

## SSTIC 2006

# Mécanismes de sécurité et de coopération entre nœuds d'un réseaux mobile ad hoc

Pietro Michiardi – Institut Eurecom

# Outline

- Trust in MANET
- Cooperation enforcement
- CORE
  - Sketch of the protocol
  - Simulations
- Analytical validation
  - Application of game theory

# Trust in MANET

- Managed environment
  - A-priori trust
  - Entity authentication → correct operation
  - But:  
requirement for authentication infrastructure
- Open environment
  - No a-priori trust
  - Authentication does not guarantee correct operation
  - *New security paradigm*

# Threats in MANET

## Passive: Selfish Nodes

- Do not cooperate
- Priority: battery saving
- No intentional damage to other nodes
- **Exposure:**
  - Selfish forwarding
  - Selfish routing

## Active: Malicious Nodes

- Goal: damage other nodes
- Battery saving is not a priority
- **Exposure:**
  - Denial of service
  - Traffic subversion
  - Attacks on vulnerable mechanisms
  - ...

# MANET Requirements

- Wireless & Mobile
  - Limited energy
  - Lack of physical security
- Ad hoc
  - No infrastructure
  - Lack of organization
- Cooperation enforcement
- Secure Routing
- Key Management

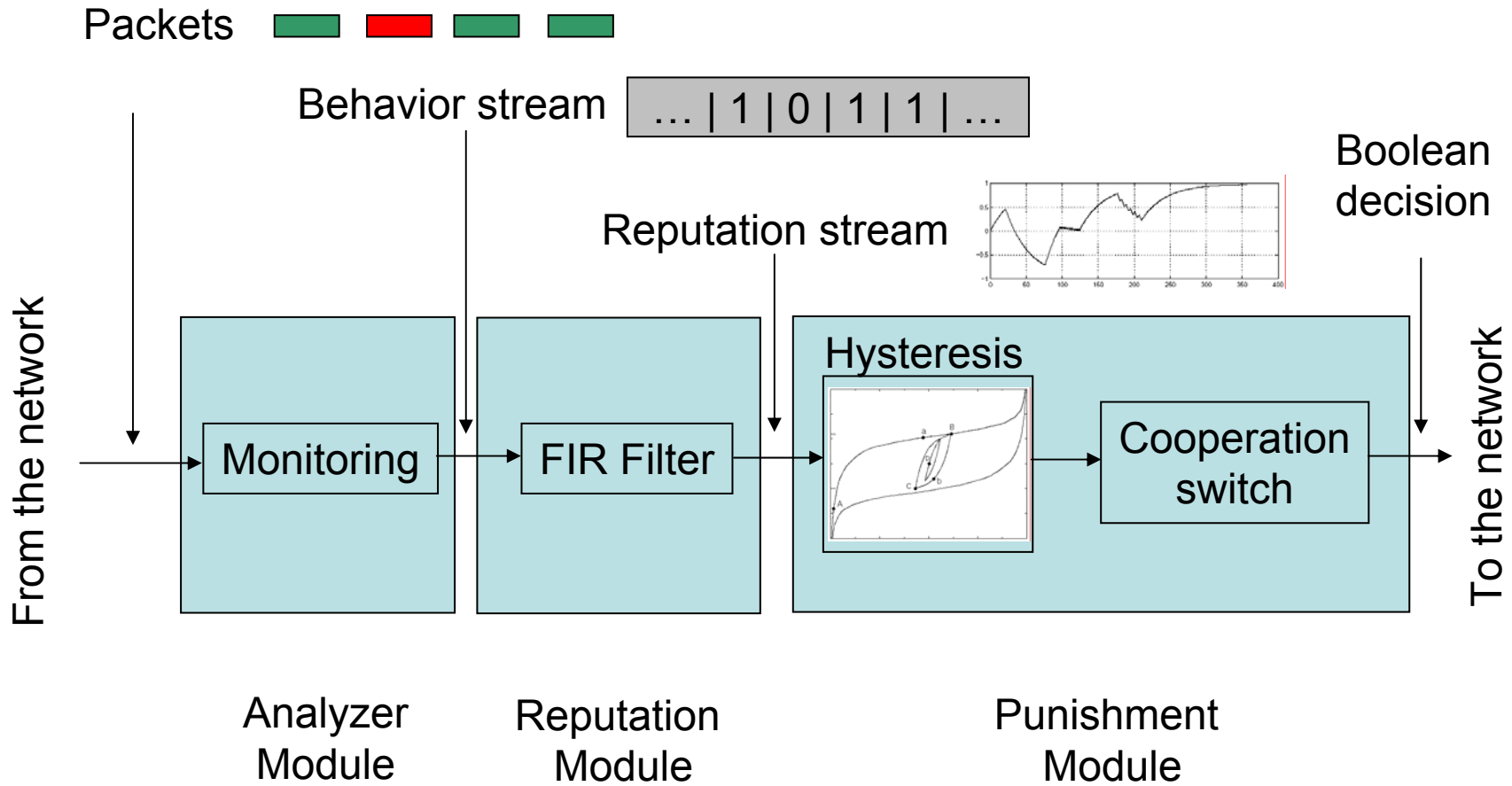
# Cooperation Enforcement in MANET

- Routing and Packet Forwarding **cost energy**
- Selfish nodes save energy for self-interested purposes
- Without any incentive for cooperation network performance can be severely degraded

# Cooperation Enforcement in MANET

- CORE: reputation based cooperation enforcement
- Key idea: bind network utilization and reputation metric
- Reputation **not** used as additional metric for routing
- Other approaches:
  - credit based systems (micro payment)
  - token based systems (threshold cryptography)
  - Mitigating routing misbehavior (reputation as routing metric)

# Sketch of CORE



# CORE Components

- **Analyzer Module**
  - Based on the watchdog (WD) technique
  - Extension: variation of the WD frequency based on local reputation
- **Reputation Module**
  - Subjective, Indirect (optional) and Functional reputation values are combined with dynamic weights
  - Reputation algorithm:
    - FIR  $B$ -order filter: initially low-pass, can be more complex (“signatures”)
    - Sliding-window of size  $B$
- **Punishment Module**
  - Packets from selfish sources are dropped (deals also with selective misbehavior)
  - Alternatives:
    - Path rater technique, BUT additional node re-integration mechanism
    - Cross-layer punishment: restrict application capabilities (P2P query limits)

# Validation of CORE

- Difficulty raised by reputation-based mechanism
- Our approaches:
  - **Simulation-based validation**
    - $\Rightarrow$  Proof of concept
    - $\Rightarrow$  Realistic measurements: energy, traffic, ...
  - **Analytical model of MANET** and node behavior
    - $\Rightarrow$  Realistic model of selfishness
    - $\Rightarrow$  Infer incentive-compatibility properties of CORE

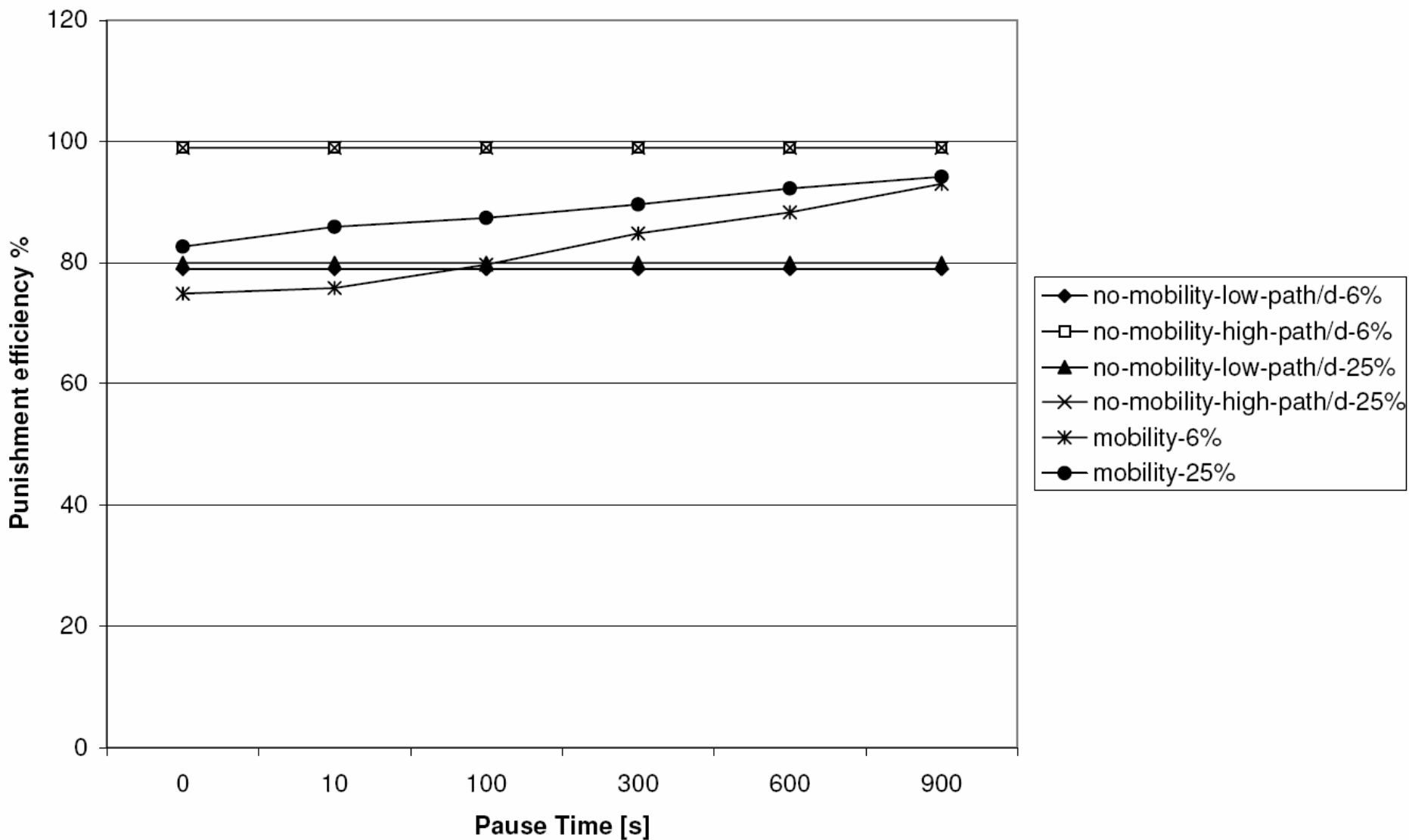
# Simulation-based validation

- **Simulation set-up**
  - Static and Dynamic Network
    - Random waypoint model (no 0 m/s!)
  - Parameters
    - Pause time, % of selfish nodes, “path diversity”
- **Simulation metrics**
  - Energy consumption
  - Punishment efficiency
  - False positives
- **Basic CORE implementation**
  - Monitoring active only for packet forwarding
  - No reputation information distribution: **no control traffic overhead**
- **Selfishness models**
  - Selfish nodes systematically fail to forward packets

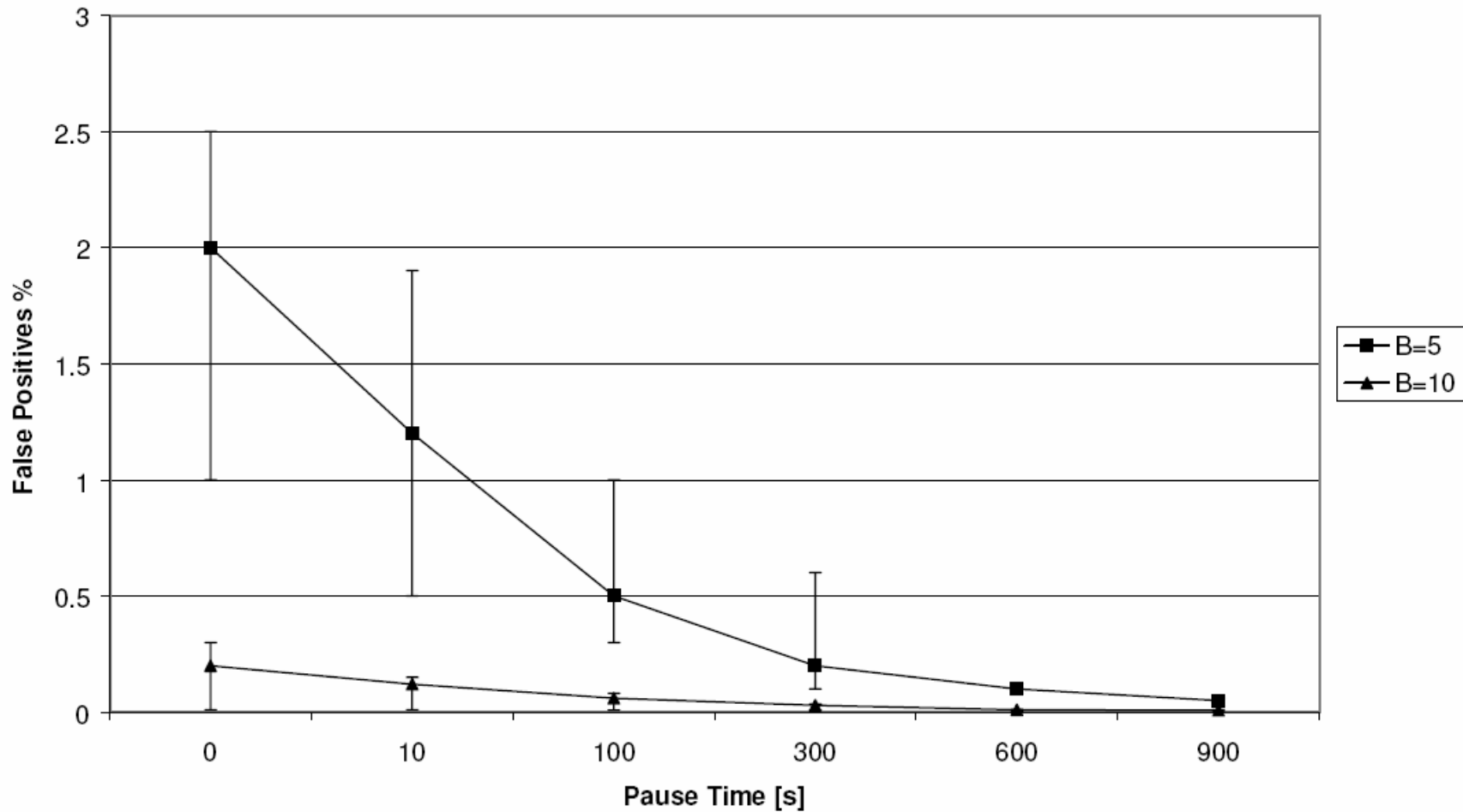
# Simulation results

- CORE-enabled legitimate nodes save up to 24% of energy  $\Rightarrow$  **legitimate nodes are better off using CORE**
- Punishment efficiency ranges from 80% to 100%, WITHOUT reputation distribution  $\Rightarrow$  **selfish nodes have strong incentive to cooperate** if they want to use the network
  - Distributing reputation is worthless and **unreliable**
  - Further improvements possible using multi-path routing
- False positives are reasonably low
  - Simple example: reputation algorithm = sliding-window of size  $B$ , doubling  $B$  cuts by order of 10 false positives (from 2% to 0.2%)

## Punishment Efficiency N=16 S={6,25}%



False Positives,  $N=16$   $S=\{6,25\}\%$   
Observation buffer size = B  
Mobility=ON



# Limitation of network simulation

- Selfishness models are **STATIC**
  - Also in related work!
- Need for analytical framework to model **DYNAMIC** selfish behavior
- Game theory offers tools to model *strategic interaction* among *rational* selfish players

# Game Theoretical Validation

- Basic model: non-cooperative game theory
- Packet forwarding as a Prisoner's Dilemma:
  - Players: random pair in the set  $\{1, \dots, N\}$  nodes of the network
  - Strategy:  $\{C, D\}$  / C=forward, D=drop packet
  - Payoff matrix  $\equiv$  utility function (example)

		Player j	
		Cooperate	Defect
Player i	Cooperate	(3,3)	(-2,4)
	Defect	(4,-2)	(-1,-1)

# Repeated game theory

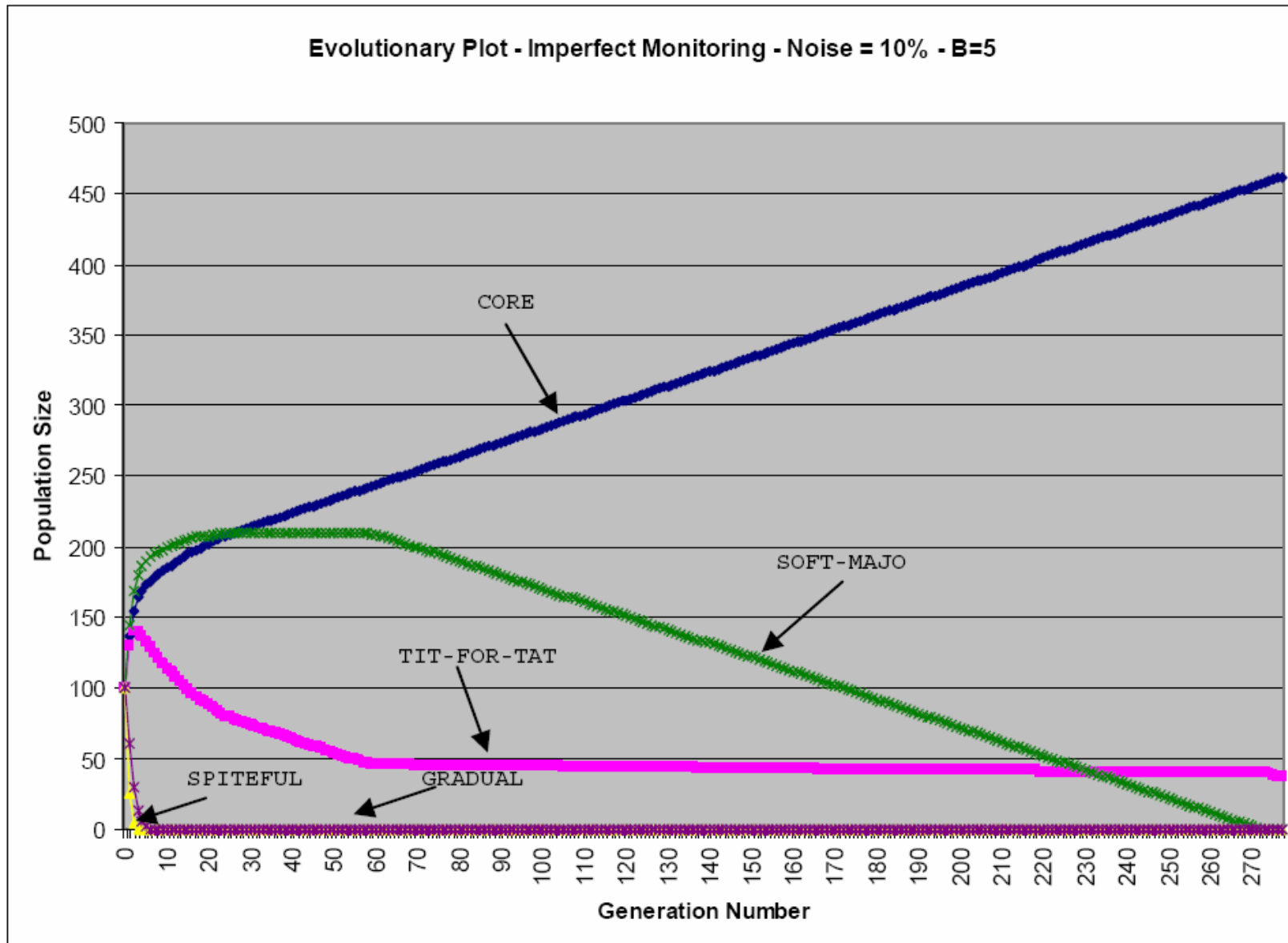
- Fine-grained modeling of CORE's reputation algorithm through iterated games
  - Players do not know when the game will end
  - **SHADOW OF THE FUTURE**
- **Important extension to the basic model**
  - Representation of MAC layer failures (interference, collisions, etc.) that affect the *watchdog mechanism*
- Comparison with alternative strategies: tit-for-tat (TFT), generous TFT (G-TFT), spiteful, gradual, ...

# Evolutionary game theory

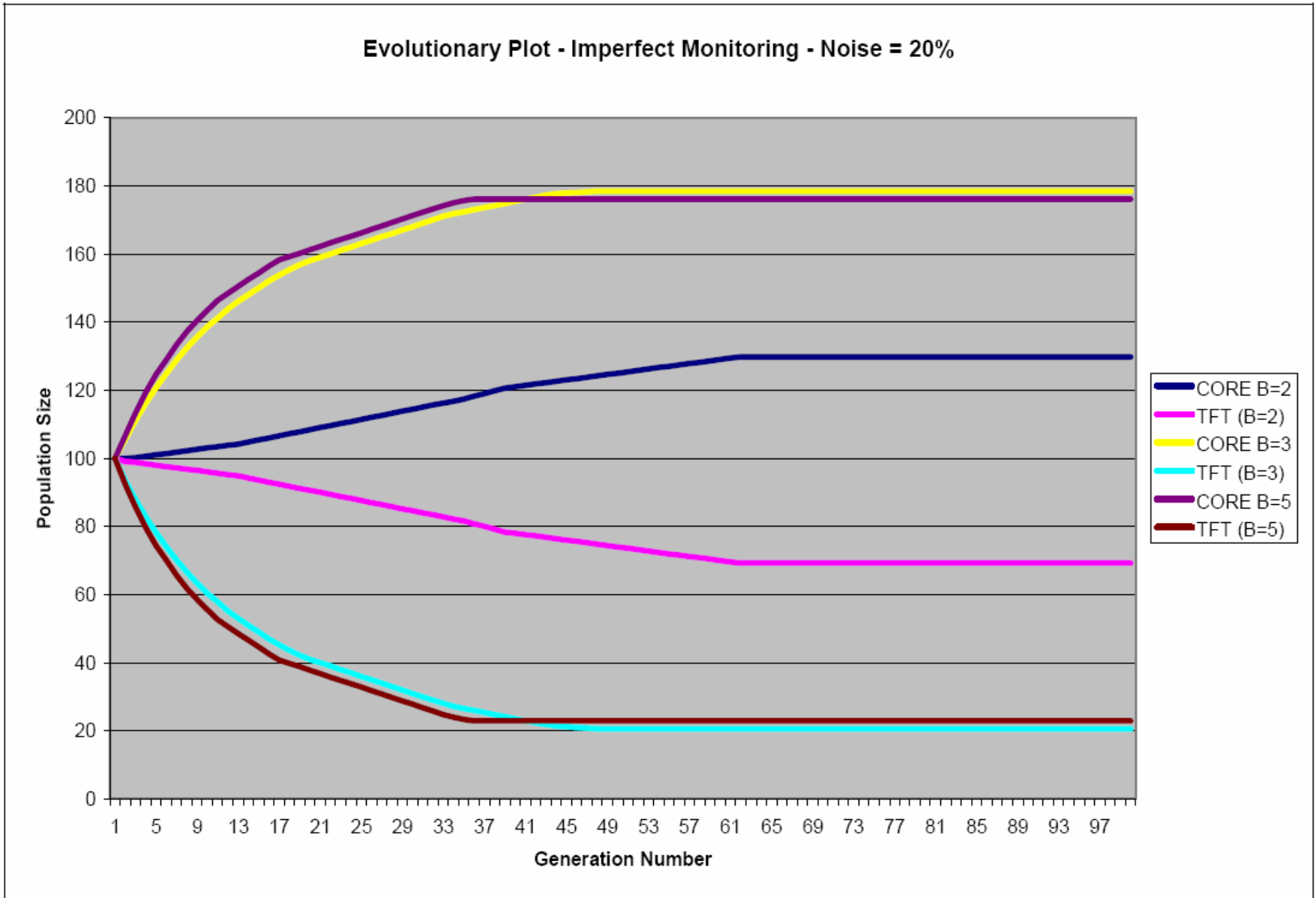
- Numerical validation to study robust and stable cooperation strategy (Genetic Algorithms Approach)
  - START: equal partitioning of population into each competing strategy
  - ITERATION: round robin tournament  
Population of bad strategies is decreased whereas good strategies obtain new elements
  - END: population is stable
- Perfect vs. Imperfect private monitoring
  - *Misperception noise* used to model **watchdog mechanism failures**

# Results

- With perfect monitoring
  - CORE and Tit-For-Tat are in equilibrium
- With imperfect monitoring
  - **CORE outperforms** other strategies because of ***reputation***
    - TFT, G-TFT unstable due to errors
    - Reputation buffer (B) size directly proportional to convergence speed



**Evolutionary Plot - Imperfect Monitoring - Noise = 20%**



# Limitations of basic model

- Network topology is not taken into account
  - Only random pair-wise node interaction
- Coalitions and group dynamics are not considered
- Further work not presented today:
  - Cooperative game theory
    - Study the **size** ( $k$ ) of a **coalition** of cooperating nodes
    - Nash Equilibrium → lower bound on  $k$
    - **CORE as a Coalition Formation Algorithm**
  - Non-cooperative forwarding
    - Study the impact of **network topology** on equilibrium strategies

# CORE summary

- Lightweight approach
  - CORE execution consumes little energy
  - Nodes that use CORE consume less than nodes that do not use CORE
- No traffic overhead
  - No reputation distribution
- Effective in presence of misperception
- Robust against attacks
- CORE principles can be extended to higher layers
  - Service discovery
  - Overlay network formation
  - ...