GRC GRUPO DE REDES DE COMPUTADORES

UNIVERSIDAD POLITECNICA DE VALENCIA

A Collaborative Bayesian Watchdog for Detecting Black Holes in MANETs

IDC 2012

Enrique Hernández Orallo

Index

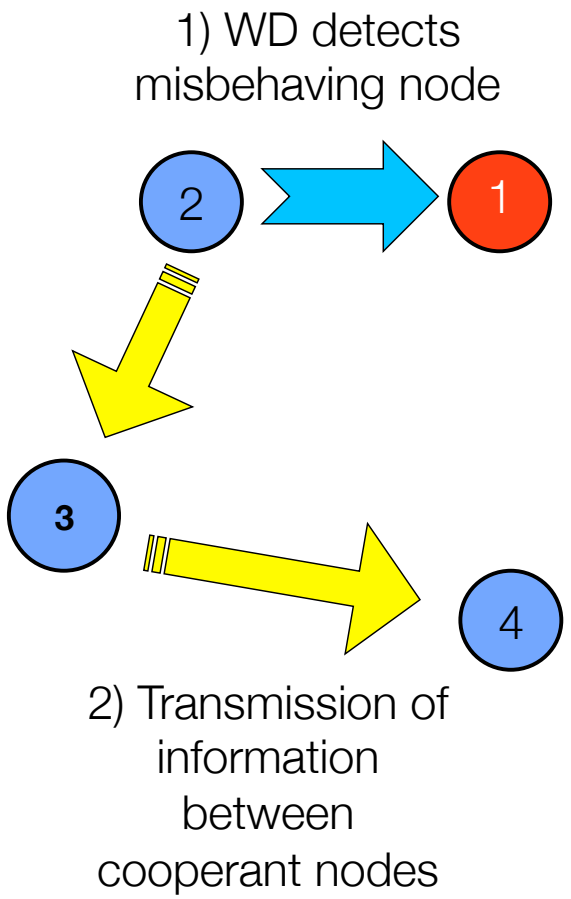
- Index
  - Introduction
  - Our approach
  - Simulation Results
  - Analytical model
  - Conclusions

Introduction

- Goal
  - Improve the detection speed and accuracy of black hole nodes (misbehaving nodes) in a MANET (or DTN).
- Importance?
  - Misbehaviour: nodes refuse to forward other nodes' packets (black hole nodes).
    - Potentially, it could partition the network and seriously degrade its performance.
  - Increasing speed detection and accuracy results in a lower risk of network degradation in presence of a significant number of black holes

Introduction

- Scenario
  - MANET (or DTN) with an undefined number of cooperant and misbehaving nodes.
  - All cooperant nodes have a watchdog
  - Local watchdog detects (or not) misbehaving nodes (a POSITIVE)
  - Detection could not be accurate
  - Information about neighbouring nodes is transmitted between cooperant nodes.



Introduction

- A Watchdog...
  - Overhears wireless channel
  - Analyzes traffic to identify misbehaving nodes
  - Performs actions to cope with these misbehaviours
- Problems/challenges?
  - **Accuracy** (high level of false positives and false negatives), due to noisy channel and nodes' speed
  - **Detection delay**: amount of packets needed to assess a node's reputation → it also depends on the number of packets transmitted and the amount of misbehaving nodes

Index

- Index
  - Introduction
  - **Our approach**
  - Simulation Results
  - Analytical model
  - Conclusions

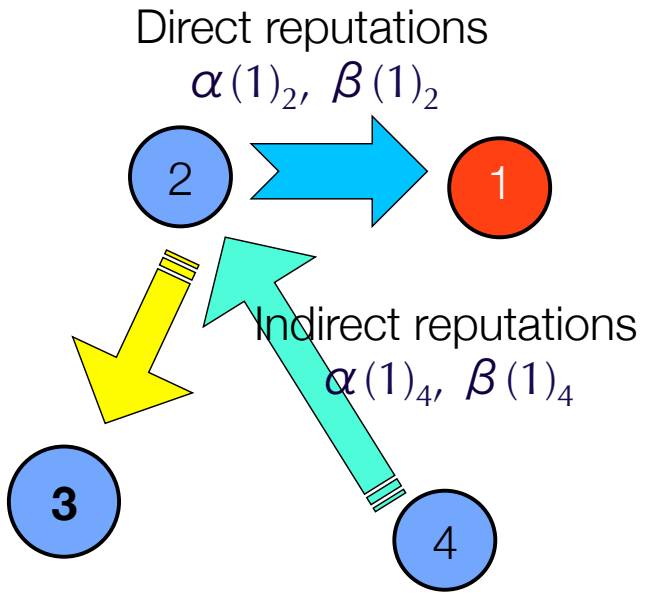
Our approach

- Starting Point: Bayesian Watchdog
  - Previous work from our group
  - Uses a bayesian filter to analyze data captured by every individual watchdog to obtain reputations of its neighbouring nodes
    - Single approach: one node, one independent diagnostic about a suspect node
  - Based on an uncertainty function whose parameters α, β represent node reputation.
    - If the relationship between α and β exceeds a predefined tolerance level, the watchdog identifies that node as malicious
  - Results obtained through simulation: increases accuracy and detection speed compared to standard watchdogs
- Next step: collaboration between watchdogs

GRC GRUPO DE REDES DE COMPUTADORES

Our approach

- Collaborative Bayesian Watchdog
  - Watchdogs analyze 'first-hand' information to obtain direct reputations (α, β)
  - Sharing these reputations between cooperant nodes provides 'second-hand' information, obtaining indirect reputations (α', β')
  - Confidence on cooperant nodes is also taken into account, modulating detection results (the δ value)



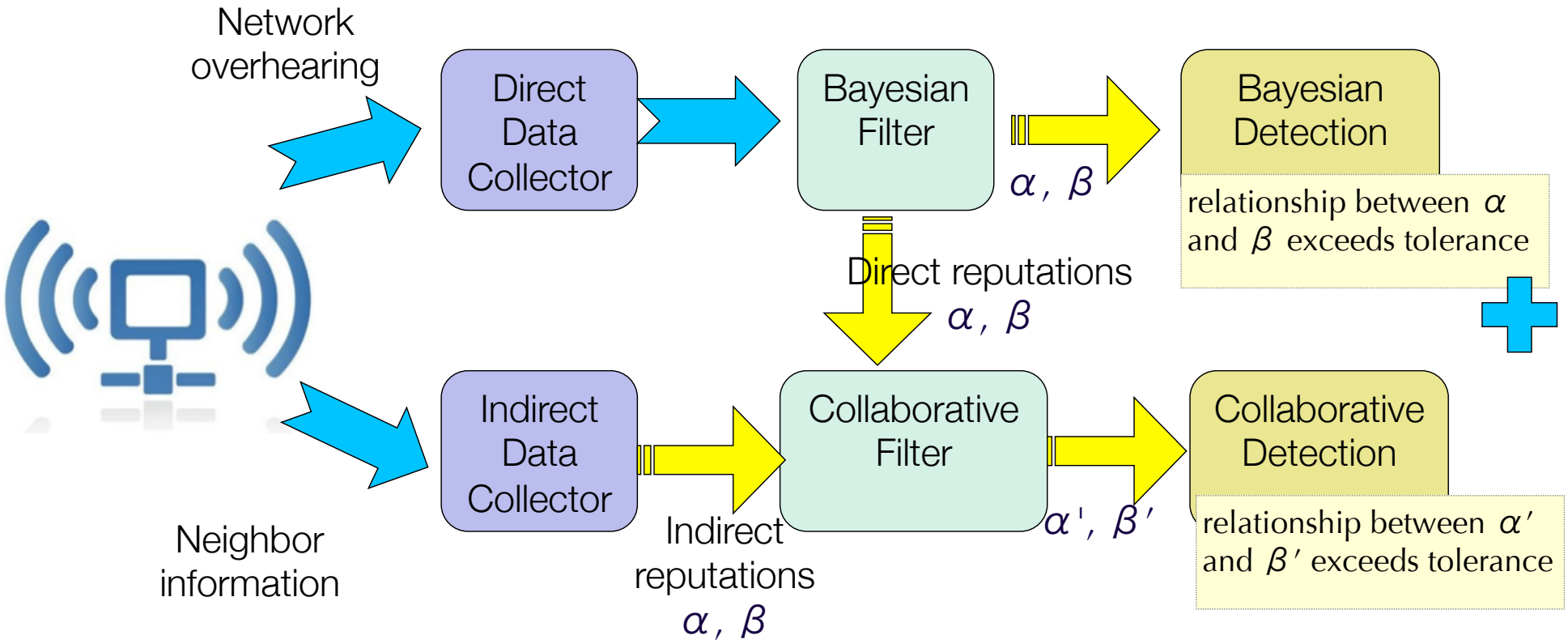
$$\alpha(1)'_2 = \frac{\alpha(1)_2 + \delta \cdot mean(\alpha(1)_j)}{2}$$
$$\forall j \neq 2 \quad (neighbours)$$

Cooperant

Black hole nodes

Our approach

- Implementation of collaborative watchdog



Index

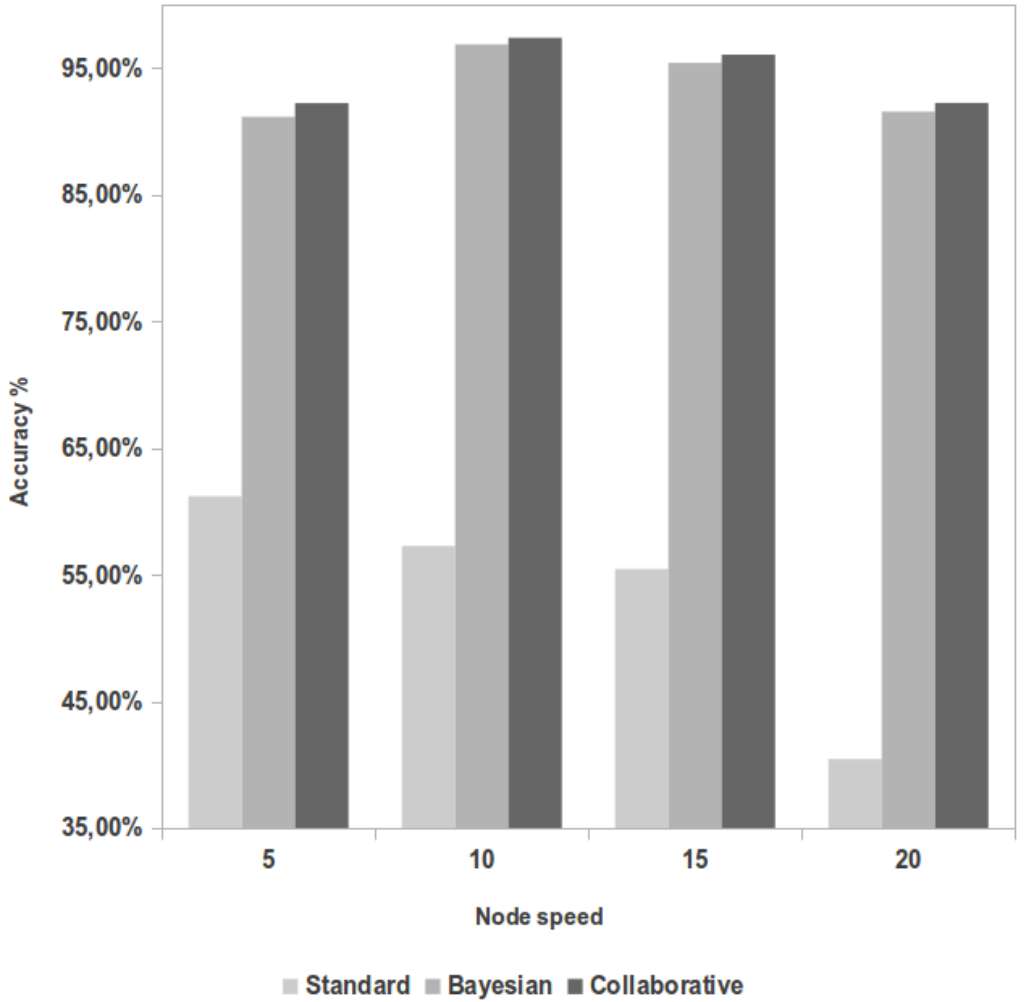
- Index
  - Introduction
  - Our approach
  - **Simulation Results**
  - Analytical model
  - Conclusions

Results

- Experiment based on ns-2 simulator
  - We implemented the Collaborative Bayesian Watchdog as a module.
- Simulation Environment
  - Mixed UDP Unicast CBR and UDP broadcast traffic patterns
  - 50 nodes
  - 10% of black holes
  - Node speed from 5 m/s to 20 m./s.
  - Simulation area 1000x1000 m.
  - Confidence on indirect reputations: 80% ($\delta=0.8$)

Results

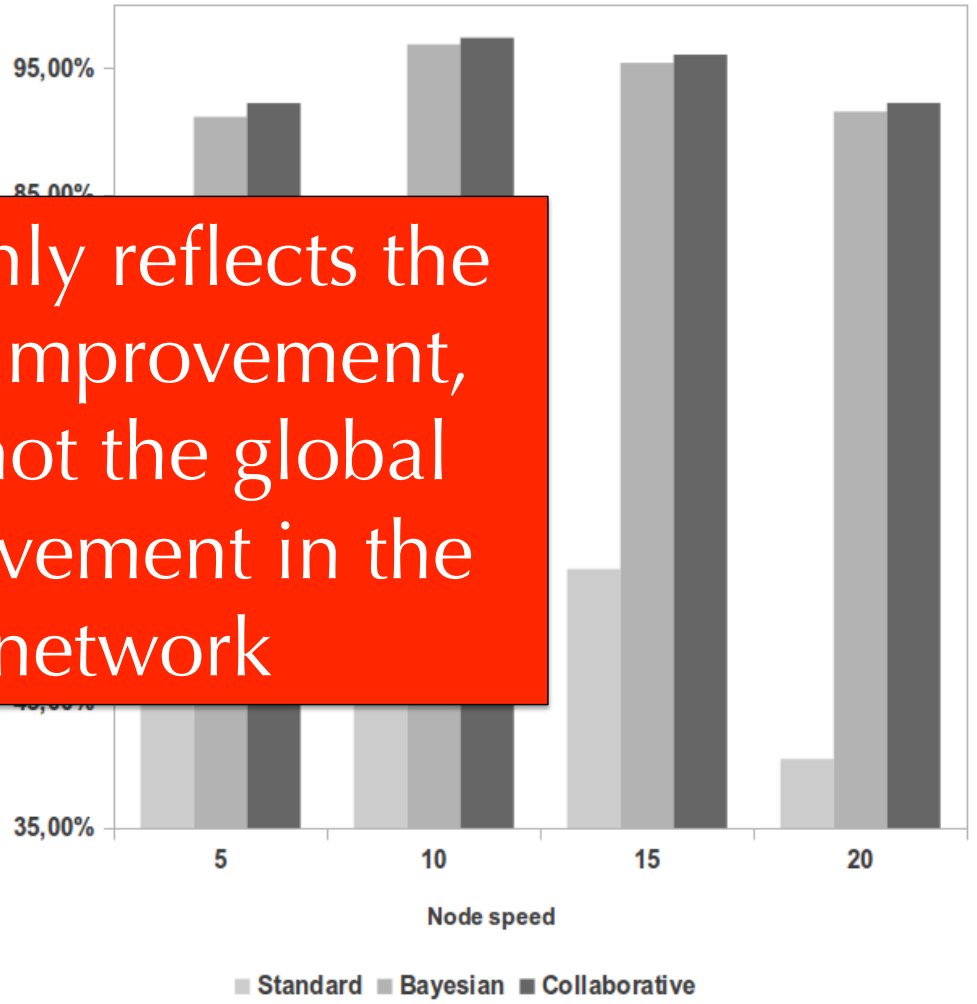
- Detection speed
  - In average, earlier in more than 7% of the cases
- Accuracy
  - 1,78% of black holes nodes detected only by the Collaborative Bayesian Watchdog



GRC GRUPO DE REDES DE COMPUTADORES

Results

- Detection speed
  - In average, earlier in more than 7% of the cases
- Accuracy
  - 1,78% of black nodes detected the Collaborativ Bayesian Watchdog



This only reflects the local improvement, and not the global improvement in the network

GRC GRUPO DE REDES DE COMPUTADORES

Index

- Index
  - Introduction
  - Our approach
  - Simulation Results
  - **Analytical model**
  - Conclusions

Analytical model

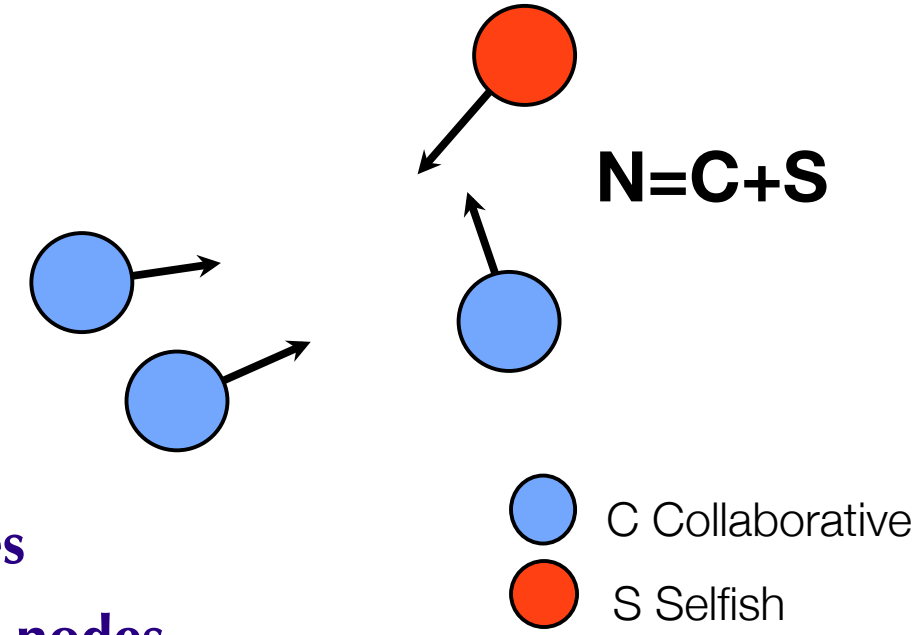
- Basic model
  - N wireless mobile nodes

    C collaborative nodes

    S misbehaving nodes
  - Goal:

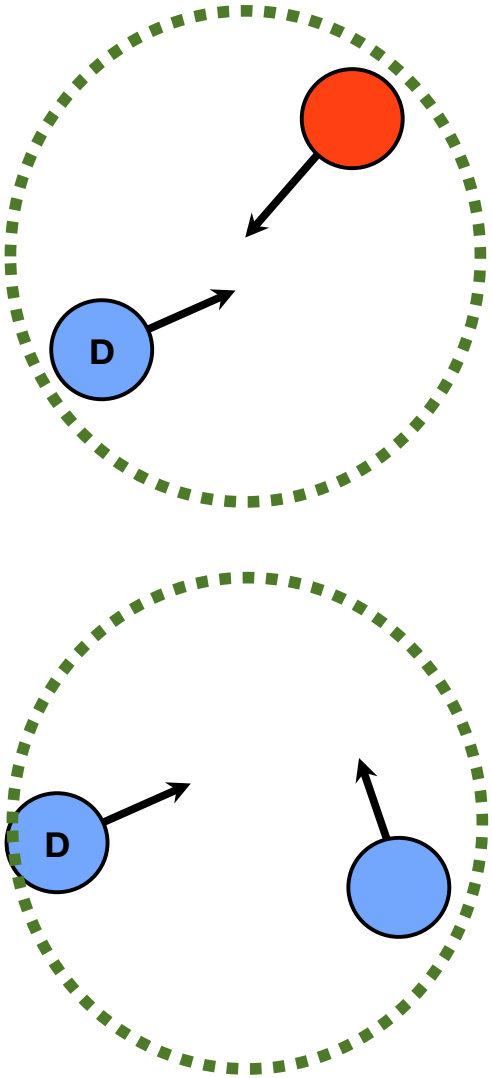
    Obtain time and cost all nodes

    knows about the misbehaving nodes
    - Contact rate follows Poisson distribution λ
- Model based in a CTMC (Continuous time Markov Chain)



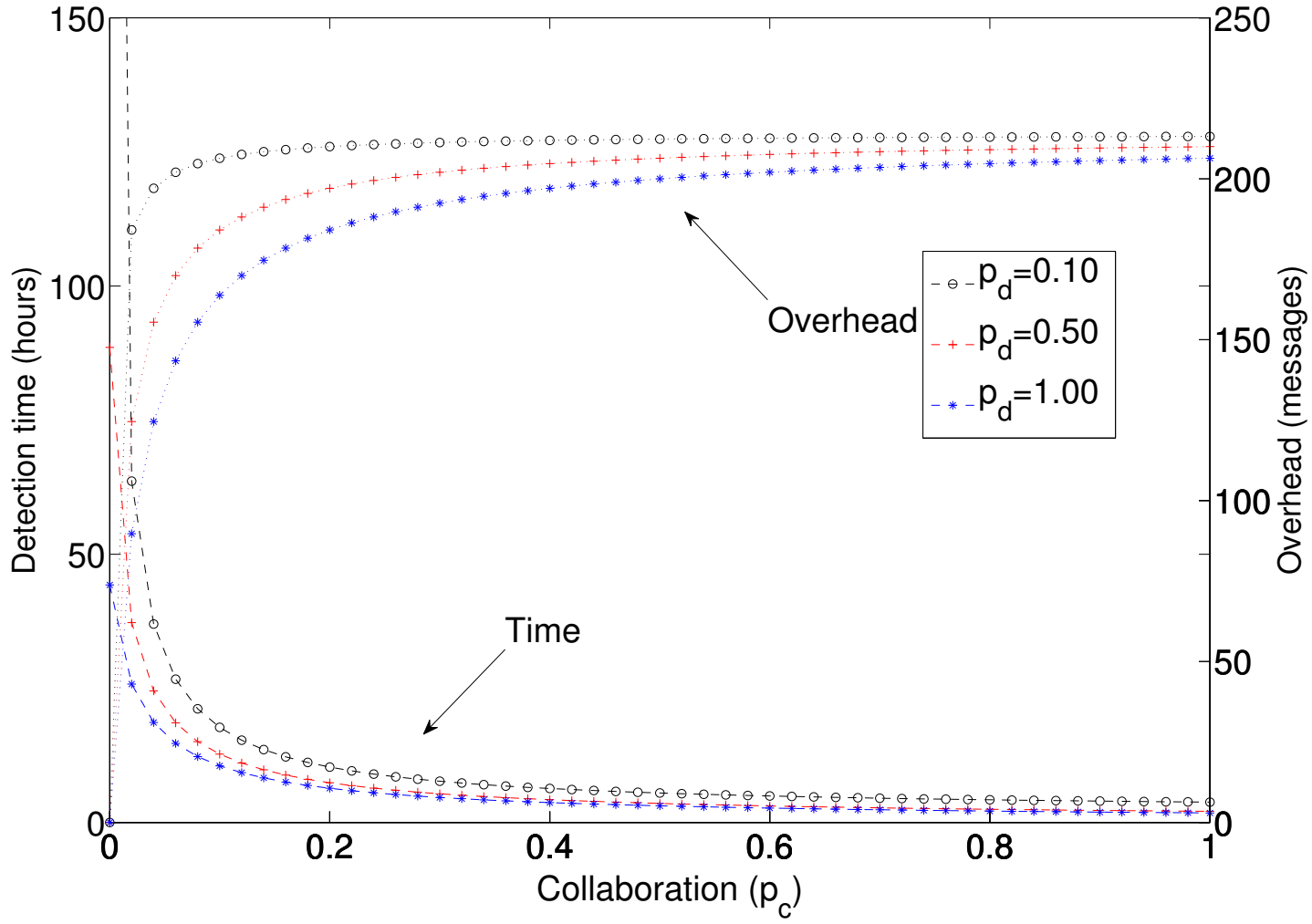
Analytical model

- The model take into account two cases:
  - Case a: One of the nodes is a misbehaving node.
    - Detection using watchdog
    - We model the case of detection using the probability of detection (p_d).
  - Case b: Both nodes collaborative.
    - If one node knows the misbehaving node it transmits this information
    - We model the degree of collaboration (0: no collaboration, 1: full collaboration) as the probability of collaboration (p_c)



Analytical model

- Influence of collaboration (N=50, $\lambda = 2.81 \times 10^{-5} s^{-1}$)



Index

- Index
  - Introduction
  - Our approach
  - Simulation Results
  - Analytical model
  - **Conclusions**

Conclusions

- We have introduced a new approach to detect misbehaving nodes using collaborative watchdogs.
- Simulation results show that our approach improves detection speed of black holes, and slightly increases the accuracy of that detection process.
- Analytical results show that the collaborative watchdog can reduce the overall detection time with a reduced overhead (messages cost).
  - This reduction is very significant when the watchdog detection effectiveness is low.
  - Furthermore, this reduction can be obtained even with a moderate degree of collaboration