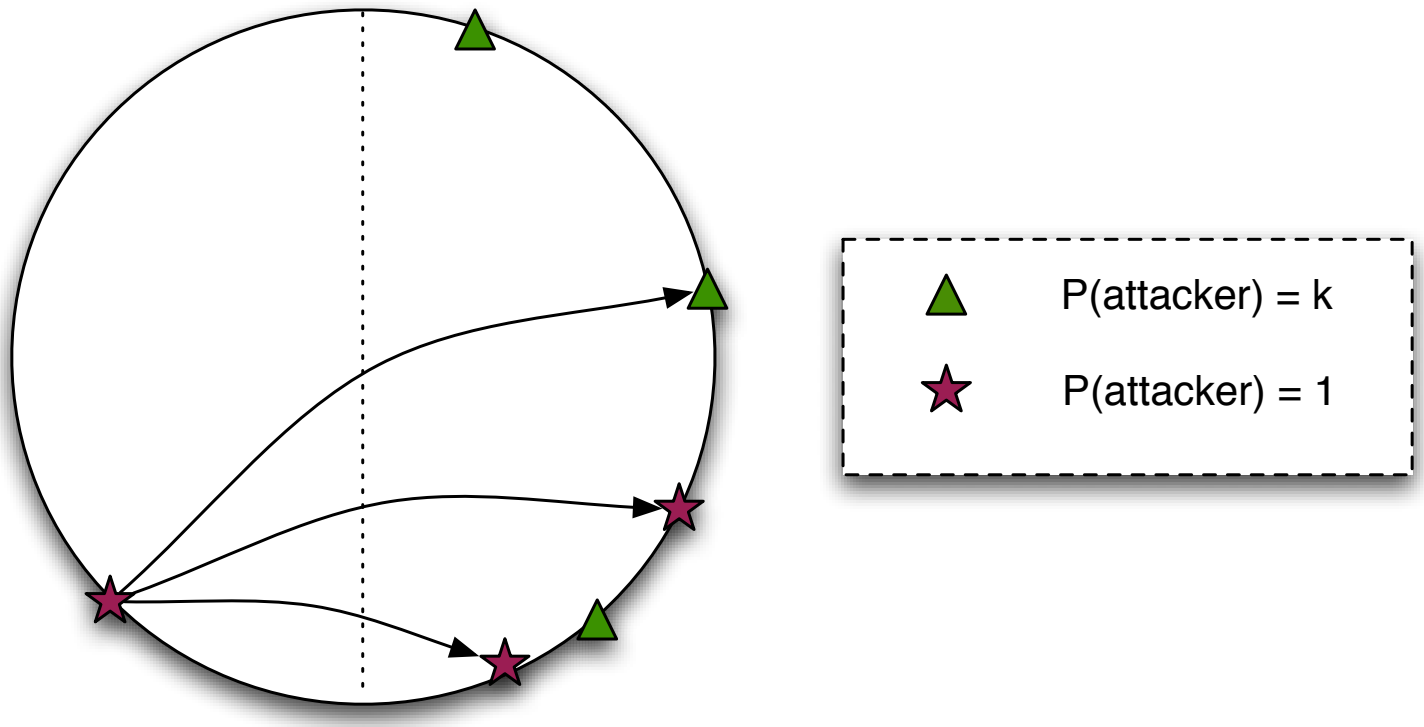
Timeframes


Legitimate update
of value(k)
Time
value(k) = v
value(k) = a
value(k) = v
value(k) = v'

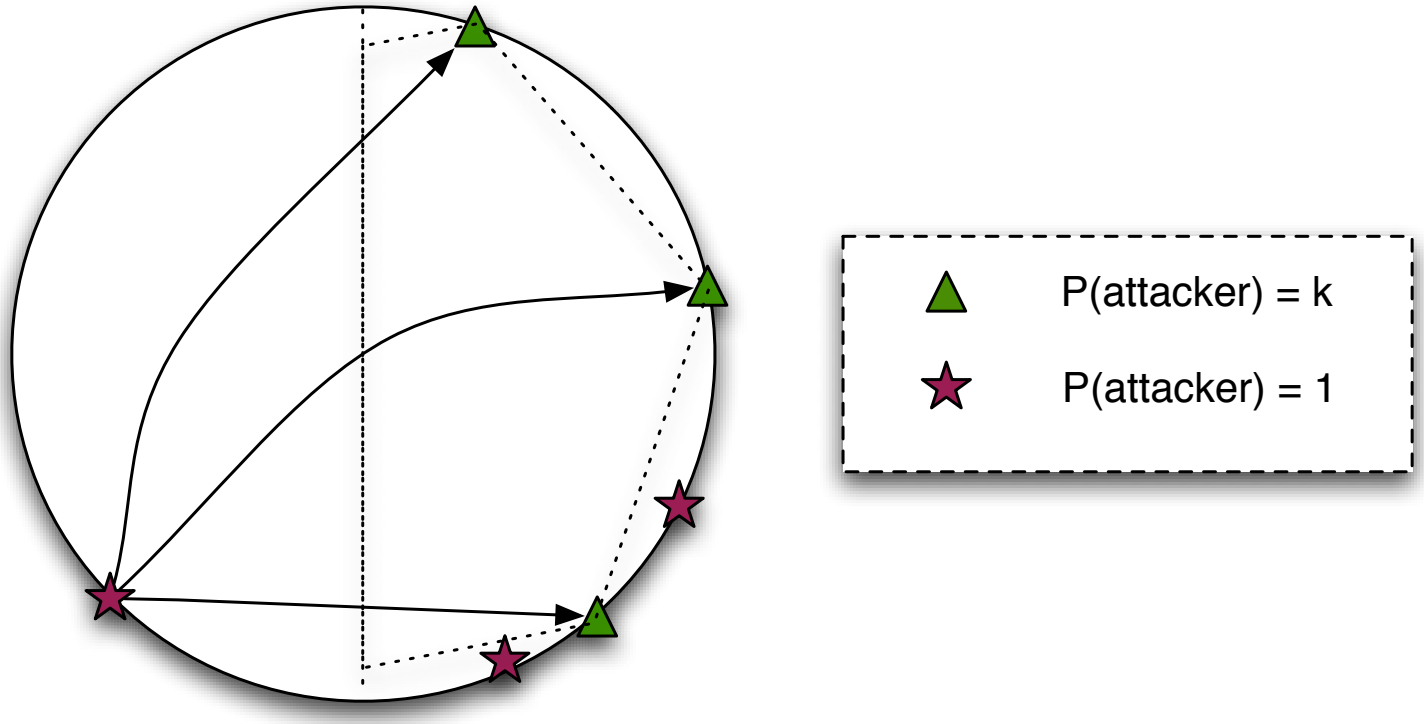
Timeframes


Legitimate update
of value(k)
Time
value(k) = v
value(k) = a
value(k) = v
value(k) = v'

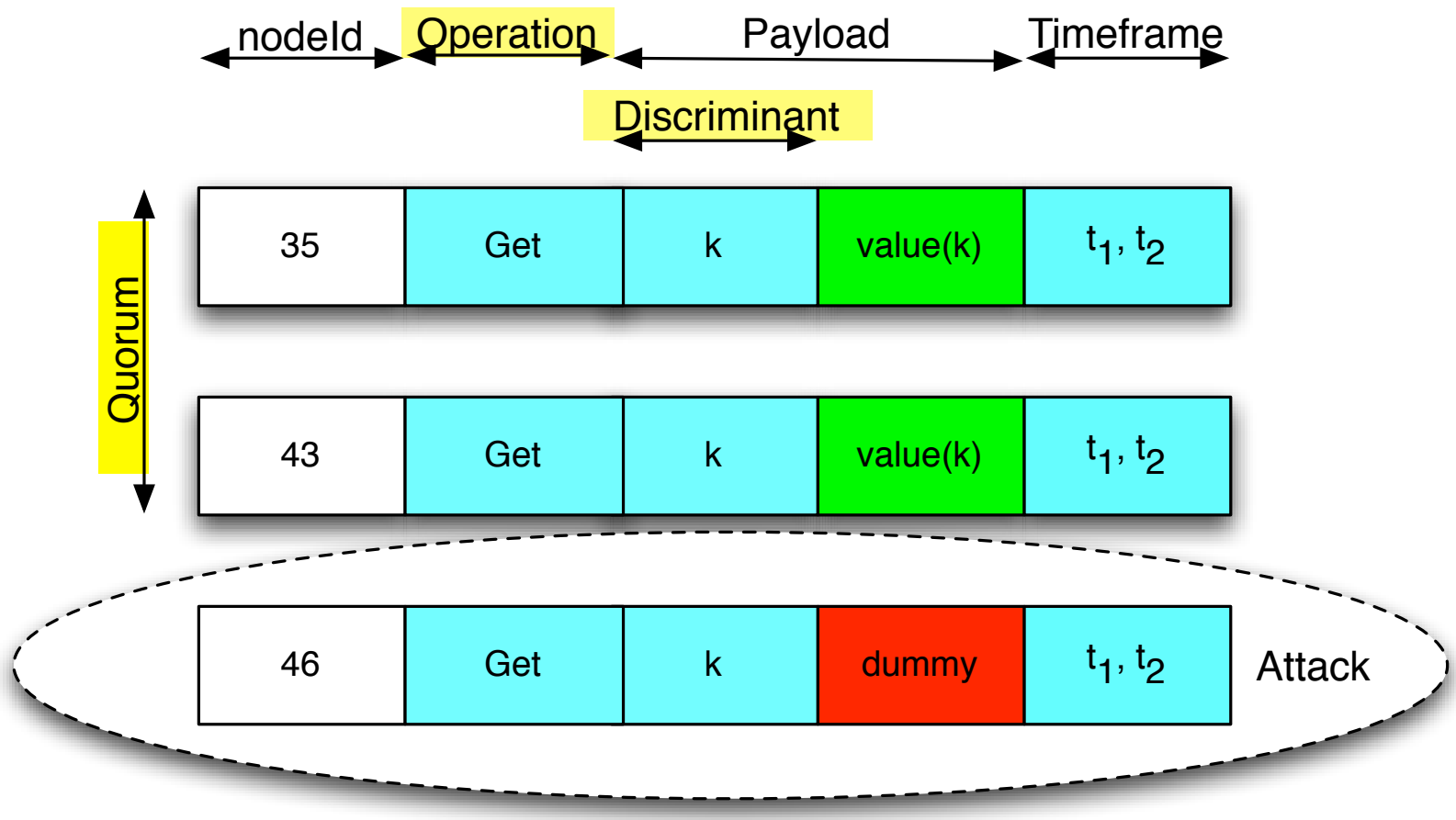
Decorrelation



Decorrelation



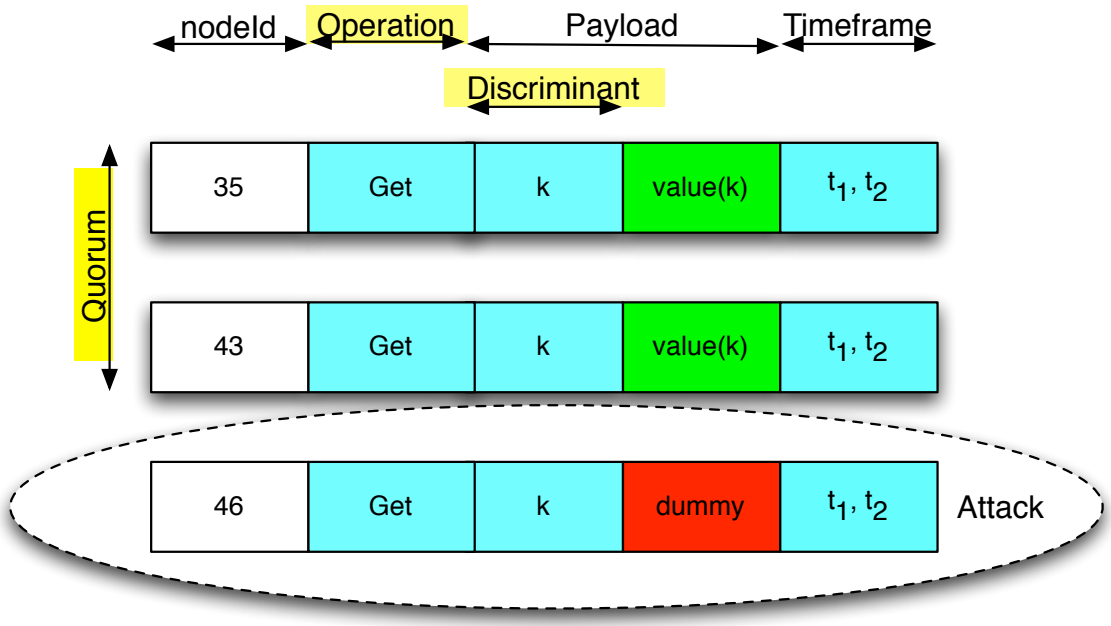
Three Messages showing an Attack



Format of Observable Behavior Specifications

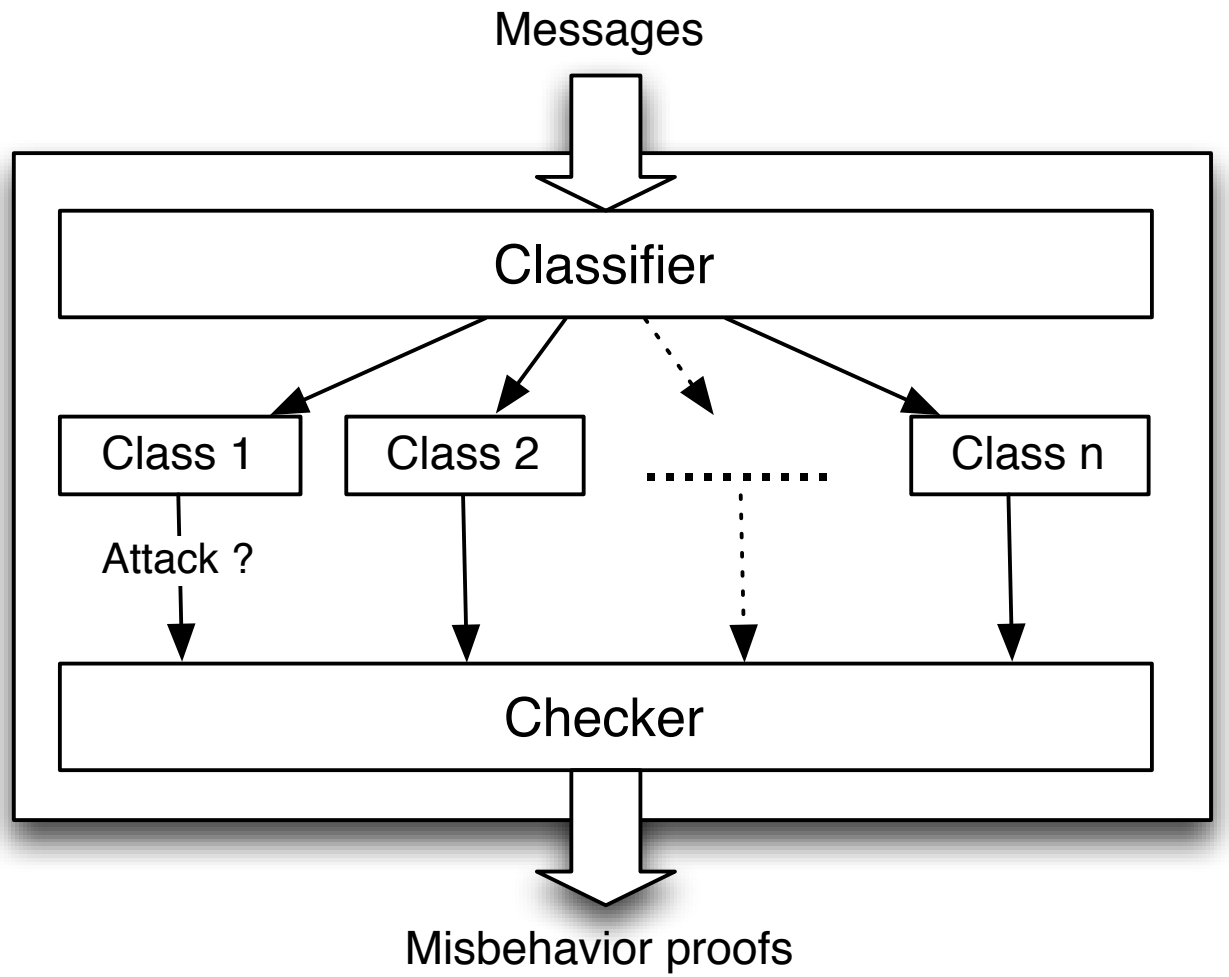
	Possible values	**Description**
Operation	Get ...	Attacked operation
Direction	Request | Response	Direction of attack
Discriminant	Field names	Equal fields in compared messages
Quorum	$\mathbb{N}$	Identical messages needed
Scope	Network | Replicas ...	Scope of the operation

Example: OBS of the sample attack



Operation	Direction	Discriminant	Quorum	Scope
Get	Response	*key*	$\frac{nbRep+1}{2}$	Replica Set

Overview


Messages
Classifier
Class 1
Class 2
Class n
Attack ?
Checker
Misbehavior proofs

Classifier

Classifier creates classes of messages

1. Related to the same OBS
2. Having the same discriminant
3. During the same timeframe

If all the nodes are honest, all messages of a given class are identical

Checker

Checker applies OBS to classes

1. Valid payload from the quorum
2. Proof against different payload(s)
3. Proof contains the minimal number of messages

The misbehavior proof is then used to exclude the attacker

Excluding Misbehaving Nodes

Excluding Misbehaving Nodes

1. Revoke the certificate of the attacker
2. Publish this revocation

Revocation

Revocation is done through Distributed Certification [AIMS 08]

1. Requires collaboration of t% of the nodes, whatever the size of the network
2. Each node locally checks the validity of the proof

If t% of the nodes validate the proof, the initiator node obtains the revocation to publish

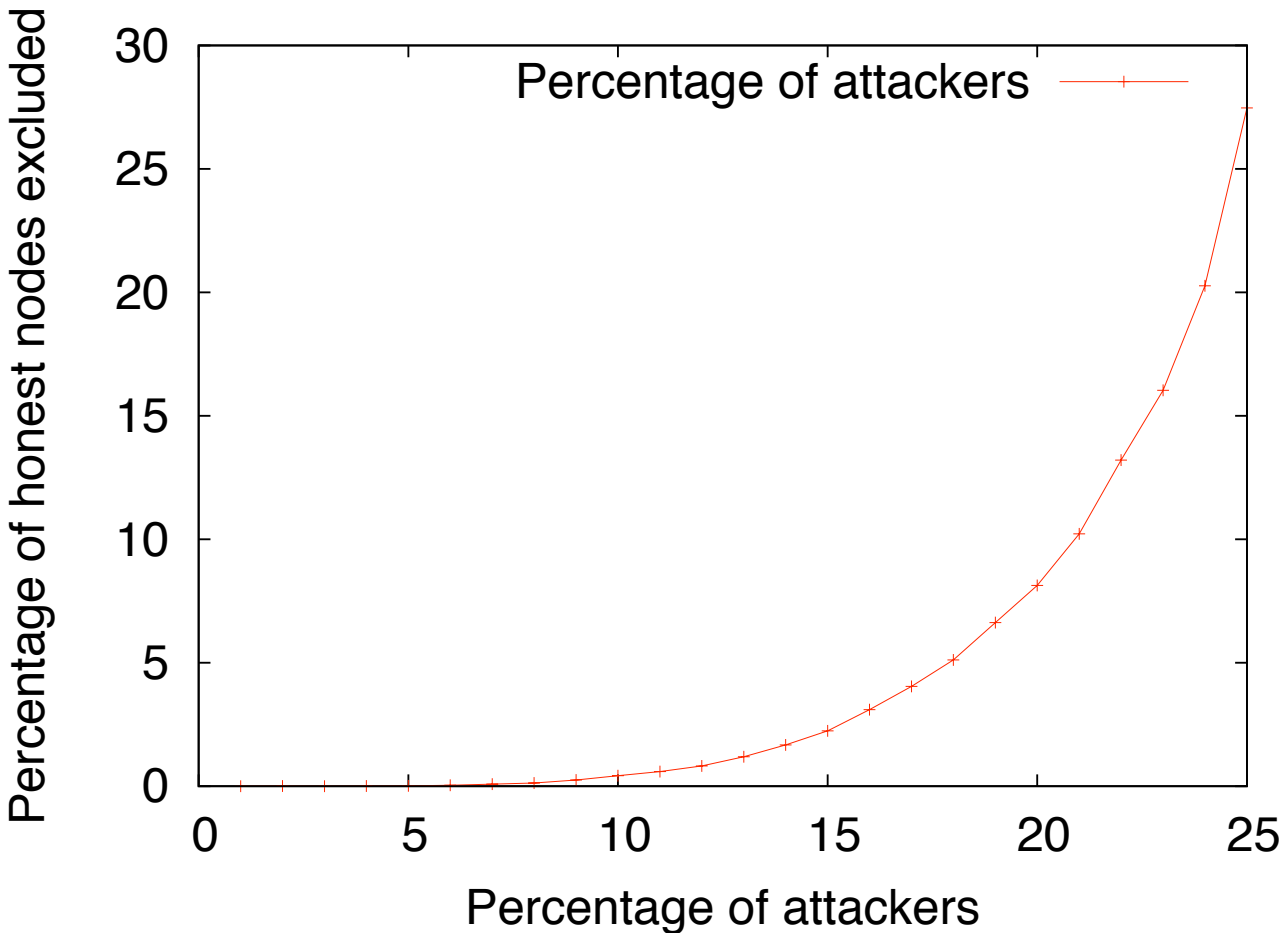
Publication

Notification of the revocation to all the nodes

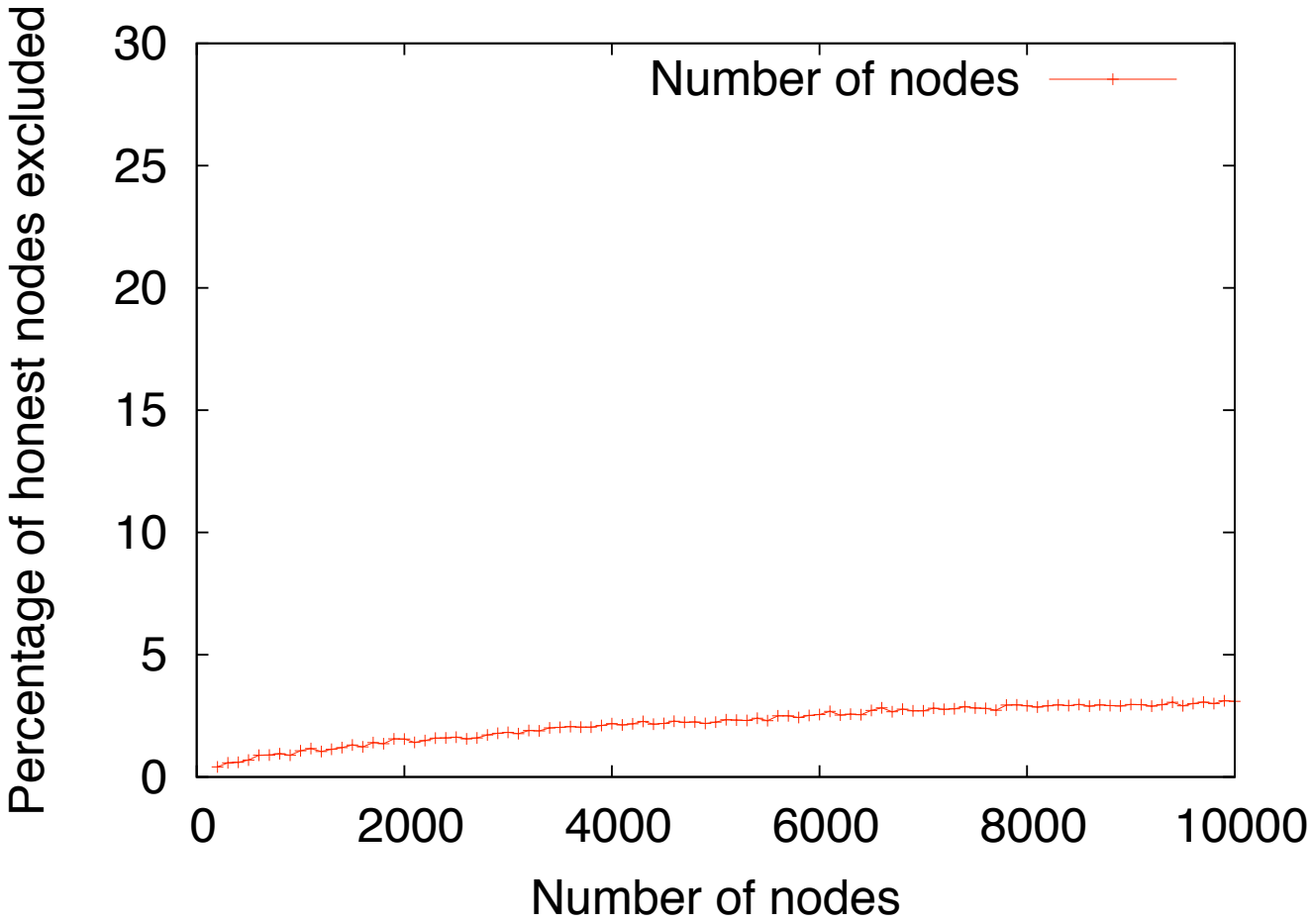
1. Put in the DHT at $h(attacker_{id})$
2. Directly notified to nodes connected to the attacker
   1. Nodes in its routing table
   2. Nodes having it in their routing table
   3. Nodes connected at application level

Simulations

Percentage of honest nodes excluded

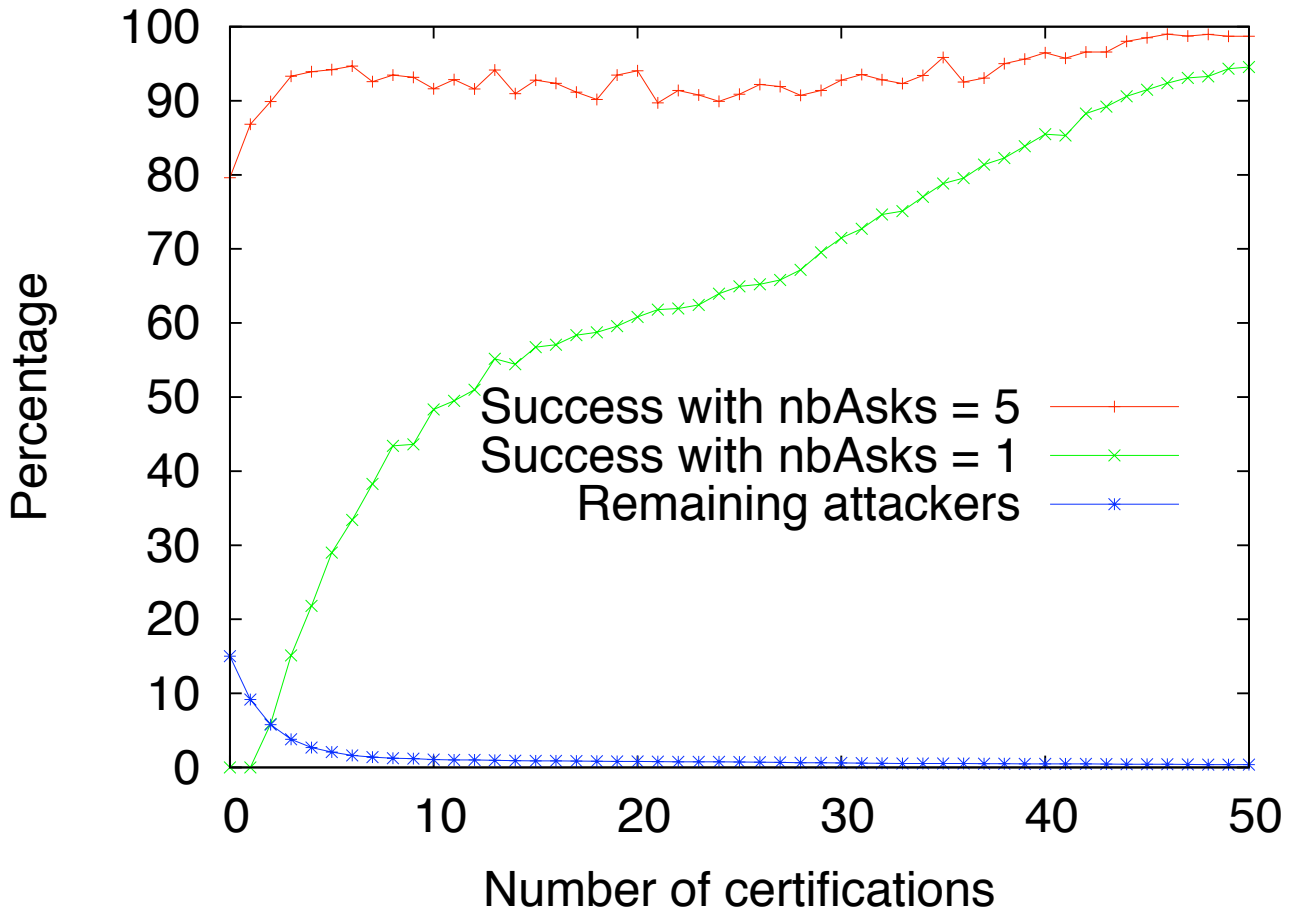


Percentage of honest nodes excluded



15% of attackers

Percentage of Success of Certification Algorithm



5000 nodes, 15% of attackers

Detecting and Excluding Misbehaving Nodes

- Misbehaviors are detected using comparison to other nodes
- Attackers are excluded using revocation and publication
- Sound in the expected case

We are now looking further on this DHT use-case...

Detecting and Excluding Misbehaving Nodes in a P2P Network

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong
firstname.lastname@supelec.fr

Supélec, SSIR Group (EA 4039)

I^{2}CS, June 2008
Schoelcher, Martinique