Security and Privacy in Wireless Networks

Mohammad Hossein Manshaei
manshaei@gmail.com

Chapter 9: (secowinet.epfl.ch)

operating principles of IEEE 802.11, detecting selfish behavior in hot spots, and selfish behavior in pure ad hoc networks

SELFISH BEHAVIOR AT THE MAC LAYER OF CSMA/CA

Chapter outline

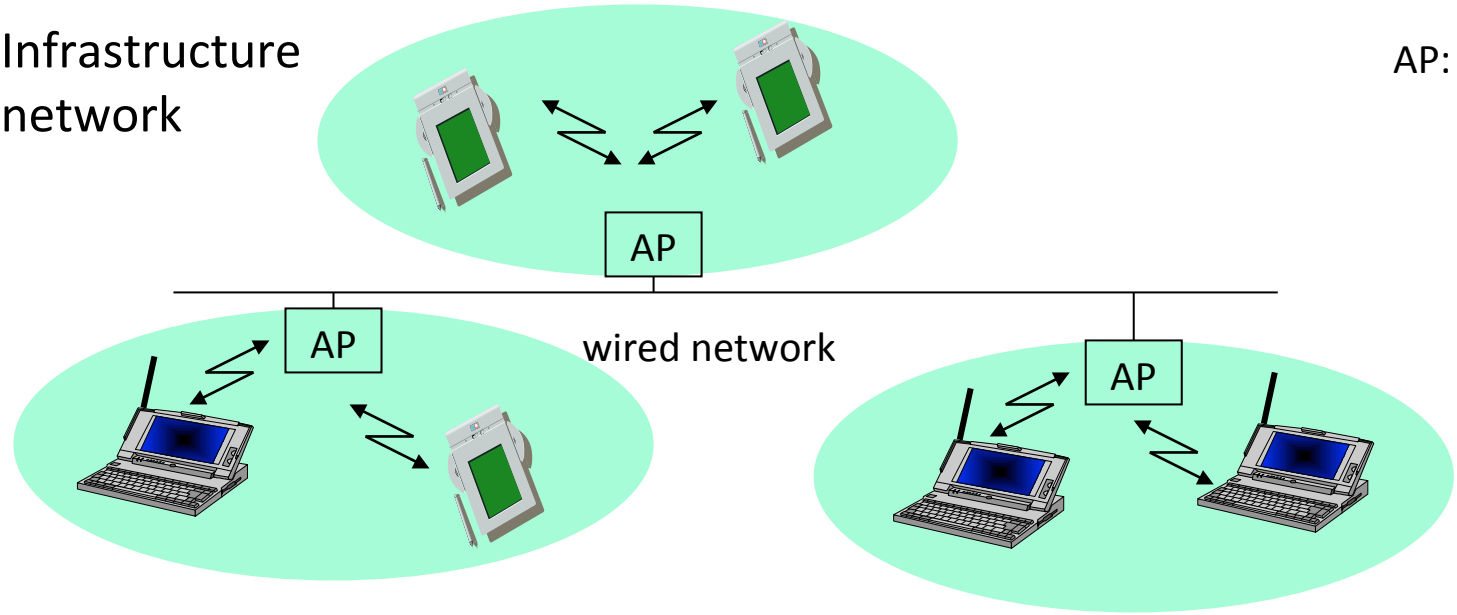
9.1 Operating principles of IEEE 802.11

9.2 Detecting selfish behavior in hotspots

9.3 Selfish behavior in pure ad hoc networks

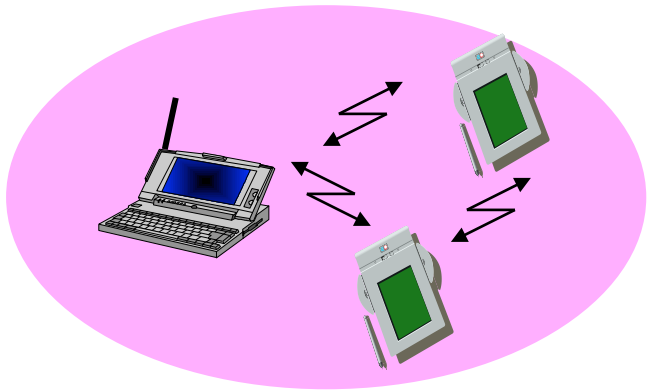
Infrastructure vs. ad hoc networks

Infrastructure network



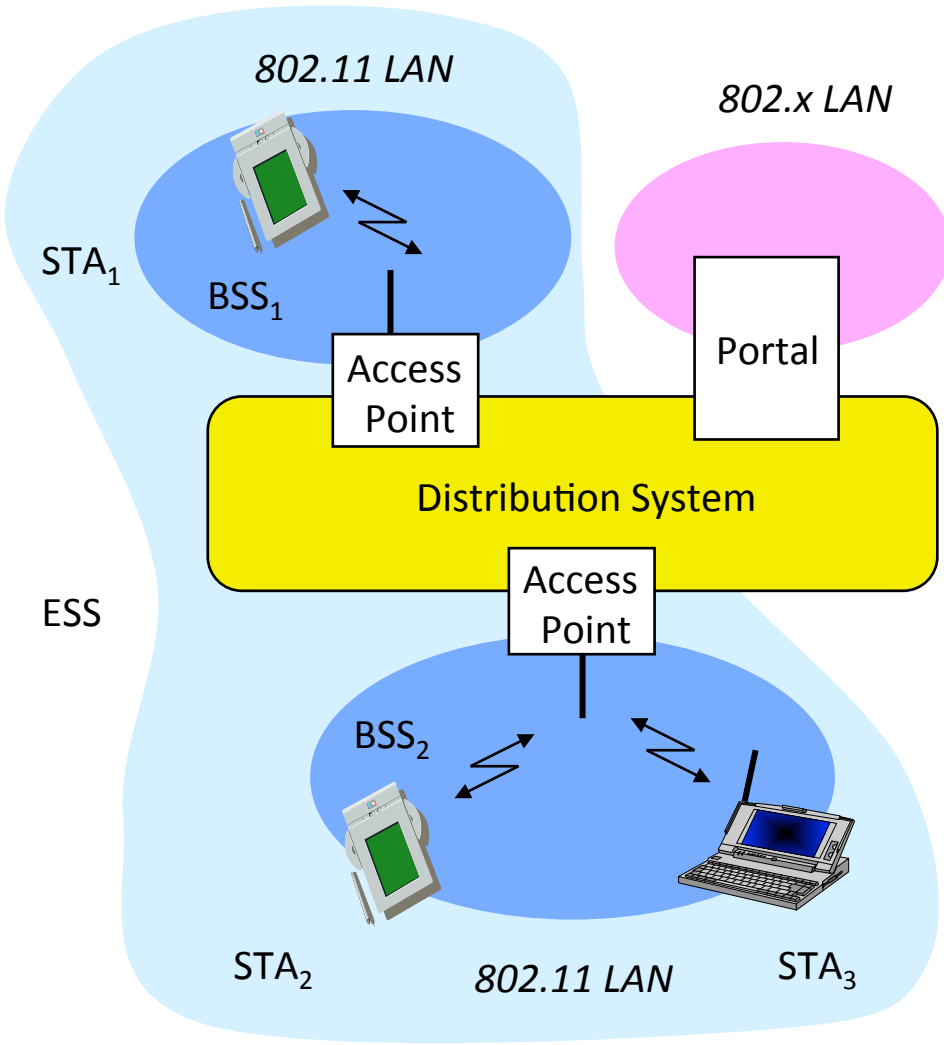
AP: Access Point

Ad hoc network



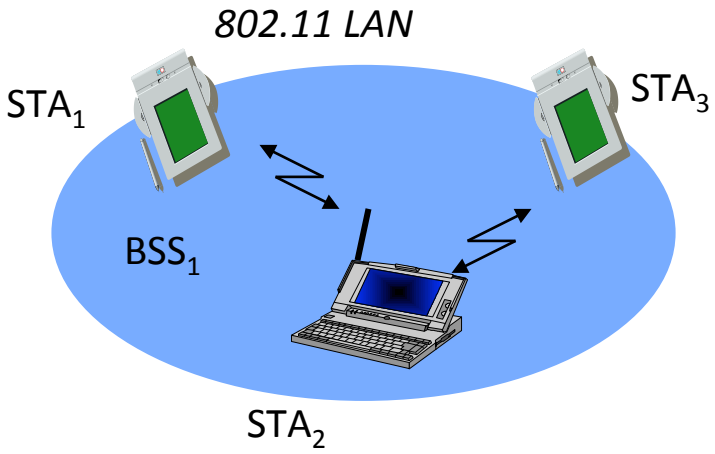
Note: Slides 3 to 14 are derived from the slide show of the book “Mobile Communications” by Jochen Stiller, Addison-Wesley, 2003

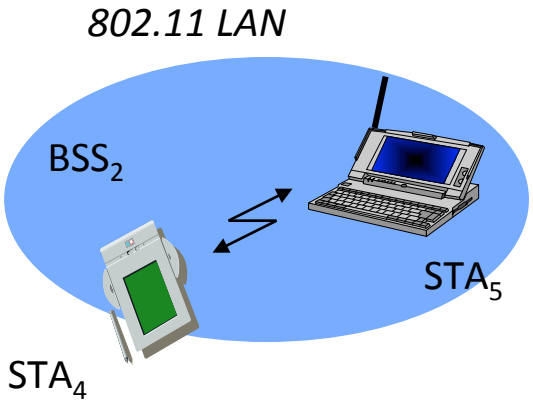
IEEE 802.11 - Architecture of an infrastructure network



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

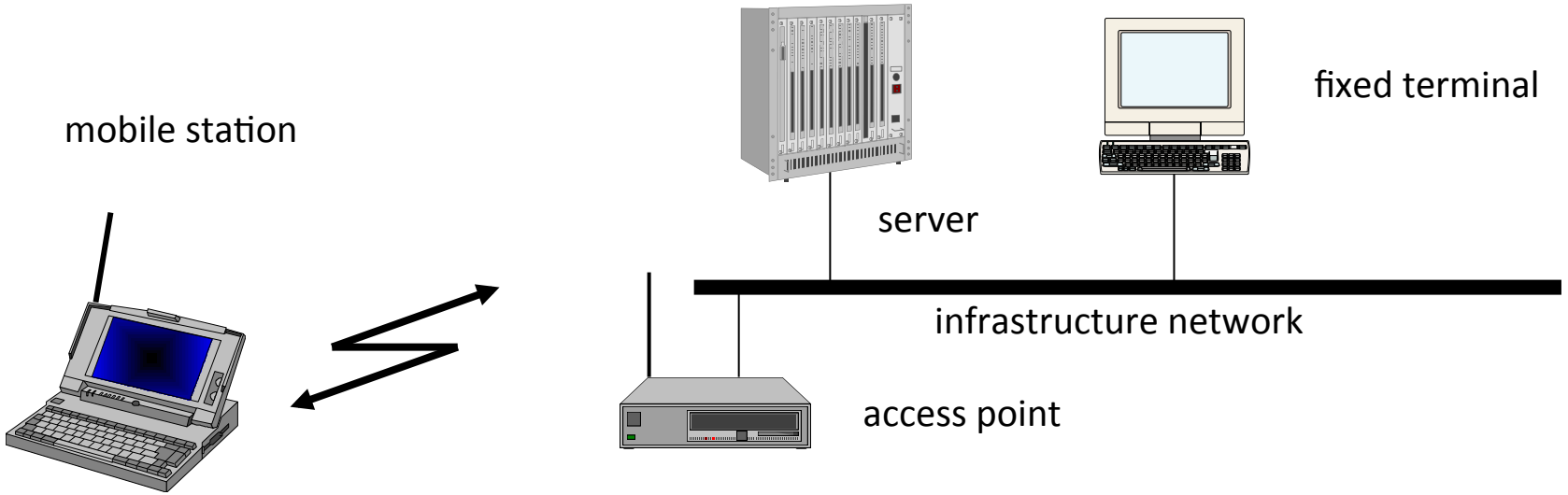
802.11 - Architecture of an ad-hoc network

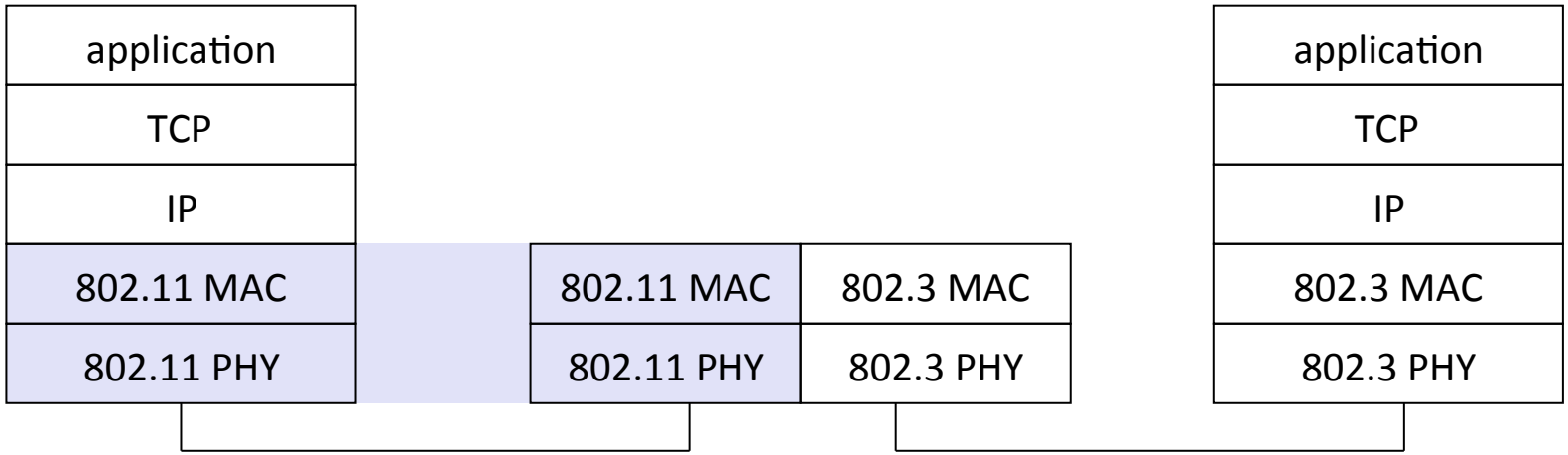




- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

Interconnection of IEEE 802.11 with Ethernet

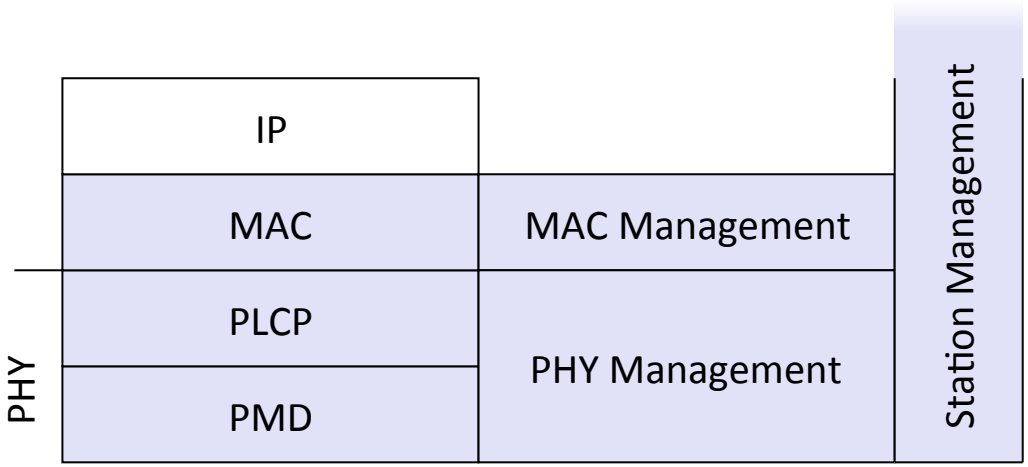




802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management

- PLCP (Physical Layer Convergence Protocol)
  - clear channel assessment signal (carrier sense)
- PMD (Physical Medium Dependent)
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



802.11 - Physical layer

- 3 versions: 2 radio: DSSS and FHSS (both typically at 2.4 GHz), 1 IR
  - data rates 1, 2, 5 or 11 Mbit/s

- **DSSS** (Direct Sequence Spread Spectrum)
  - DBPSK modulation (Differential Binary Phase Shift Keying) or DQPSK (Differential Quadrature PSK)
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

- **FHSS** (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength
  - min. 2.5 frequency hops/s, two-level GFSK modulation (Gaussian Frequency Shift Keying)

- **Infrared**
  - 850-950 nm, diffuse light, around 10 m range
  - carrier detection, energy detection, synchronization

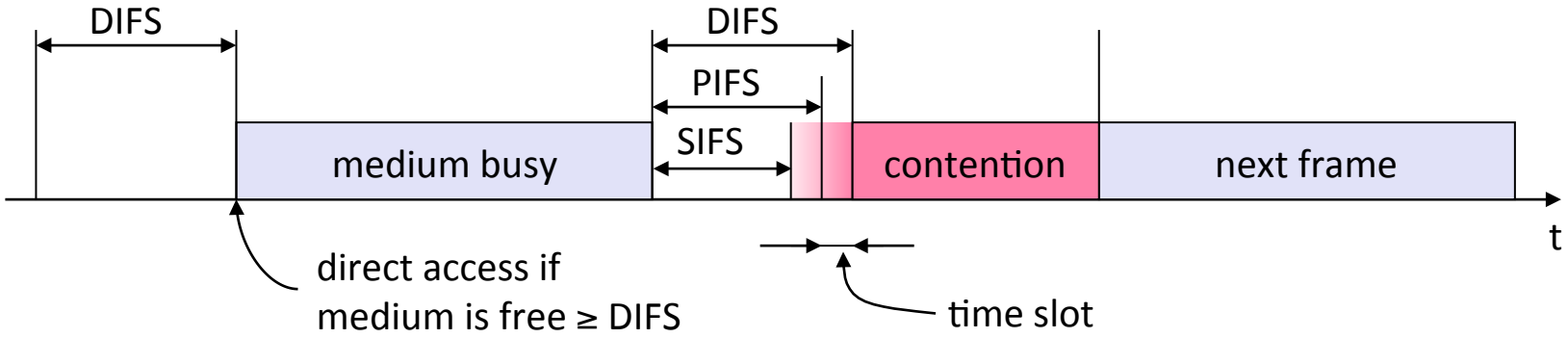
802.11 - MAC layer principles

- Traffic services
  - Asynchronous Data Service (mandatory)
    - exchange of data packets based on “best-effort”
    - support of broadcast and multicast
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)
- Access methods (called DFWMAC: Distributed Foundation Wireless MAC)
  - DCF CSMA/CA (mandatory)
    - collision avoidance via randomized “back-off” mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF with RTS/CTS (optional)
    - avoids hidden terminal problem
  - PCF (optional)
    - access point polls terminals according to a list

- DCF: Distributed Coordination Function
- PCF: Point Coordination Function

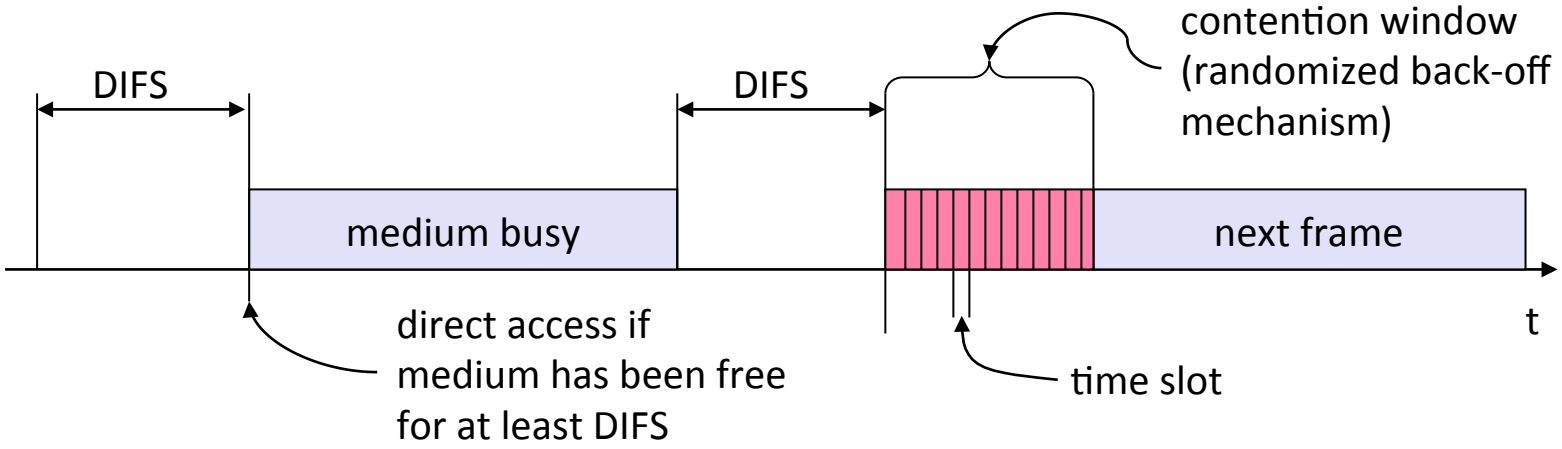
802.11 - MAC layer principles

- Priorities
  - defined through different inter frame spaces
  - no guaranteed, hard priorities
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
  - PIFS (PCF IFS)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF, Distributed Coordination Function IFS)
    - lowest priority, for asynchronous data service



Note : IFS durations are specific to each PHY

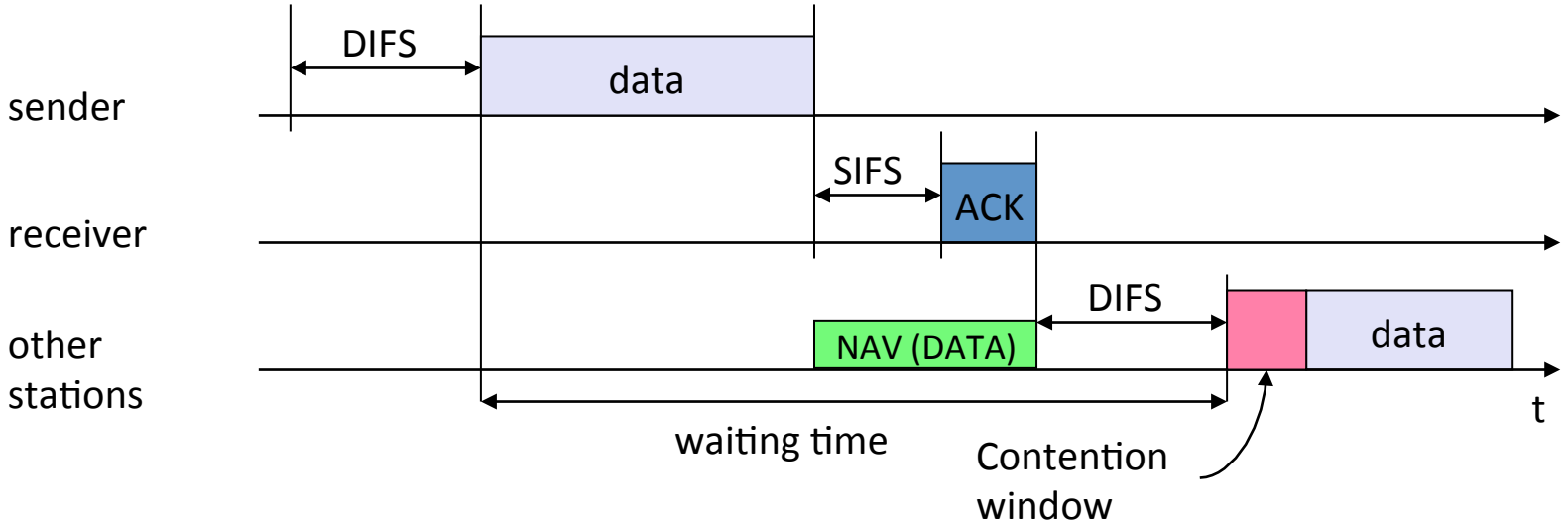
802.11 - CSMA/CA principles



- Station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- If the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- If the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- If another station occupies the medium during the back-off time of the station, the back-off timer stops (to increase fairness)

802.11 - CSMA/CA unicast

- **Sending unicast packets**
  - station has to wait for DIFS before sending data
  - receiver acknowledges at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors

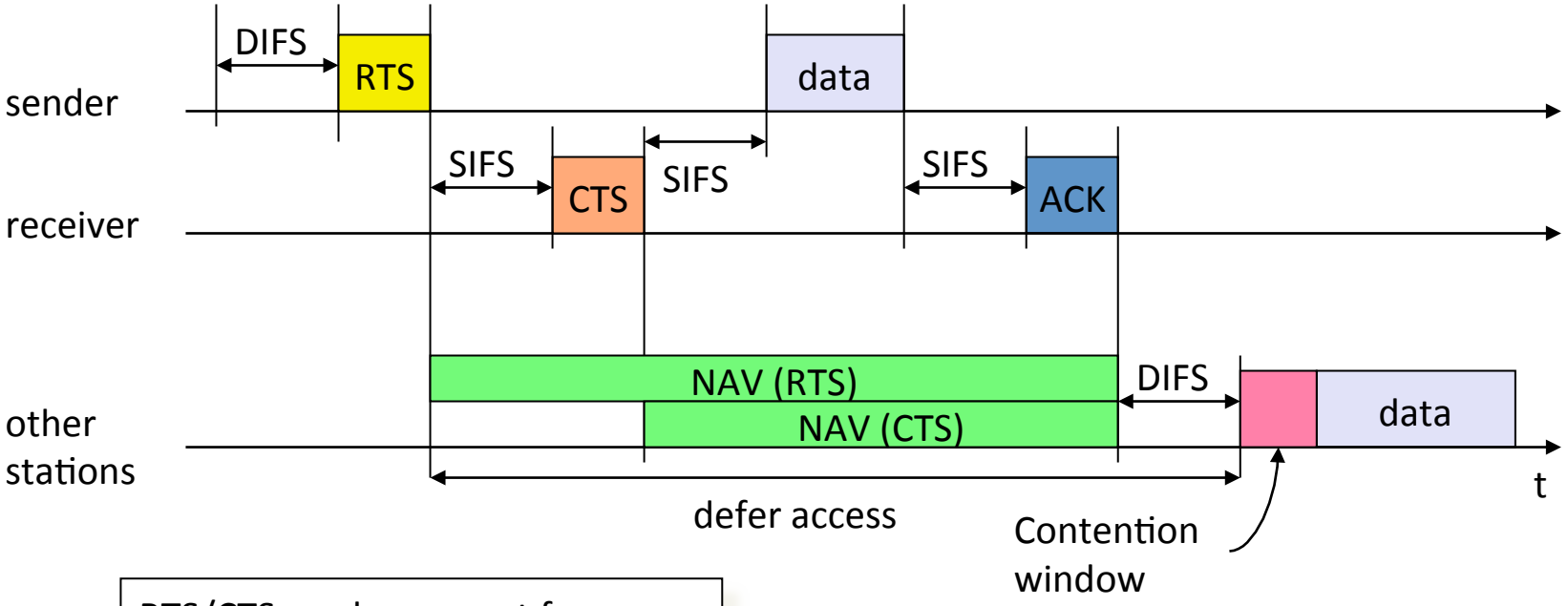


The ACK is sent right at the end of SIFS (no contention)

NAV: Net Allocation Vector

802.11 – DCF with RTS/CTS

- **Sending unicast packets**
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement via ACK
  - other stations store medium reservations distributed via RTS and CTS



RTS/CTS can be present for some packets and not for other

NAV: Net Allocation Vector

Chapter outline

9.1 Operating principles of IEEE 802.11

9.2 Detecting selfish behavior in hotspots

9.3 Selfish behavior in pure ad hoc networks

Section outline

- Motivation
- System model
- Misbehavior techniques
- Components of **DOMINO** (System for **D**etection **O**f greedy behavior in the **M**AC layer of **I**EEE 802.11 public **N**etw**O**rks)
- Simulation
- Implementation
- Related work
- Conclusion

Motivation

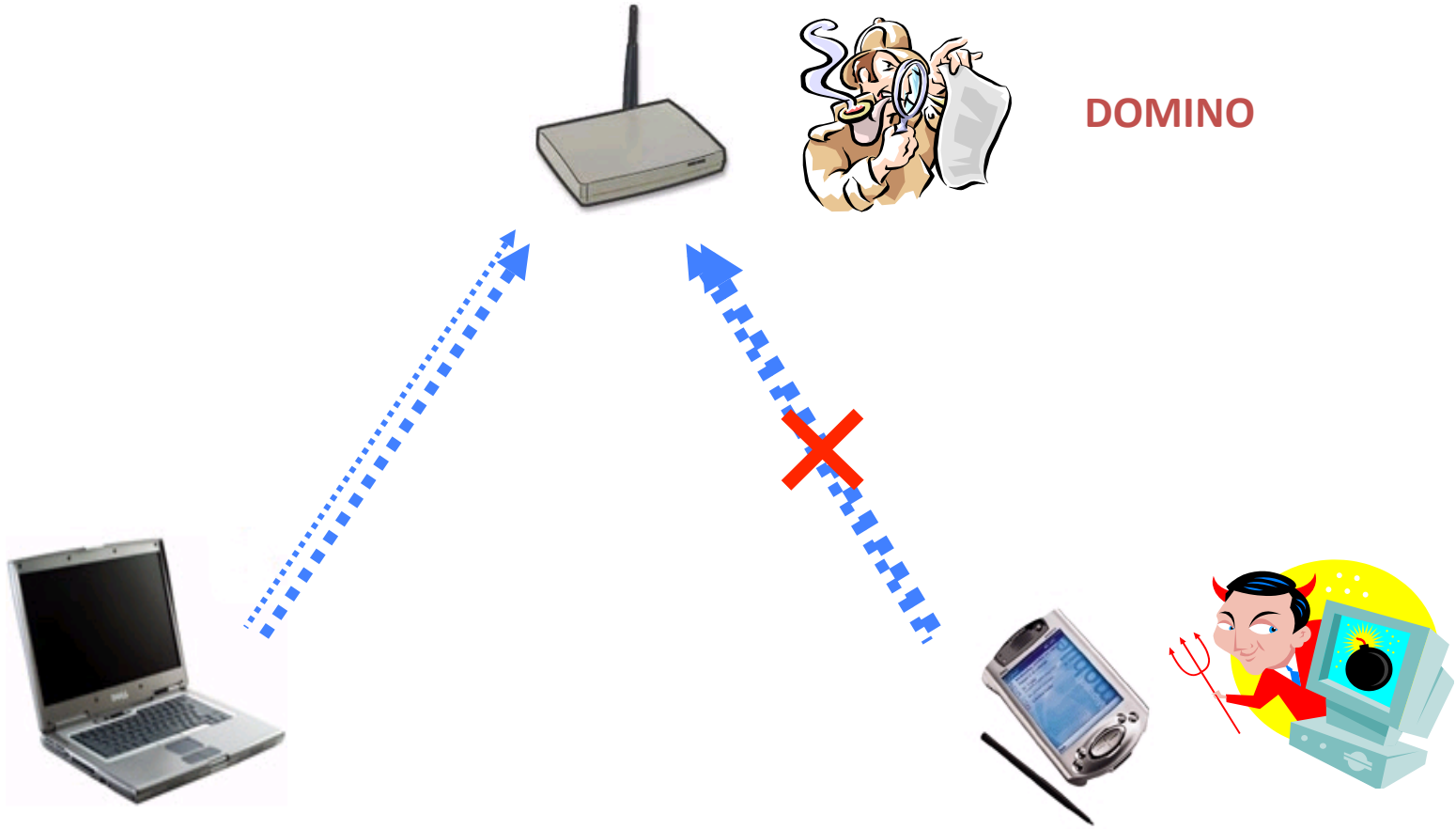
- Internet access through public hotspots
- Problem: misuse of protocols
- What about MAC-layer misbehavior?
  - Considerable bandwidth gains
  - Hidden from the upper layers
  - Always usable
- If the misbehavior is detected, the WISP can take measures

How to detect?

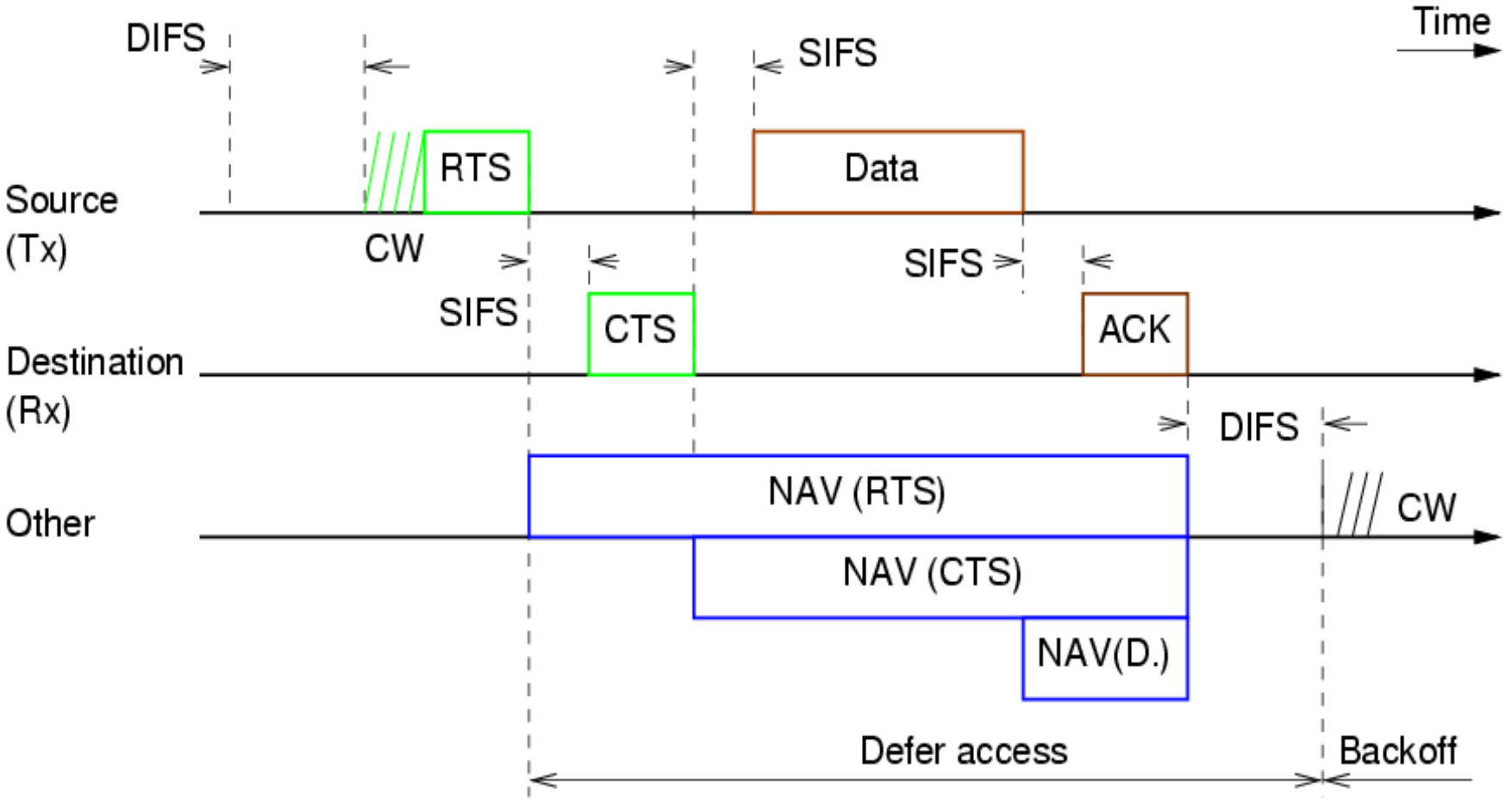
System model

- Infrastructure mode
- DCF (Distributed Coordination Function)
- Single trusted AP operated by a WISP
- Misbehavior is greedy as opposed to malicious
- DOMINO is implemented **only** at the AP

Example scenario



IEEE 802.11 MAC – Brief



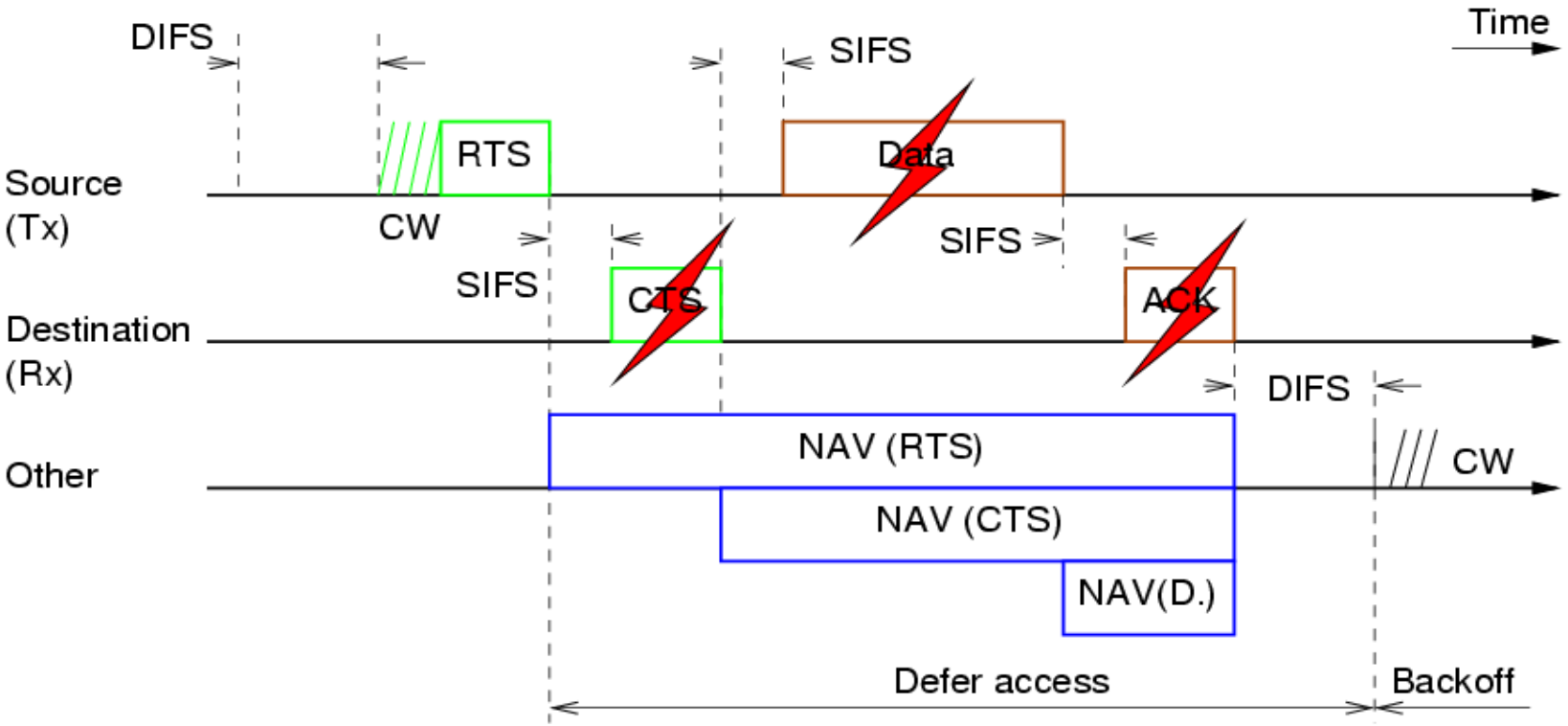
CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Misbehavior techniques – Overview

- Uplink traffic (stations ⇨ AP)
  - Example scenarios: backup, webcam, …
- Downlink traffic (AP ⇨ stations)
  - Constitutes most of the wireless traffic
  - Over 90% is TCP
  - Example scenarios: Web browsing, FTP, video streaming, …

Uplink traffic – Frame scrambling



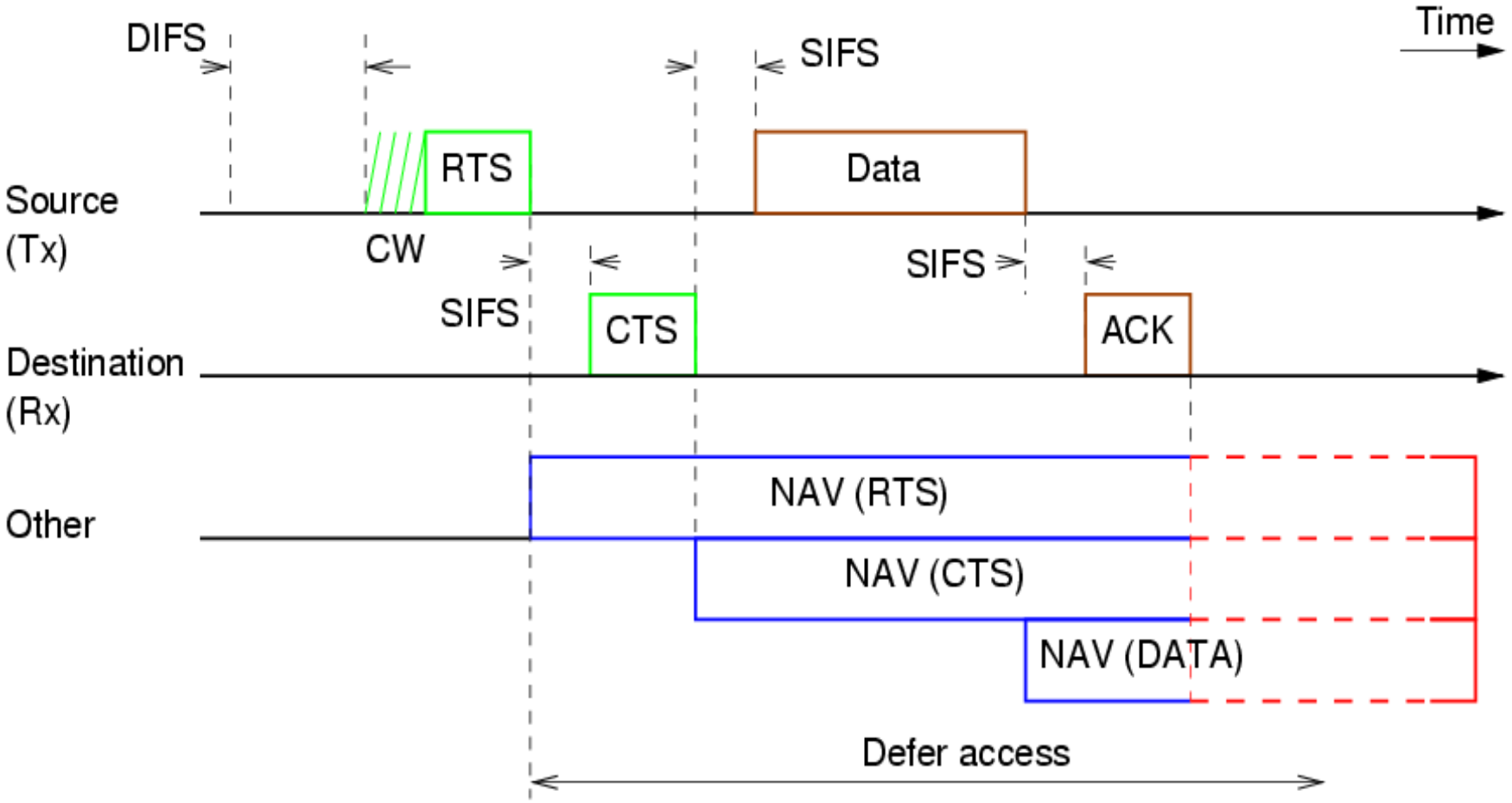
CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Solution: Number of retransmissions

- Lost frames are retransmitted
- Sequence numbers in the MAC header distinguish retransmissions
- Cheater's retransmissions are fewer than those of well-behaved stations
- By counting retransmissions, the AP can single out the cheater

Uplink traffic – Oversized NAV



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

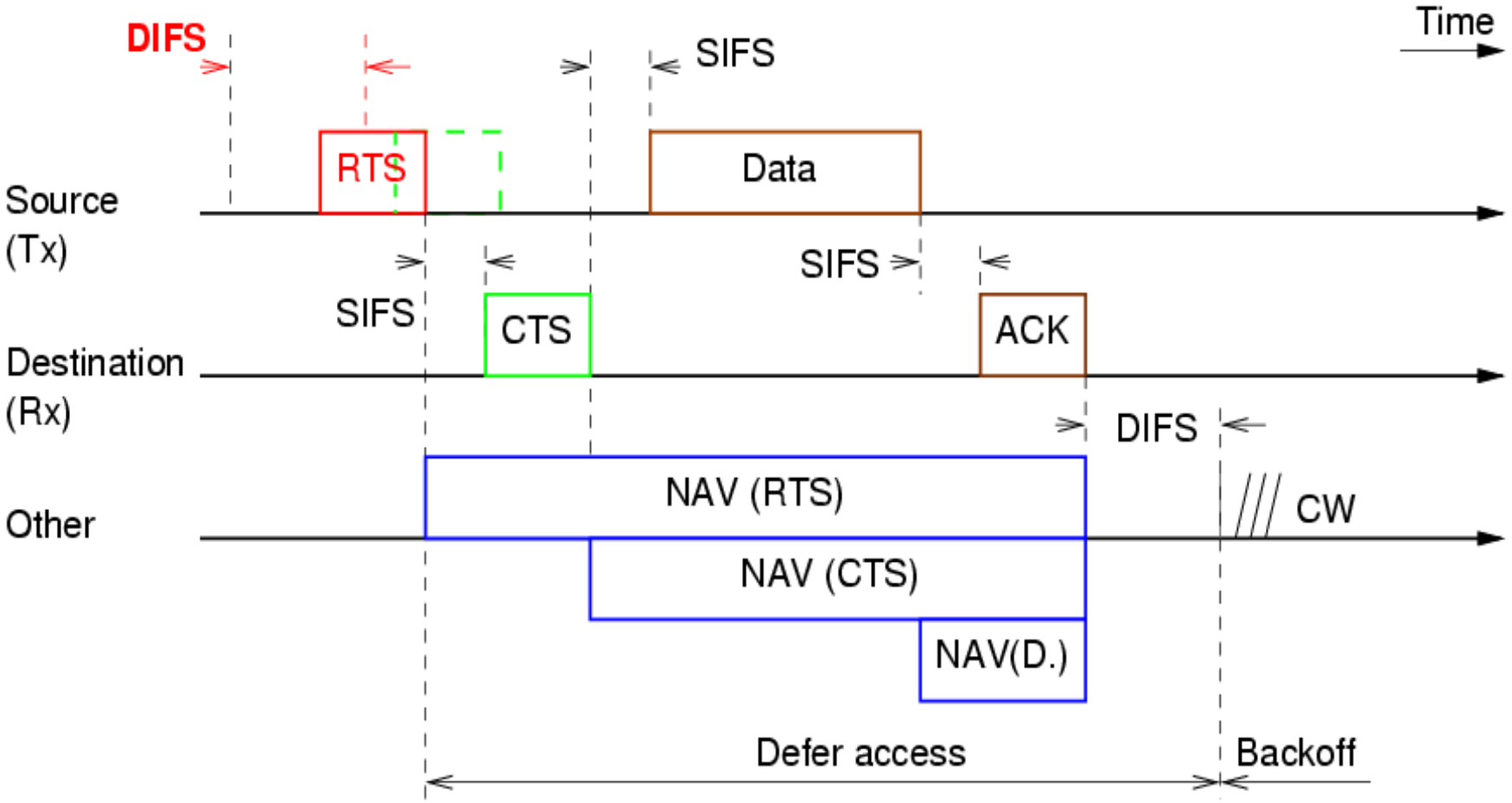
RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Solution: Comparison of NAVs

- AP measures the actual NAV and compares to the received one

- A repeated pattern of oversized NAVs distinguishes the cheater

Uplink traffic – Short DIFS



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

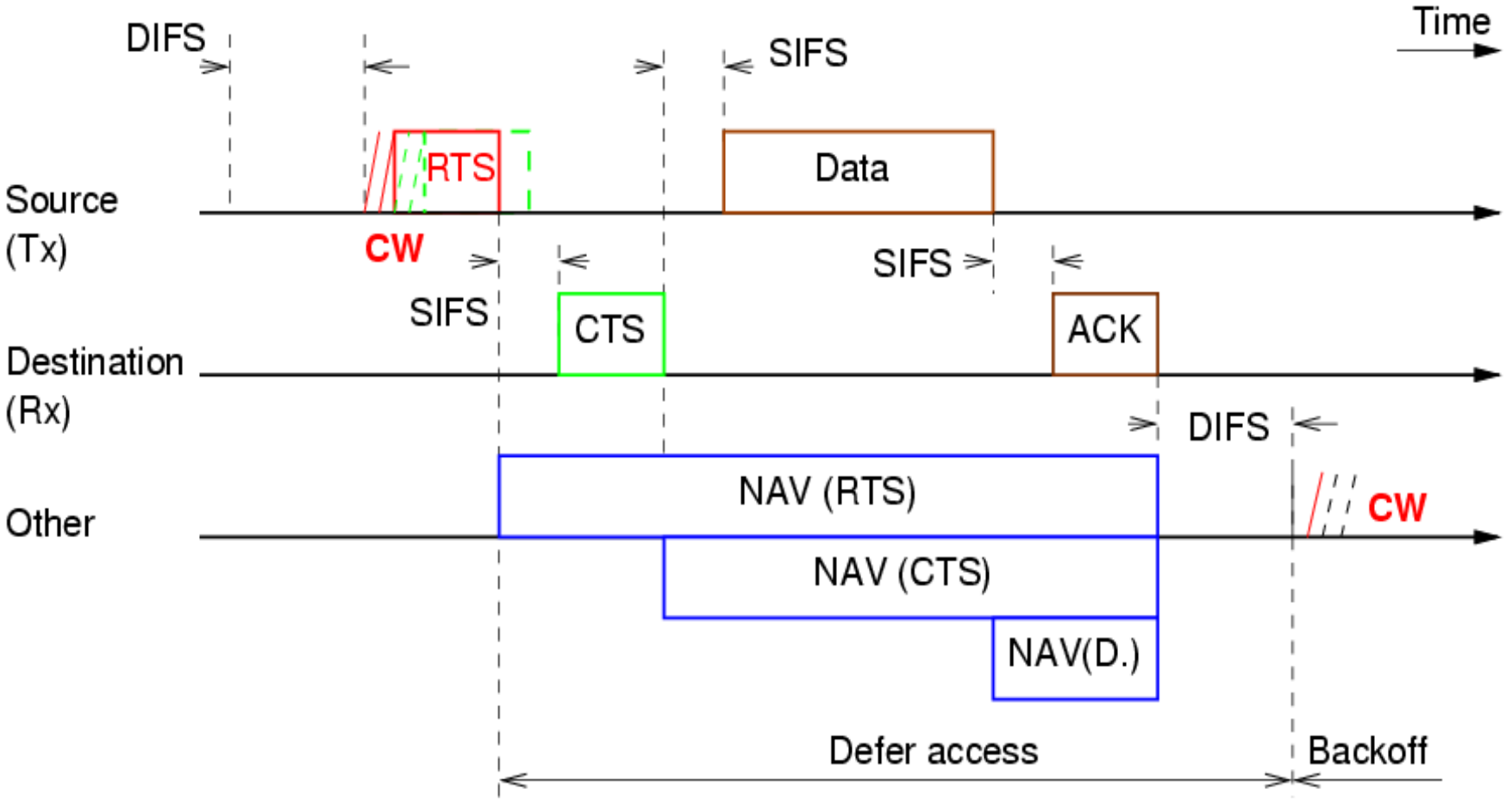
RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Solution: Comparison of DIFS

- The value of DIFS is constant and provided by the IEEE 802.11 standard

- A short DIFS cannot be but the result of cheating

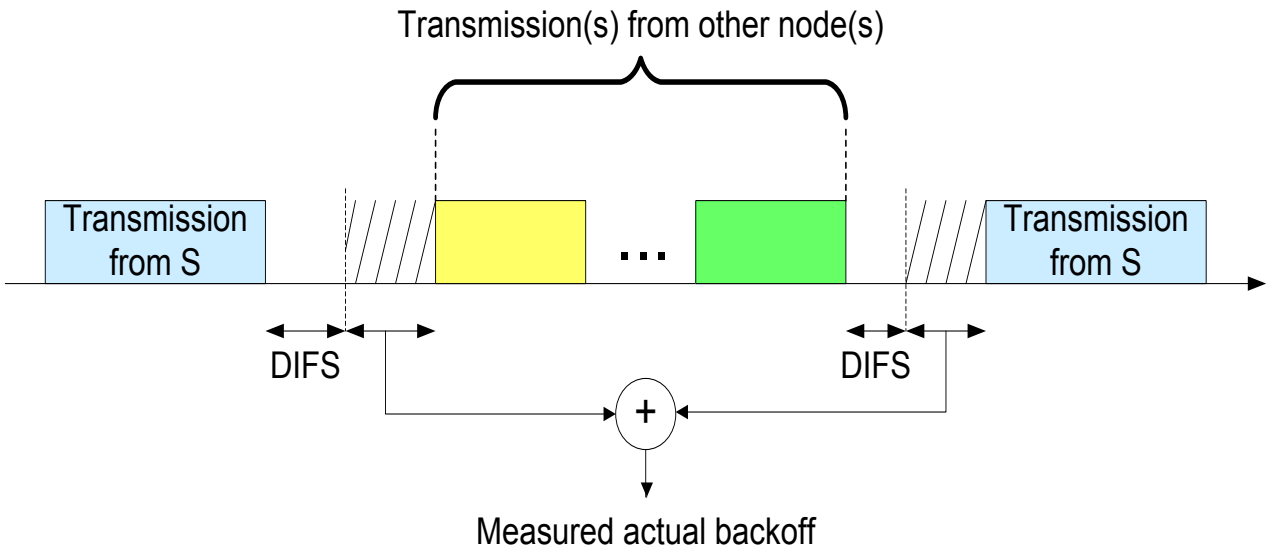
Uplink traffic – Backoff



CW: Contention Window
SIFS: Short Inter–Frame Spacing
DIFS: Distributed Inter–Frame Spacing

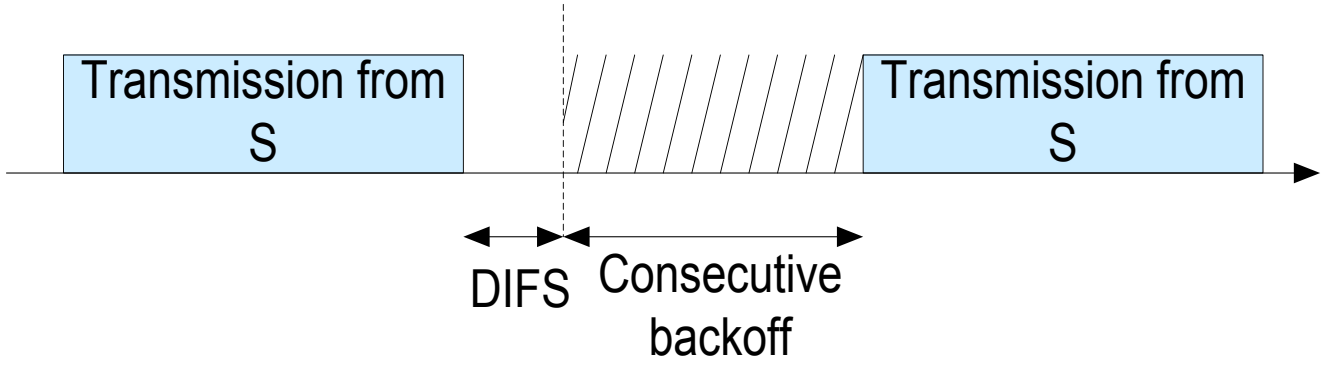
RTS / CTS: Request To Send / Clear To Send
ACK: ACKnowledgement
NAV: Network Allocation Vector

Solution (1/2): Actual backoff test



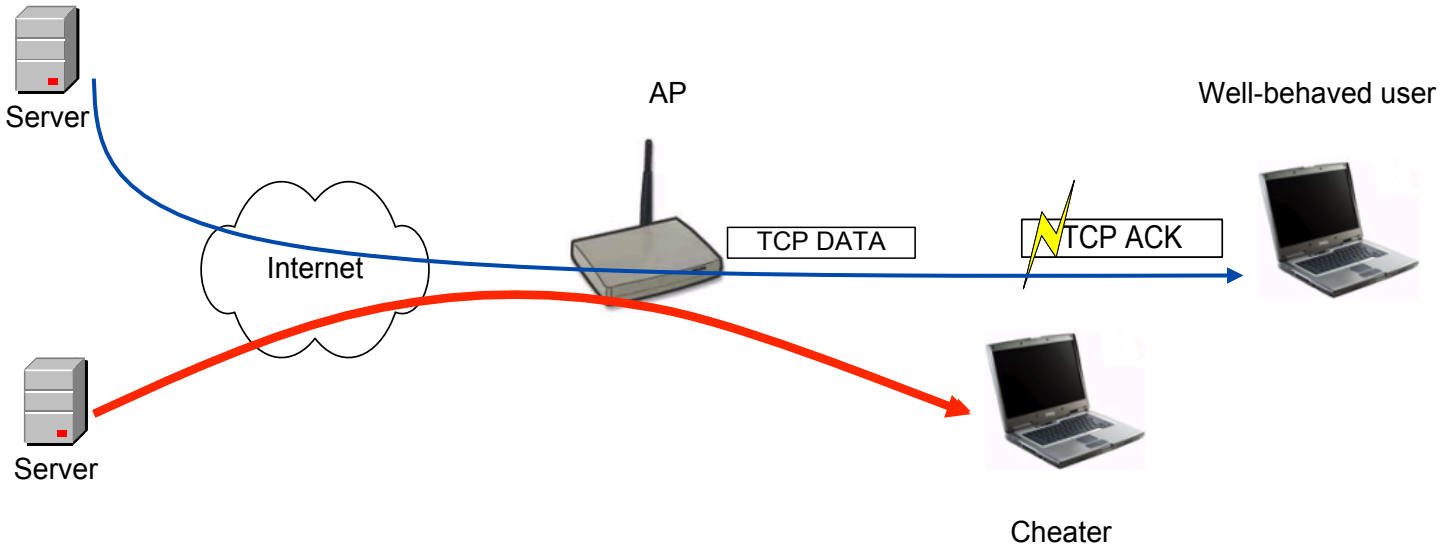
- Compares the average actual backoff of each station to the average actual backoff of the AP
- Collisions are not taken into account
- Unsuitable for sources with interframe delays (e.g., due to TCP congestion control)

Solution (2/2): Consecutive backoff test



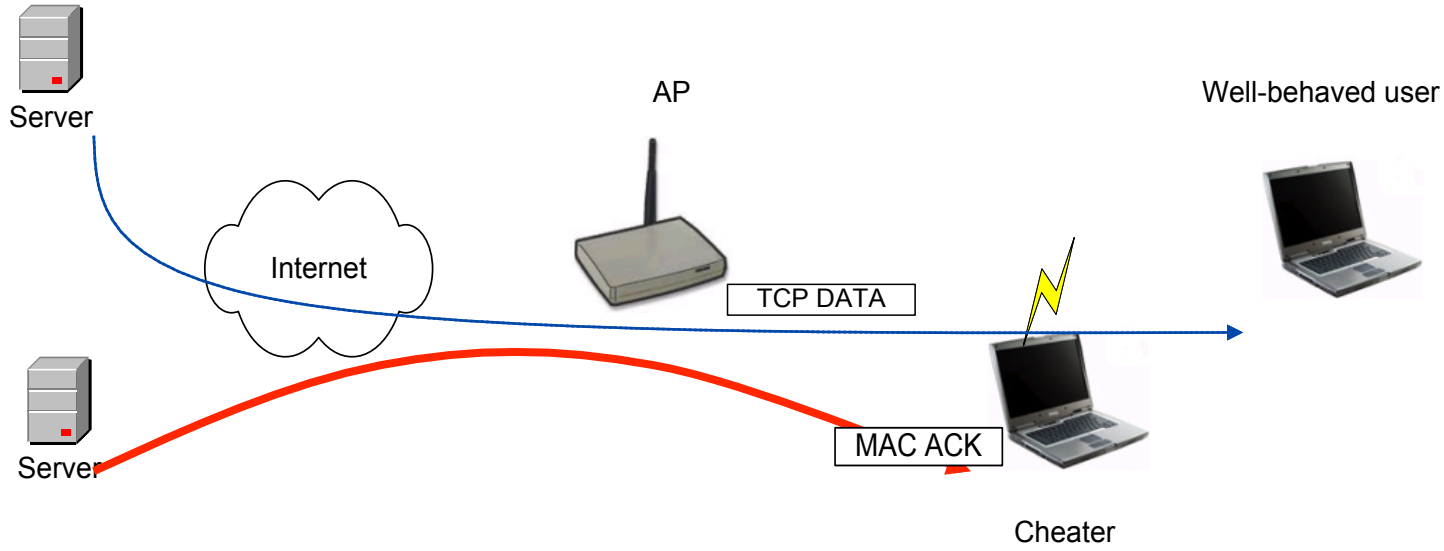
- Useful when cheaters have interframe delays (mainly TCP sources)
- Does not work if the traffic is very high due to the lack of samples
- Complementary to the actual backoff test

Downlink traffic – TCP ACK scrambling



- Server receives no TCP ACK and slows down the TCP flow
- Repeated scrambling kills the TCP connection
- The AP receives less packets destined to the well-behaved station
- Packets destined to the cheater are delayed less in AP's queue

TCP DATA scrambling with MAC forging



- Tries to kill the TCP connection like the previous attack
- MAC ACK contains no source address
- The forged MAC ACK prevents the AP from retransmitting the lost packet

Solution: Dummy frame injection

- AP periodically injects dummy frames destined to non- existing stations
- If it receives corresponding MAC ACKs, there is cheating
- Higher-layer mechanisms will identify the cheater (e.g., by monitoring the TCP flows of stations)

Components of DOMINO

Cheating method	Detection test
Frame scrambling	Number of retransmissions
Oversized NAV	Comparison of the declared and actual NAV values
Transmission before DIFS	Comparison of the idle time after the last ACK with DIFS
Backoff manipulation	*Actual backoff*
	Consecutive backoff
Frame scrambling with MAC forging	Periodic dummy frame injection

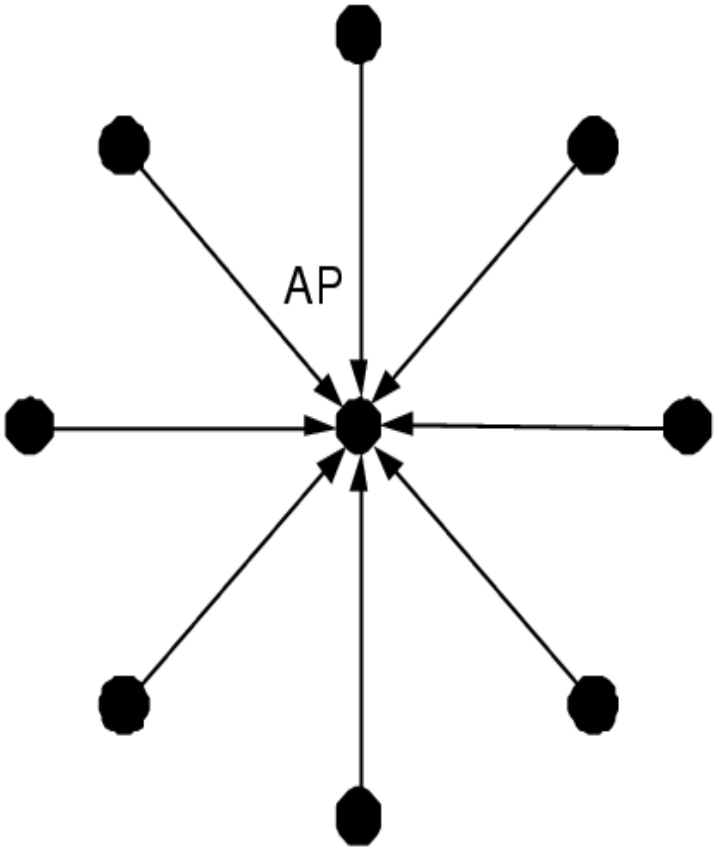
Simulation – Topology

- ns-2
- Backoff manipulation
- CBR / UDP traffic
- FTP / TCP traffic
- *misbehavior coefficient* (*m*):

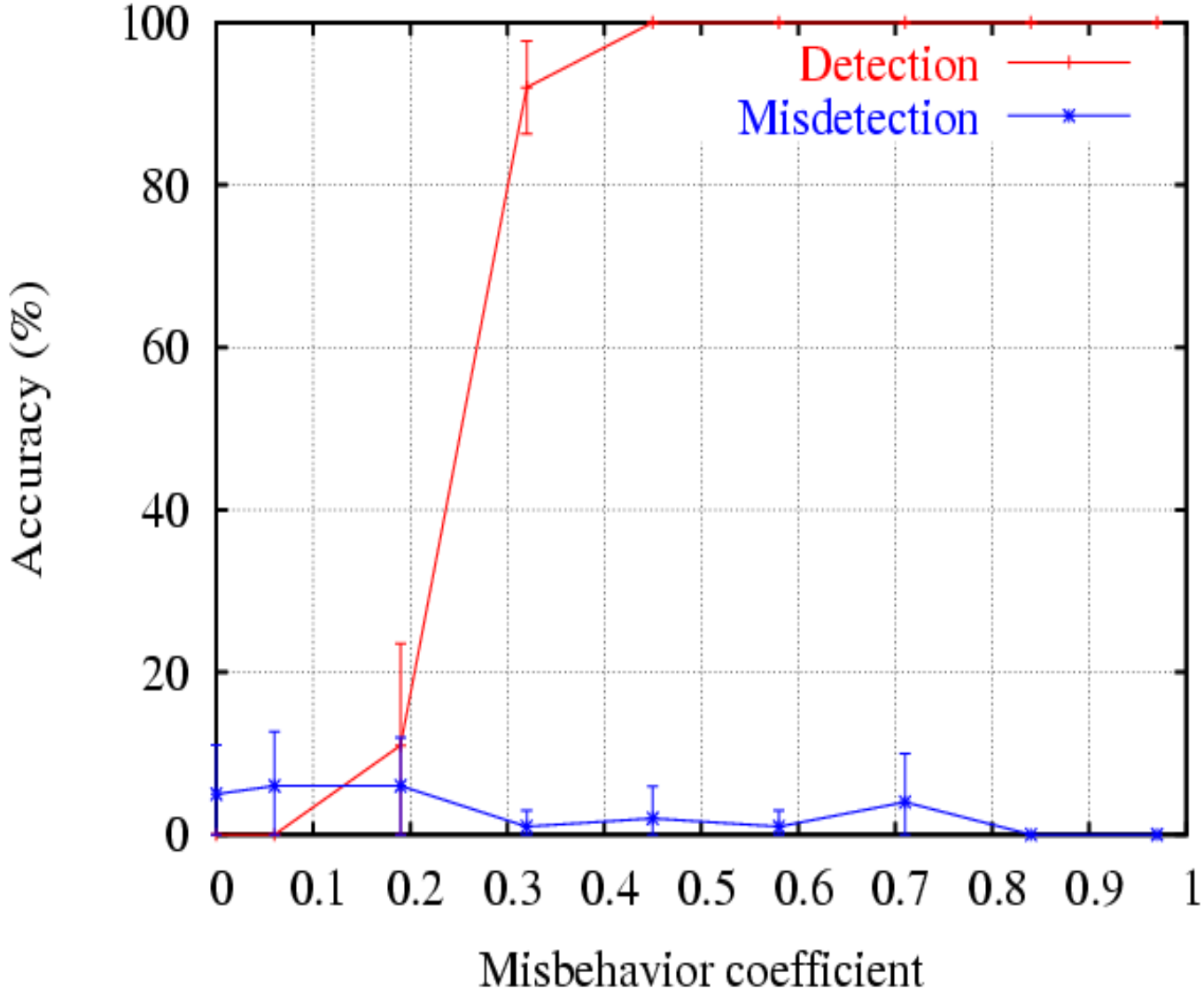
  cheater chooses its backoff from

  the fixed contention window

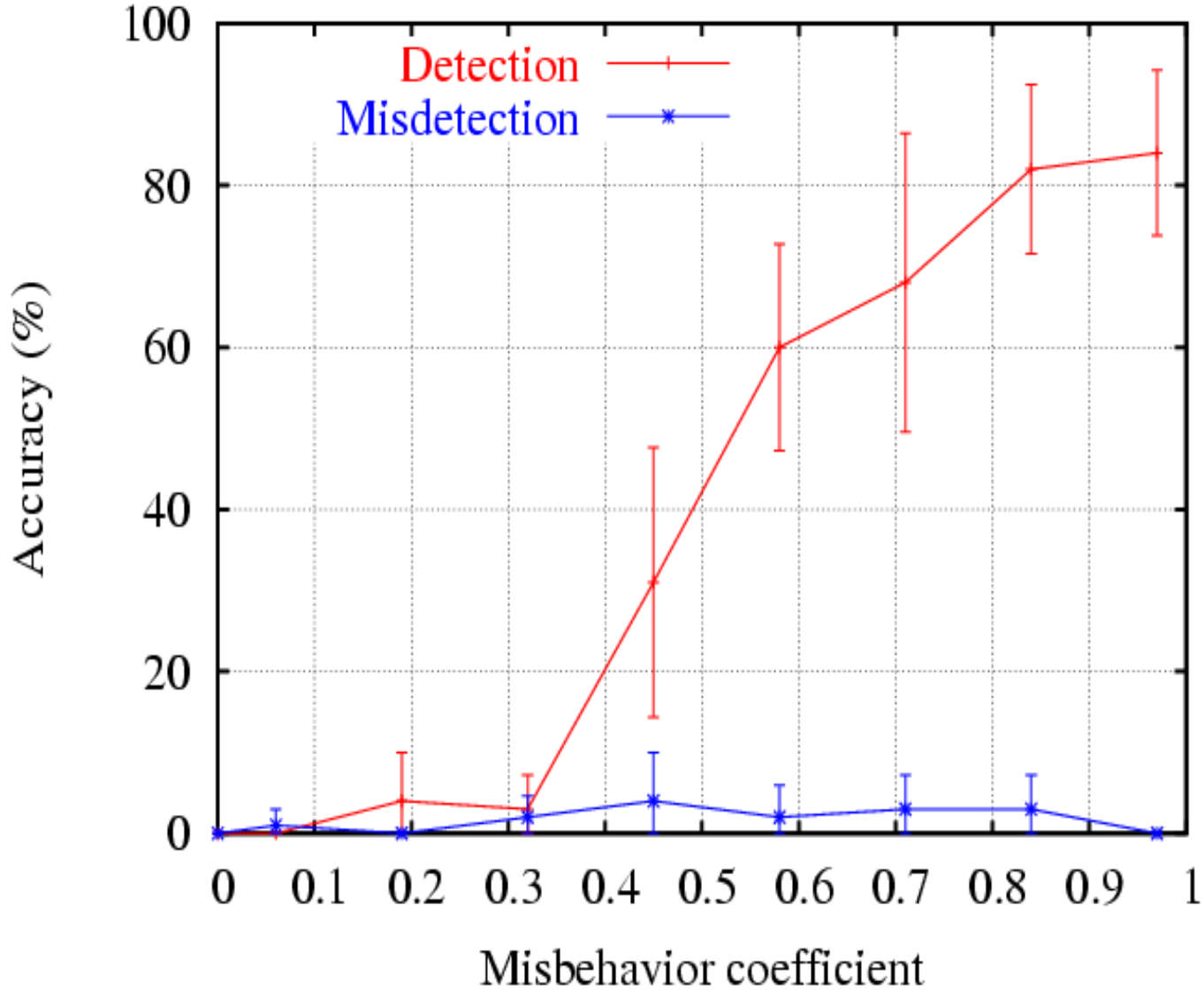
  (1 - m) x CWmin



Simulation – DOMINO performance – UDP case (Actual Backoff)

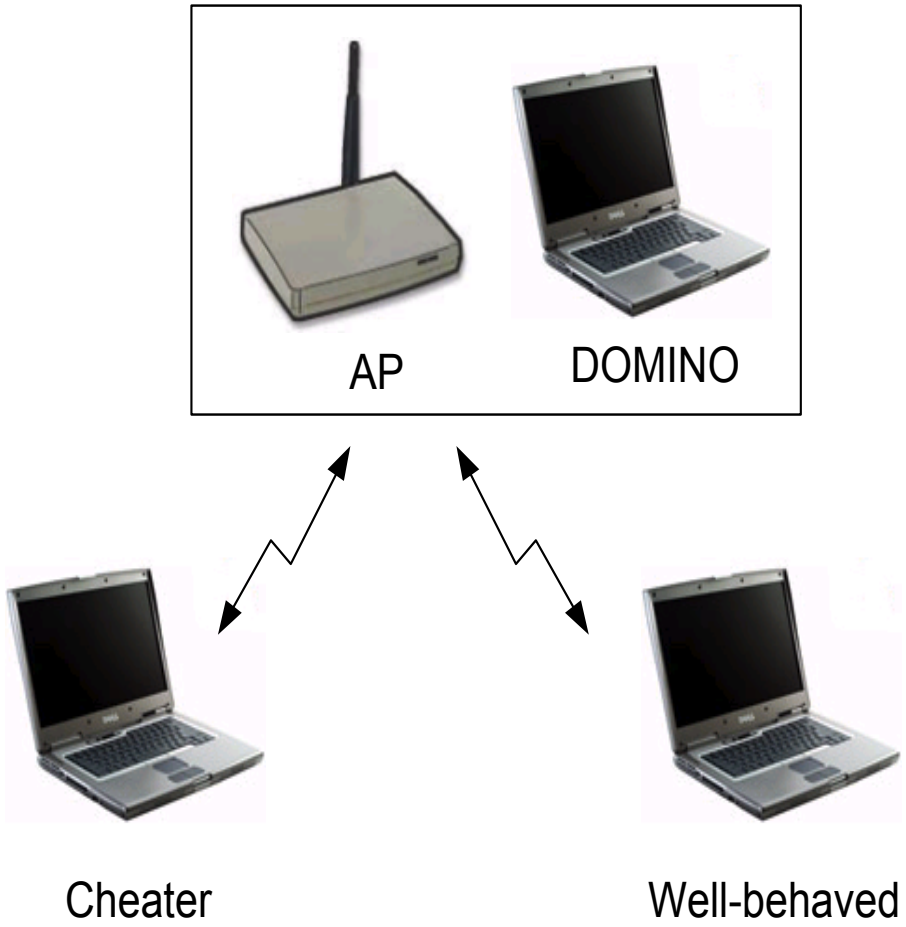


Simulation – DOMINO performance – TCP case (Consecutive Backoff)

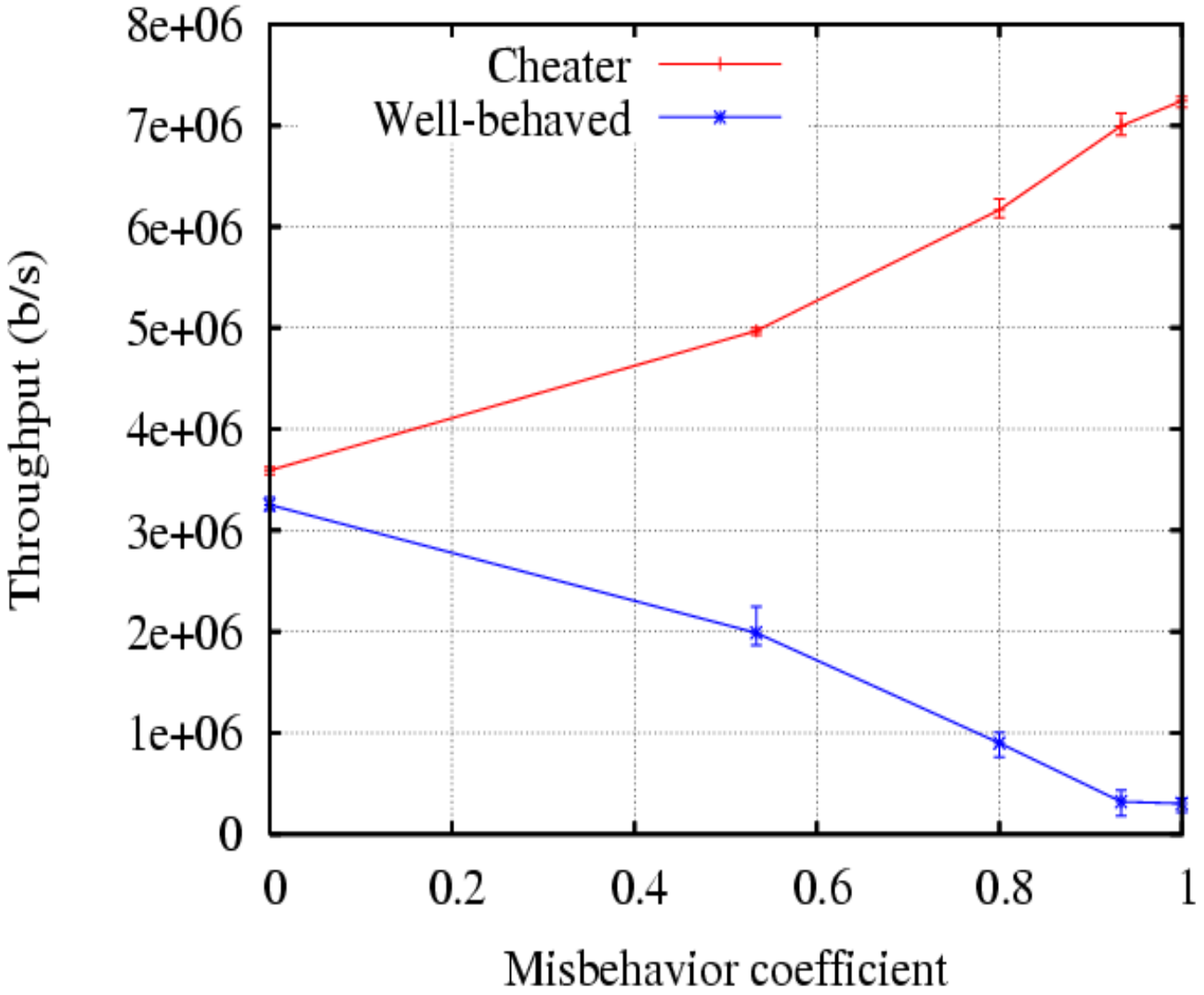


Implementation

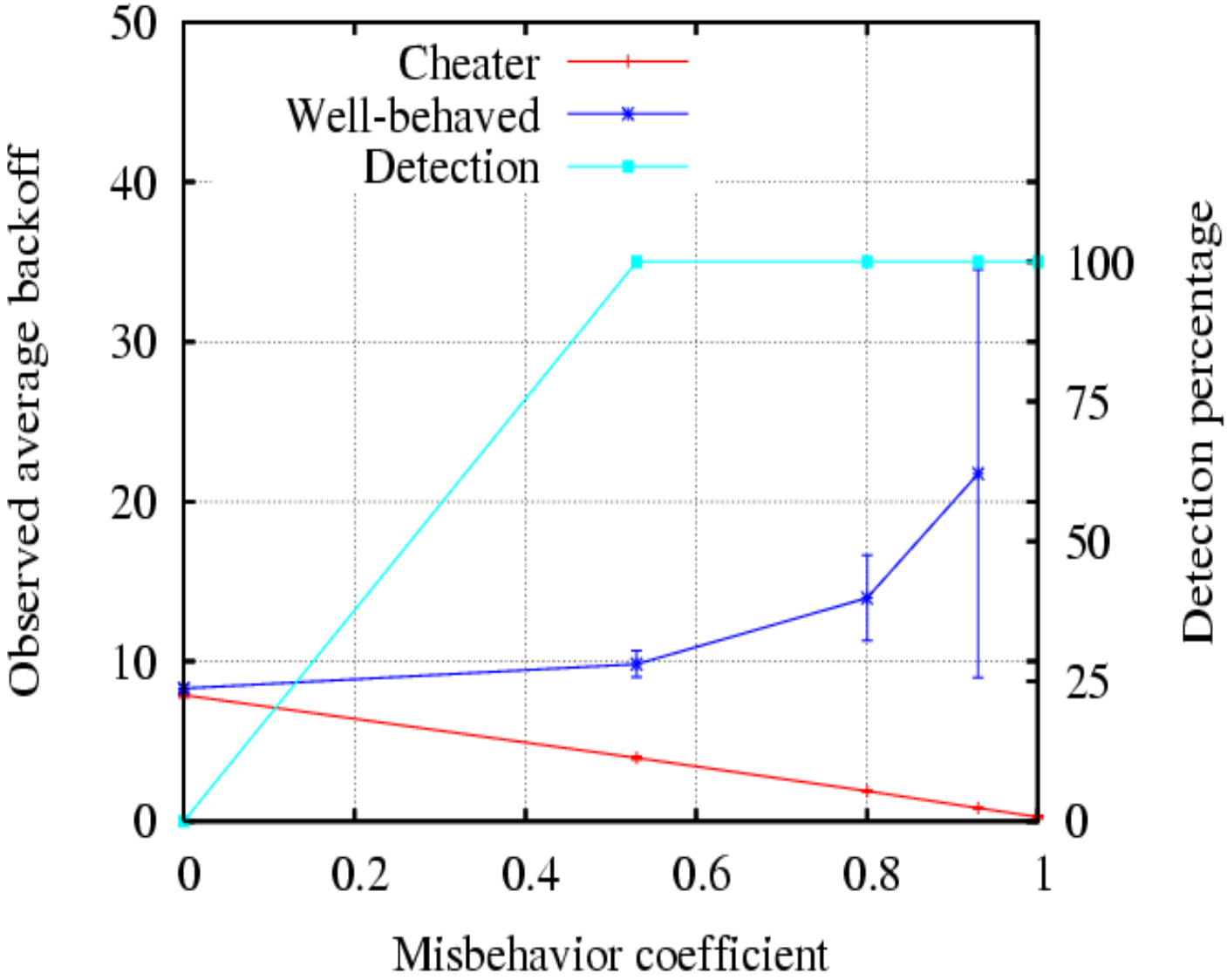
- **Equipment**
  - Adapters based on the Atheros AR5212 chipset
  - MADWIFI driver
- **Misbehavior (backoff)**
  - Write to the register containing CWmin and CWmax (in driver)
- **Monitoring**
  - The driver in MONITOR mode
  - *prism2* frame header



Implementation – Throughput



Implementation – Backoff and DOMINO



Conclusion on Section 9.2

- MAC-layer greedy behavior can be a serious problem
- DOMINO is a simple and efficient solution compatible with the existing infrastructure
- DOMINO can be seamlessly integrated with existing WiFi security tools to provide ultimate protection
- First proof-of-concept implementation prototype
- **http://domino.epfl.ch**

Chapter outline

9.1 Operating principles of IEEE 802.11

9.2 Detecting selfish behavior in hotspots

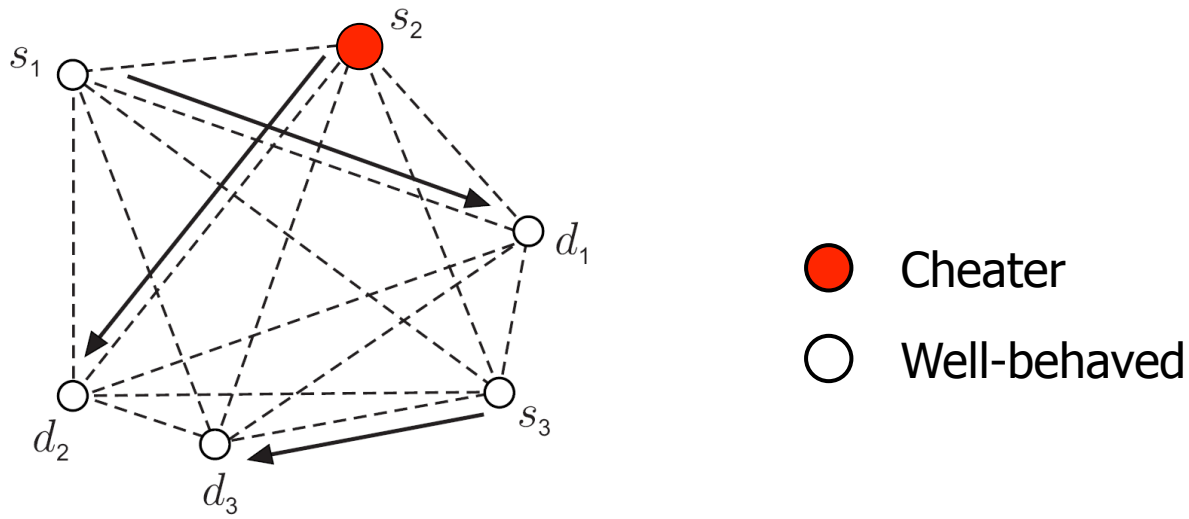
9.3 Selfish behavior in pure ad hoc networks

Section outline

- System Model and Assumptions
- Bianchi's Model
- Static CSMA/CA Game
- Repeated CSMA/CA Game
- Implementation

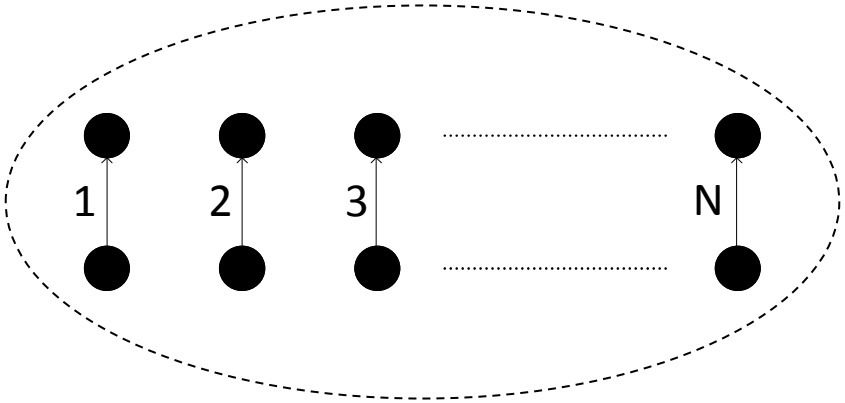
9.3.1 System Model and Assumptions

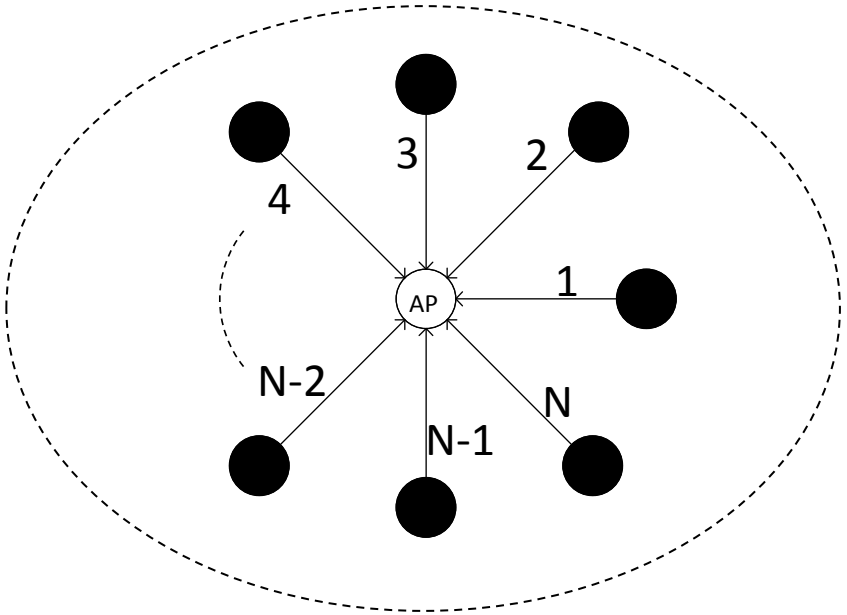
- Ad hoc mode (no access point)
- N wireless nodes transmit to N receivers (N links)
- Any node can hear any other node (single-collision domain)
- IEEE 802.11 CSMA/CA MAC layer
- Bianchi's Model for throughput calculation



Bianchi's Model: Topology and Parameters

- N links with the same physical condition (single-collision domain):



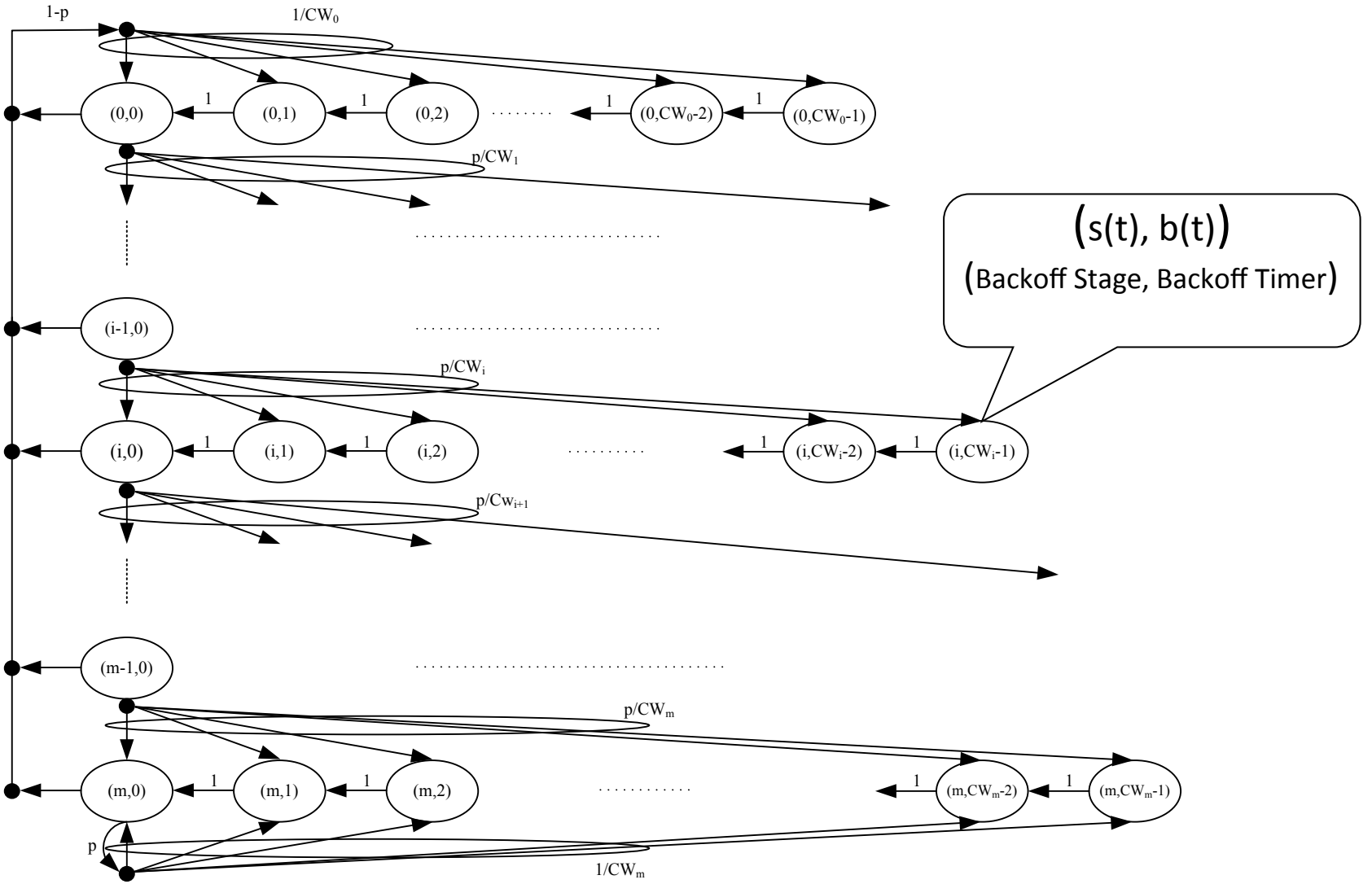


MAC Layer
PHY Layer

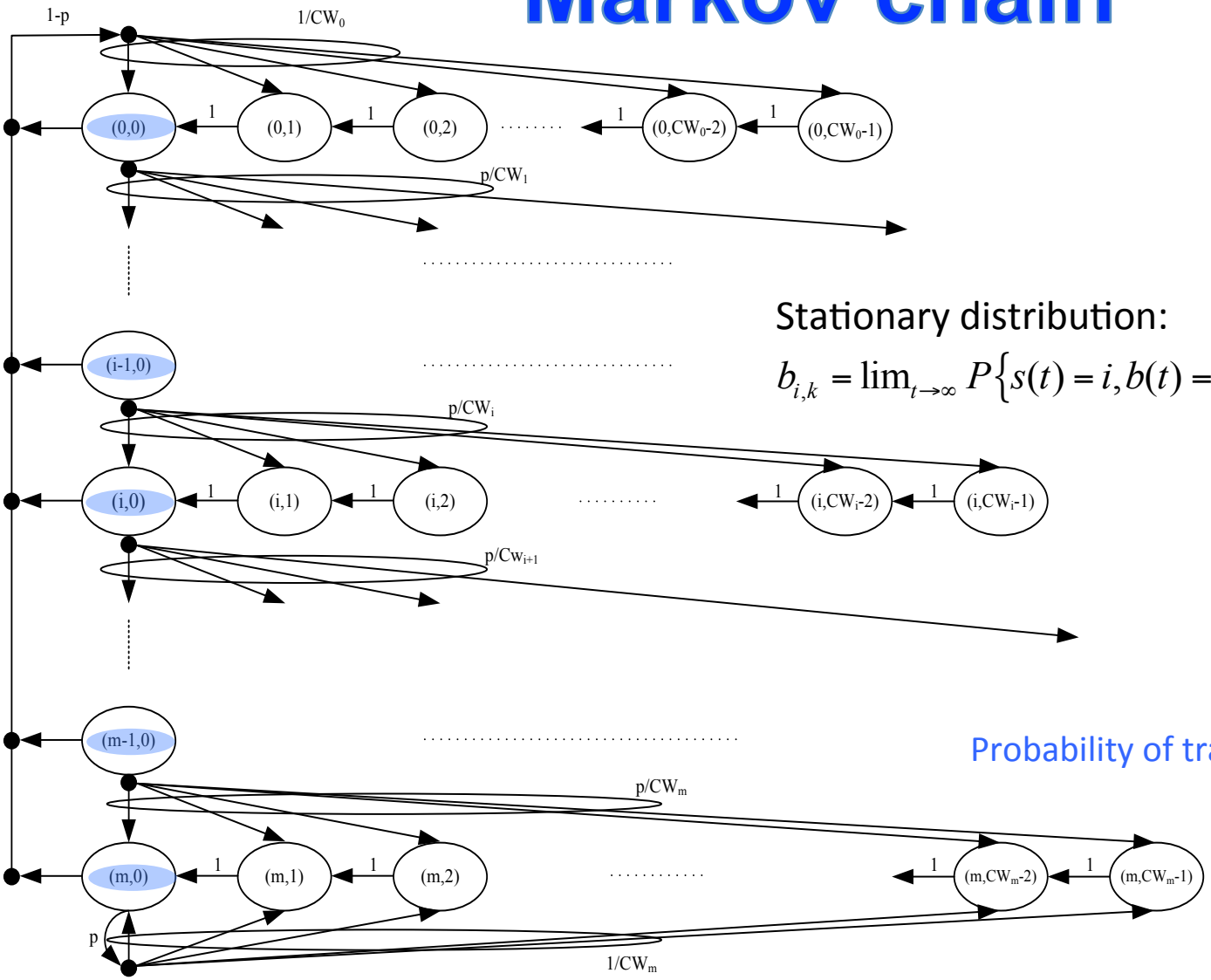
π = Probability of Transmission

P = Probability of Collision
= More than one transmission at the same time
= $1 - (1- \pi)^{N-1}$

Bianchi's Model: Two Dimensional Markov chain



Bianchi's Model: Two Dimensional Markov chain

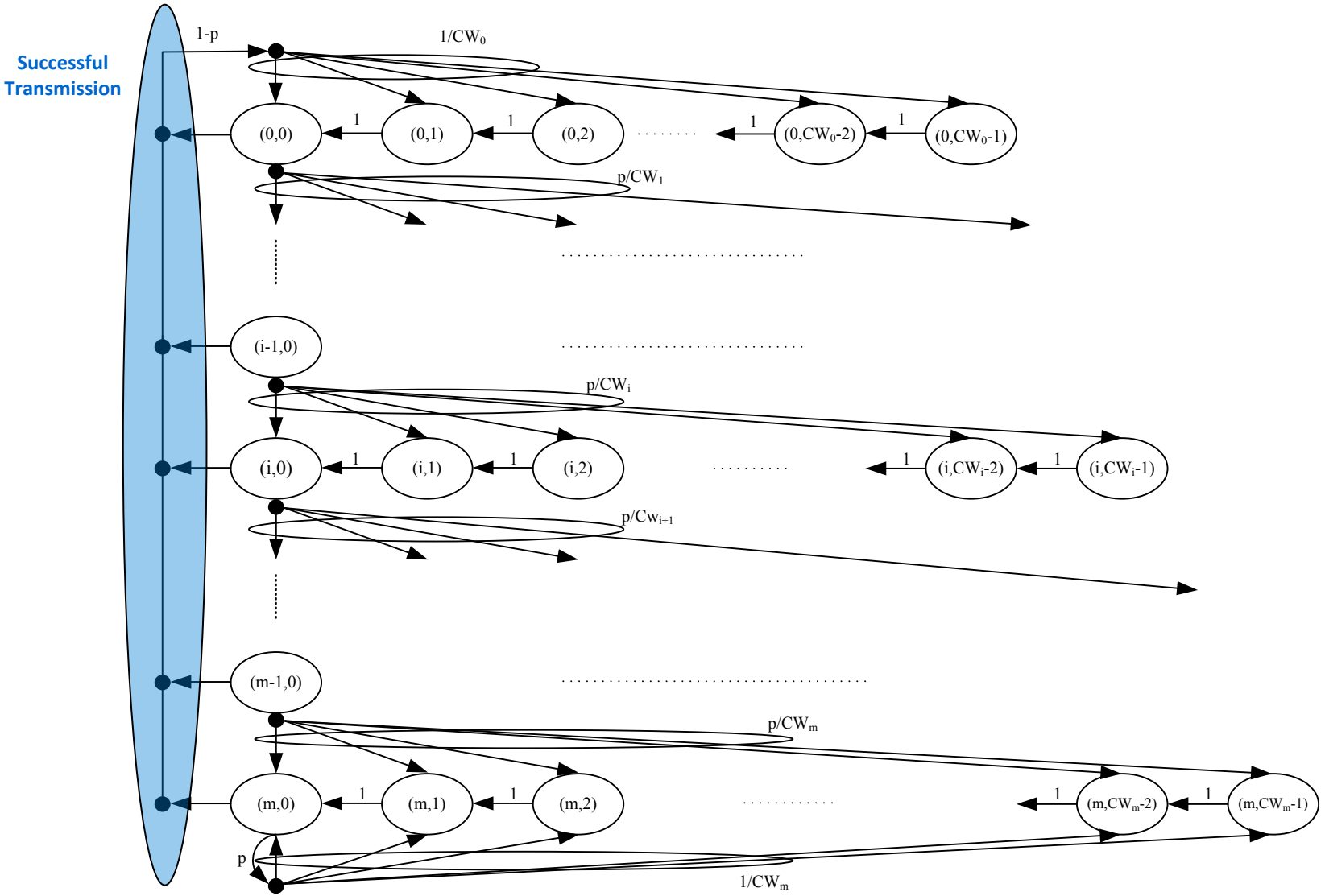


Stationary distribution:

$$b_{i,k} = \lim_{t\to\infty} P\{s(t)=i, b(t)=k\}, i\in(0,m), k\in(0,CW_i-1)$$

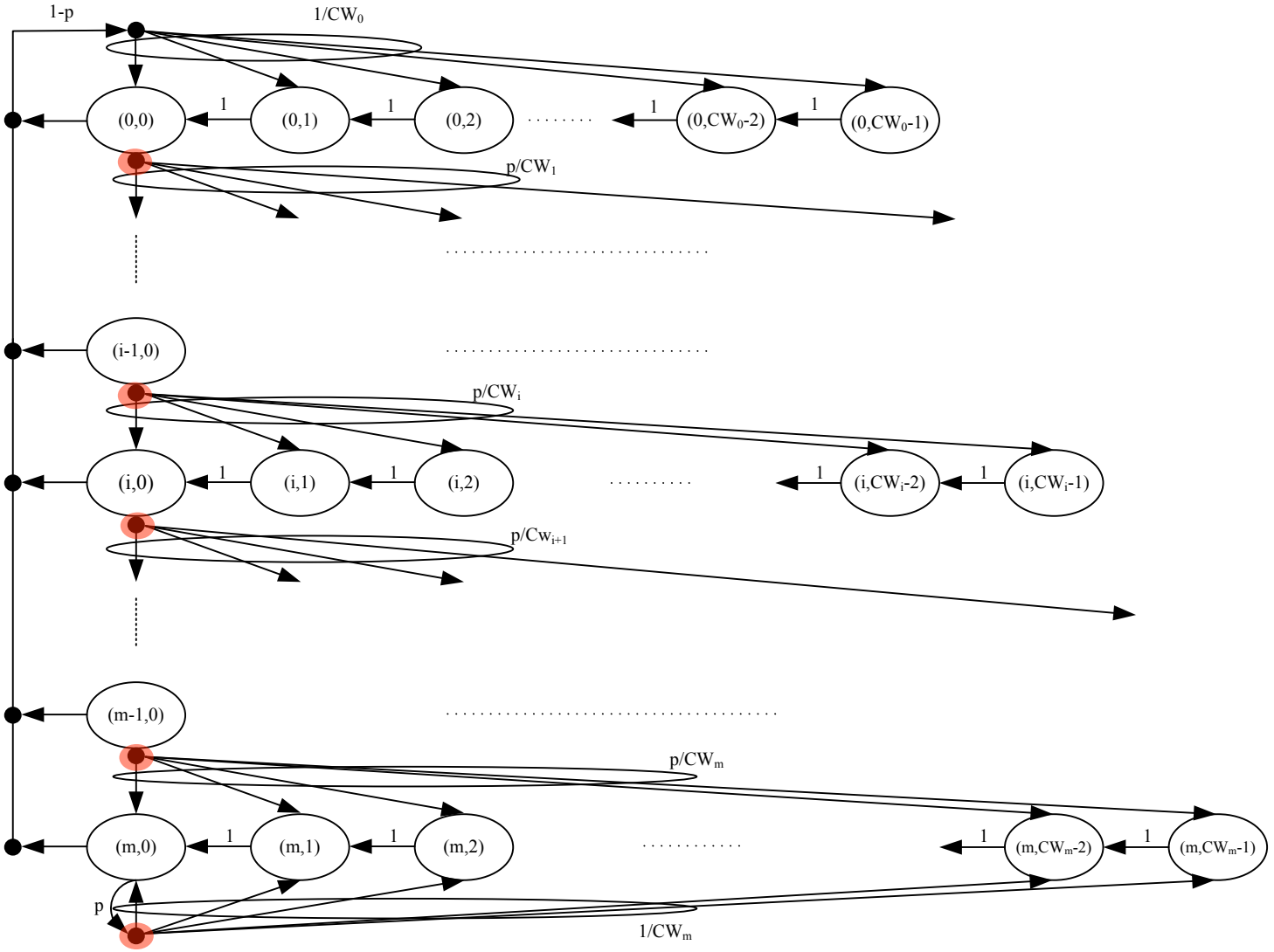
Probability of transmission: $\pi = \sum_{i=0}^{m} b_{i,0}$

Bianchi's Model: Two Dimensional Markov chain

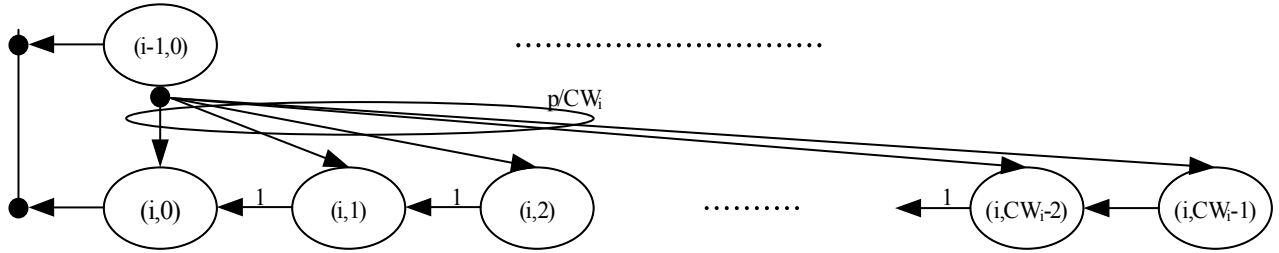


Bianchi's Model: Two Dimensional Markov chain

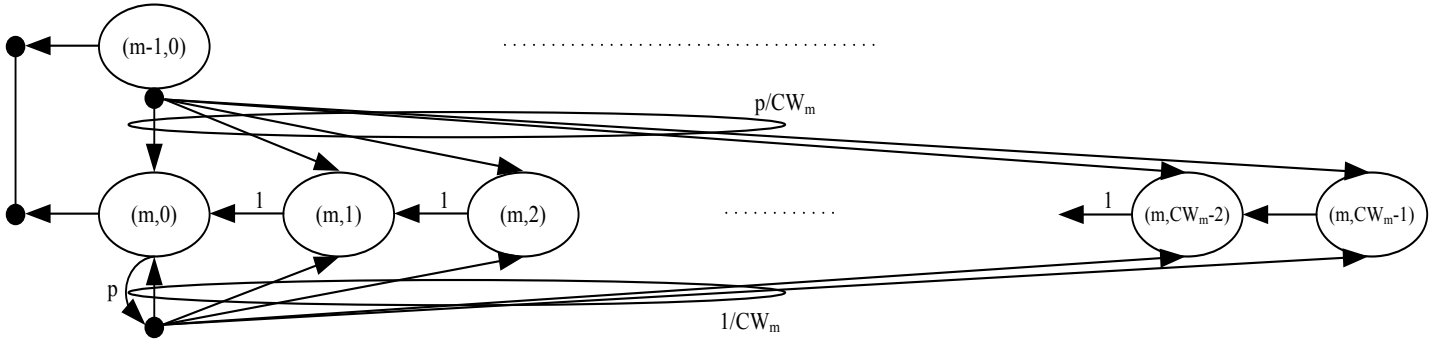
Collision



Bianchi's Model: Stationary Distribution of Chain



$$b_{i,0} = p\, b_{i-1,0}$$



$$b_{m,0} = p\, b_{m-1,0} + p\, b_{m,0}$$

Bianchi's Model: Solution for p and π

After some derivations → system of two nonlinear equations with two variables p and π:

$$\begin{cases} p = 1 - (1-\pi)^{N-1} \\ \\ \pi = \dfrac{2}{1 + W_{min} + pW_{min} \sum_{k=0}^{m-1} (2p)^k} \end{cases}$$

➔ Can be solved numerically to obtain p and π

Bianchi's model: Throughput Calculation

- Throughput of node i:

$$\tau_i = \frac{E[Payload\ Transmitted\ by\ user\ i\ in\ a\ slot\ time]}{E[Duration\ of\ slot\ time]} = \frac{P_i^s L}{P^s T^s + P^c T^c + P^{id} T^{id}}$$

  - P_i^s: Probability of successful transmission of i during a random time slot
  - L: Average packet payload size
  - T^s: Average time to transmit a packet of size L
  - P^{id}: Probability of the channel being idle
  - T^{id}: Duration of the idle period
  - P^c: Probability of collision
  - T^c: Average time of collision

$$P_i^s = \pi_i \prod_{j \neq i}(1 - \pi_j)$$

$$P^s = \sum_{j=1}^{N} P_j^s$$

$$P^{id} = \prod_{j=1}^{N}(1 - \pi_j)$$

$$P^c = 1 - P^{id} - \sum_{j=1}^{N} P_j^s$$

9.3.2 CSMA/CA Game: $G_{CSMA/CA}$

- A single cheater
  - Selfish
  - Tends to use the full channel capacity
  - Does not respect the binary exponential backoff
  - Keeps her W after a collision unchanged (m=0)

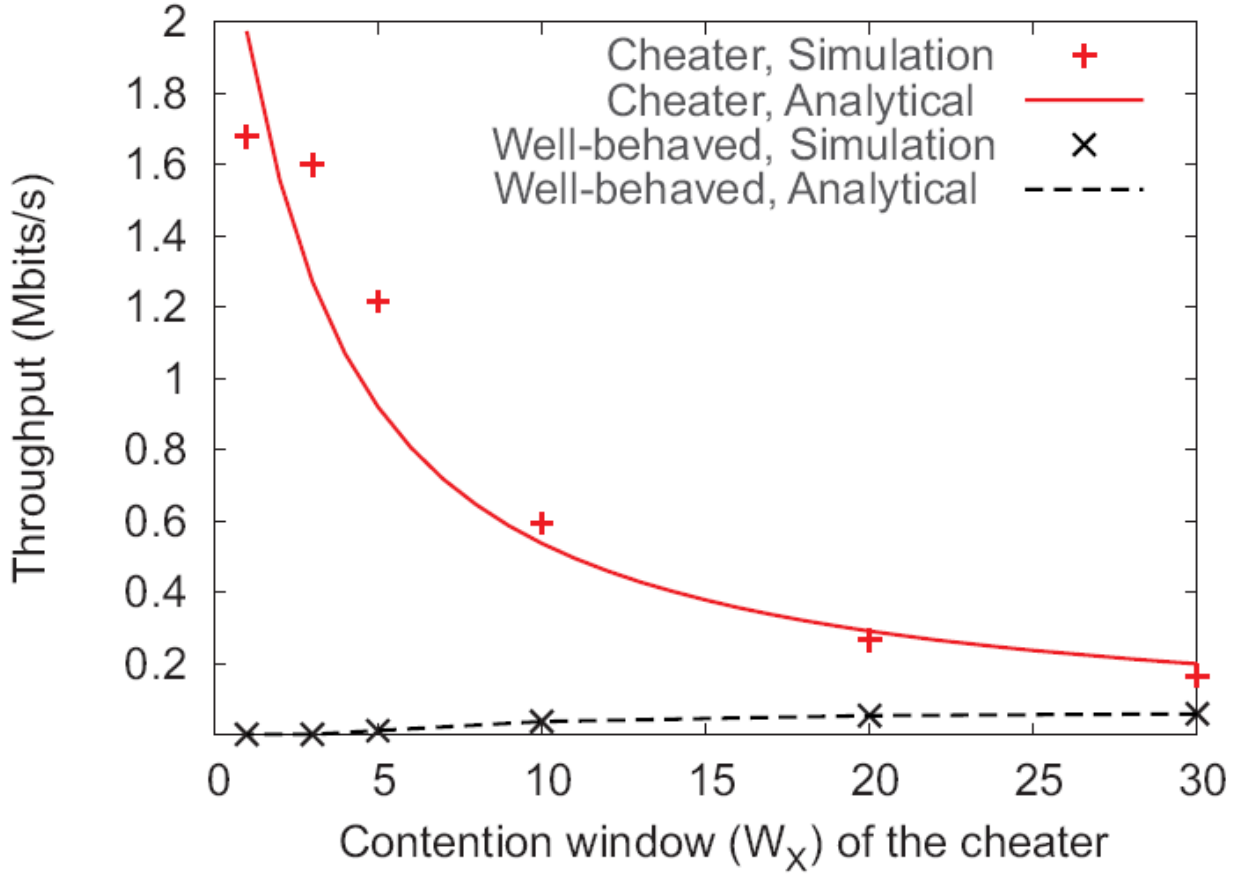
- Strategy set: $S_i = \{1, 2, \ldots, W_{max}, W_\infty\}$

- Payoff function:
$$u_i(W) = \tau_i^{(c)}(W)$$

$G_{CSMA/CA}$: cheaters payoff function

- Access probability of cheater i: $\pi_i^{(c)} = \frac{2}{W_i + 1}$
- Throughput of cheater i: $\tau_i^{(c)} = \frac{\pi_i^{(c)} c_i^{(1)}}{\pi_i^{(c)} c_i^{(2)} + c_i^{(3)}}$
- $\frac{\partial \tau_i^{(c)}}{\partial W_i} \leq 0$
- If $\pi_j^{(c)} < 1$ for all j in P\{i}:
  - strict inequality, so ➔ **throughput: strictly decreasing function of W_i**
  - **by unilaterally decreasing its own Wi: a selfish node can increase its throughput**

Model Verification



NE of the $G_{CSMA/CA}$

- **Lemma 9.1:**
  For any strategy profile W that constitutes a NE, $\exists i \in P$ such that $W_i = 1$

- **Theorem 9.1:**
  $G_{CSMA/CA}$ admits exactly $(W_{max}+1)^{|P|} - W_{max}^{|P|}$ NEs.

NE of the $G_{CSMA/CA}$

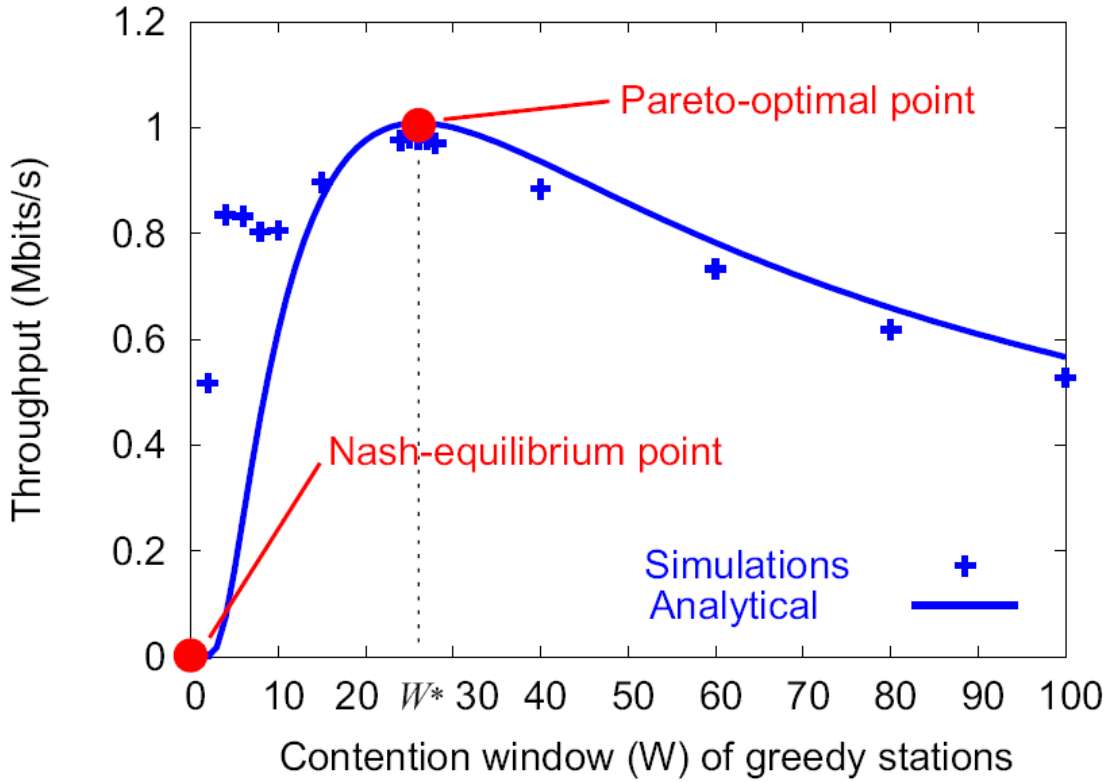
- Define: $D = \{i: W_i=1, i \in P\}$
- Two families of NE:
  - $|D|=1$: only one player receives a non-null throughput and throughput = 0 for all others
  - $|D|>1$: throughput = 0 for all players.

- Some NE from the first family are Pareto optimal.
  - Example: $W = (W_1=1, W_2=W_\infty, \ldots, W_{|P|}=W_\infty)$ is a Pareto optimal NE
- NE of the 2nd family: tragedy of the commons (misuse of the public good).

Uniqueness, Fairness and Pareto Optimality

- **two families of NE:**
  - 1st: great unfairness, a single player gets some positive payoff
  - 2nd: highly inefficient NE, zero payoff for every player
- **none is satisfactory**
- **A desirable solution:**
  - Uniqueness
  - Pareto optimality
  - Fairness

Uniqueness, Fairness and Pareto Optimality



- Transformation of the Pareto-optimal point to a NE:
  - Repeated games
  - Selective jamming

9.3.3 Repeated CSMA/CA Game: $G^{\infty}_{CSMA/CA}$

- $G^{\infty}_{CSMA/CA}$ = $G_{CSMA/CA}$ played repeatedly T times.
- Payoff function:

$$u_i^{\infty} = \liminf_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} u_i^t(\pi_i^t, \pi_{-i}^t)$$

- the cheaters' per stage payoff function change to

$$u_i^t(\pi) = \tau^{(c)t}(\pi) - pf_i^t(\pi)$$

- pf: penalty function

Penalty Function

- Penalty function:

$$pf_i(\pi_i, \pi_{-i}) = \begin{cases} \varphi_i(\pi_i, \pi_{-i}), & \pi_i \in (\overline{\pi}, 1] \\ 0, & \pi_i \in [0, \overline{\pi}] \end{cases}$$

- $\varphi_i(\pi_i, \pi_{-i}) > 0$ and $\frac{\partial}{\partial \pi_i}\varphi_i(\pi_i, \pi_{-i}) > \frac{\partial}{\partial \pi_i}\tau_i^{(c)}(\pi_i, \pi_{-i})$,

  $\forall \pi_i \in (\overline{\pi}, 1]$ and $\pi_j < 1 \quad (j \in P \backslash \{i\})$.

- Then u_i has a unique maximizer $\overline{\pi} \in (0, 1)$. (Lemma 9.2)

Subgame Perfect NE (SPNE) of $G^{\infty}_{CSMA/CA}$

- **Theorem 9.4:** The strategy profile $(\pi_i^t = \overline{\pi})_{i \in P, t=\{1,\ldots,T\}}$ is a SPNE of the $G^{\infty}_{CSMA/CA}$.

- **Corollary 9.1:** any strategy profile $(\pi_i^t = \pi)_{i \in P, t=\{1,\ldots,T\}}$ such that $\pi \in (0,1)$ can be made a SPNE.

Making W* a NE: Practical Penalty Function

- Two players k and i
- k selectively jams i if $\tau_i(\pi) > \tau_k(\pi)$

- k calculates the penalty to be inflicted on i:

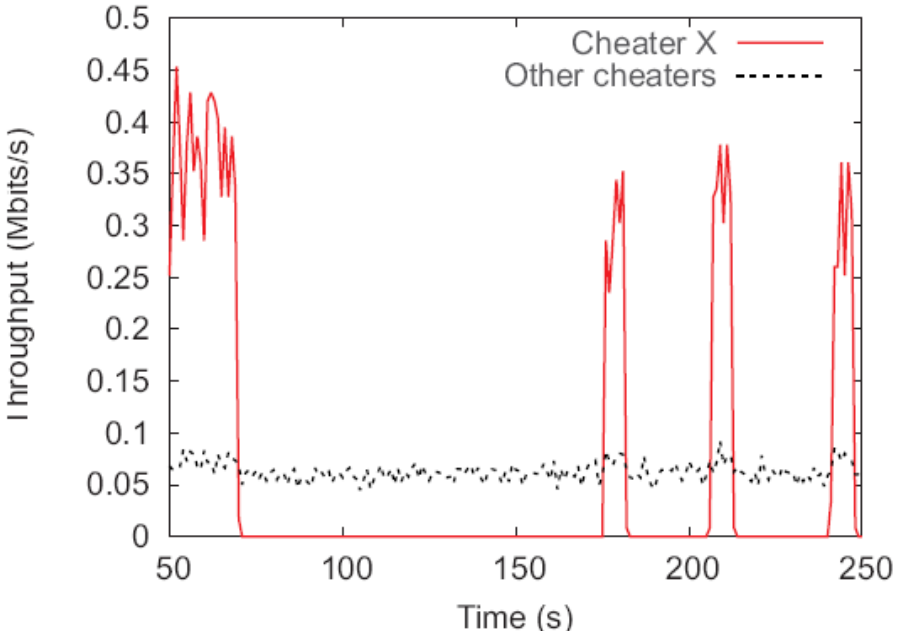
$$pf_i(\pi_i, \pi_{-i}) = \begin{cases} \tau_i^{(c)}(\pi_i, \pi_{-i}) - \tau_k^{(c)}(\pi_i, \pi_{-i}), & \text{if } \tau_i^{(c)}(\pi_i, \pi_{-i}) > \tau_k^{(c)}(\pi_i, \pi_{-i}) \\ 0, & \text{otherwise .} \end{cases}$$

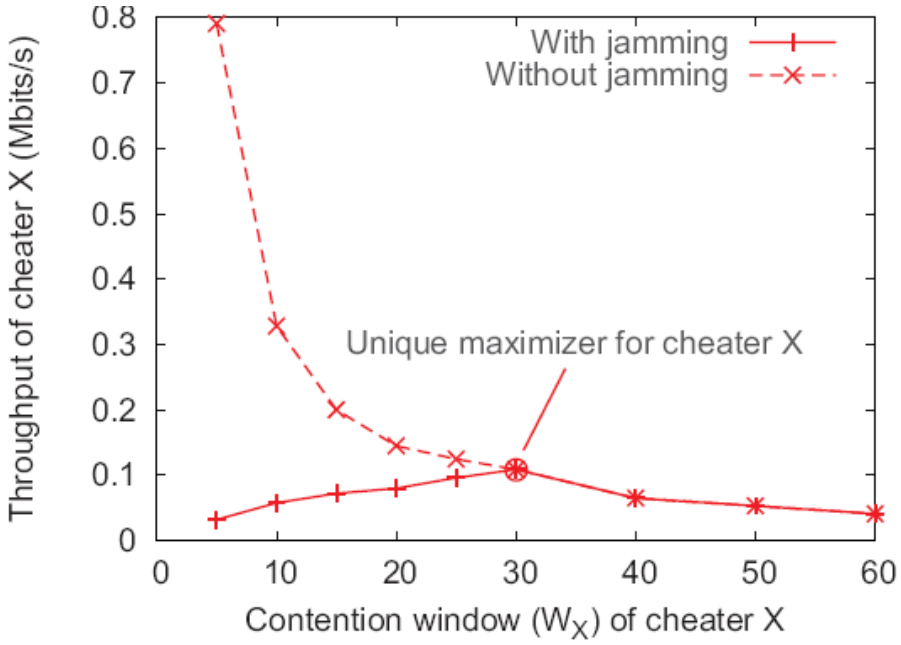
- u_i has a unique maximizer: $\pi_i = \pi_k$

- so, $\overline{\pi} = \min(\pi_i, \pi_k)$ i.e. $\overline{W} = \max(W_i, W_k)$ is a unique NE.

- equal payoffs for two players at NE.

Example: Penalization

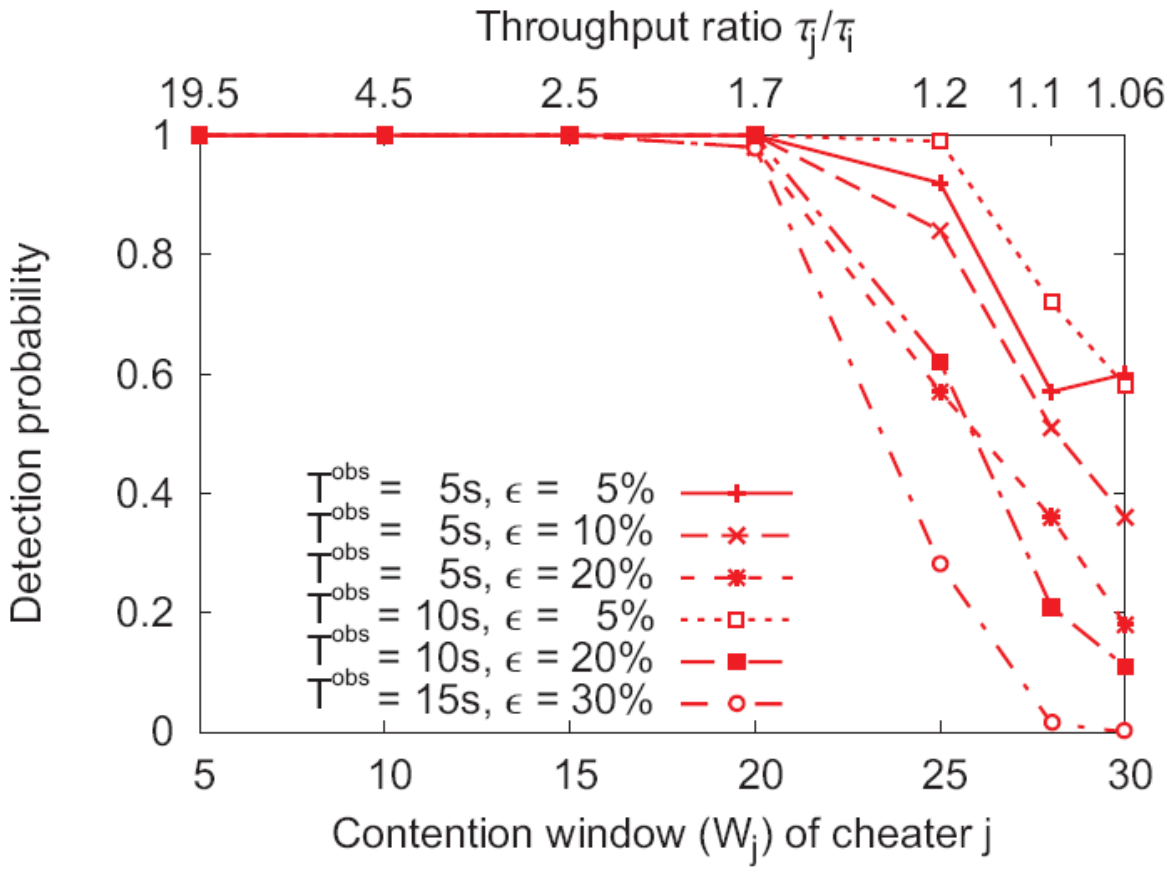




9.3.4 Implementation: Detection Mechanism

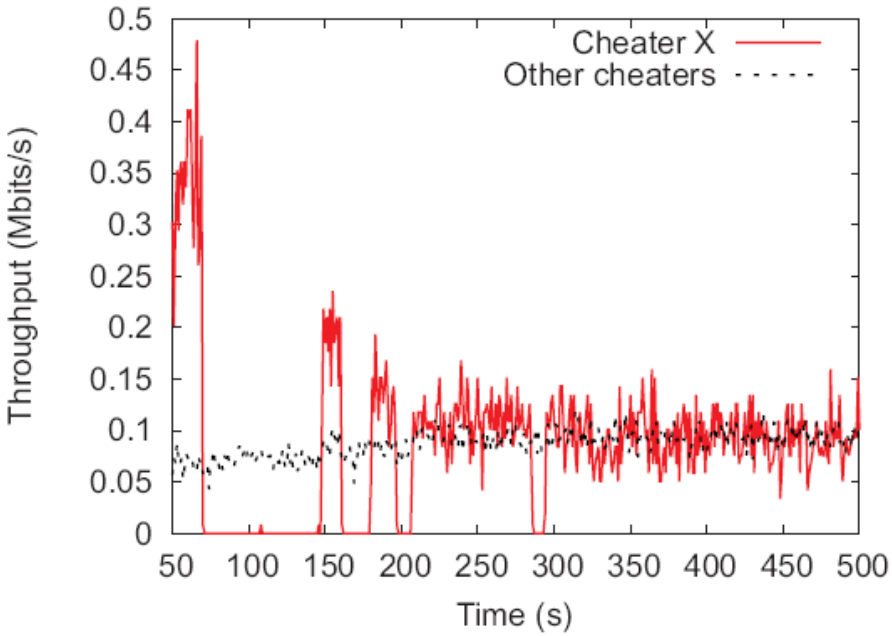
– each cheating node measures the throughput of all the others.

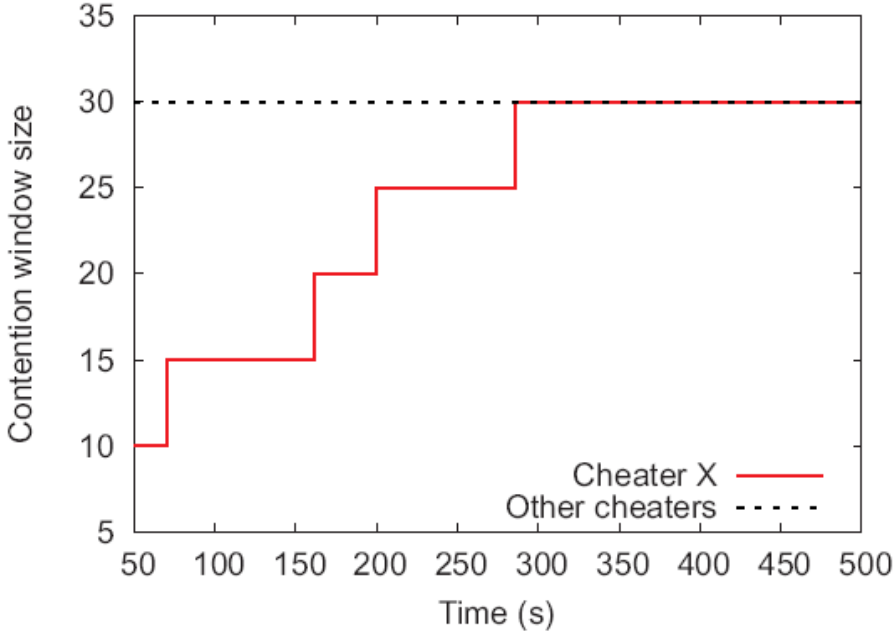
– cheater j is deviating if $\frac{\tau_j}{\tau_i} > 1 + \epsilon$ for T^{obs}.



Adaptive Strategy

– When cheater i is jammed (penalized) during Δ: increases her W by steps of size γ.





Reaching the Pareto-optimal Point

- $W_i = W^{init}$ for all cheaters
- Every cheater sets up a random timer to increase her W by γ.

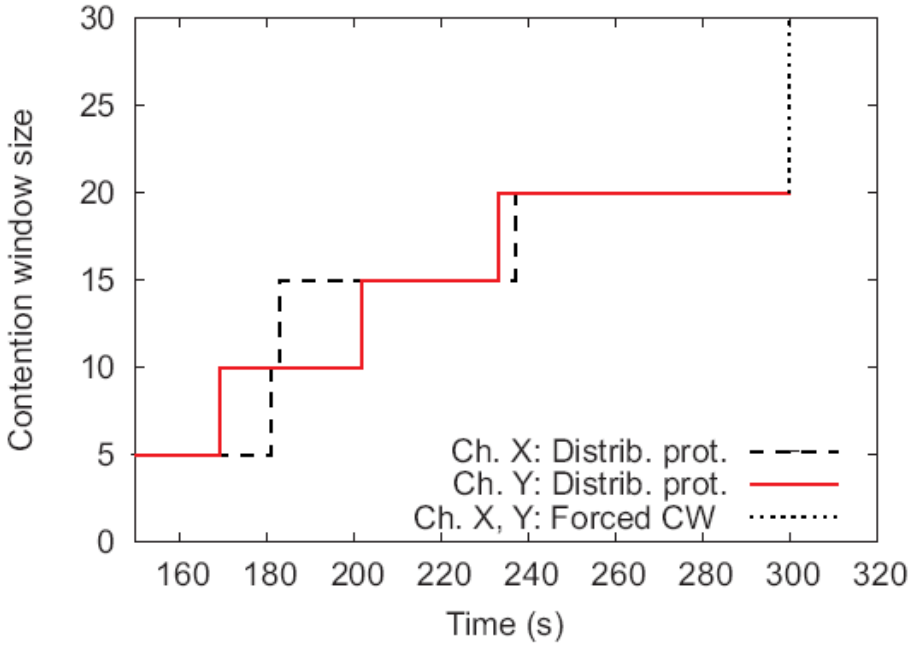
- X increase her W to $W_x^{init} + \gamma$.
- X detects all other cheaters as deviating: begin penalizing them.

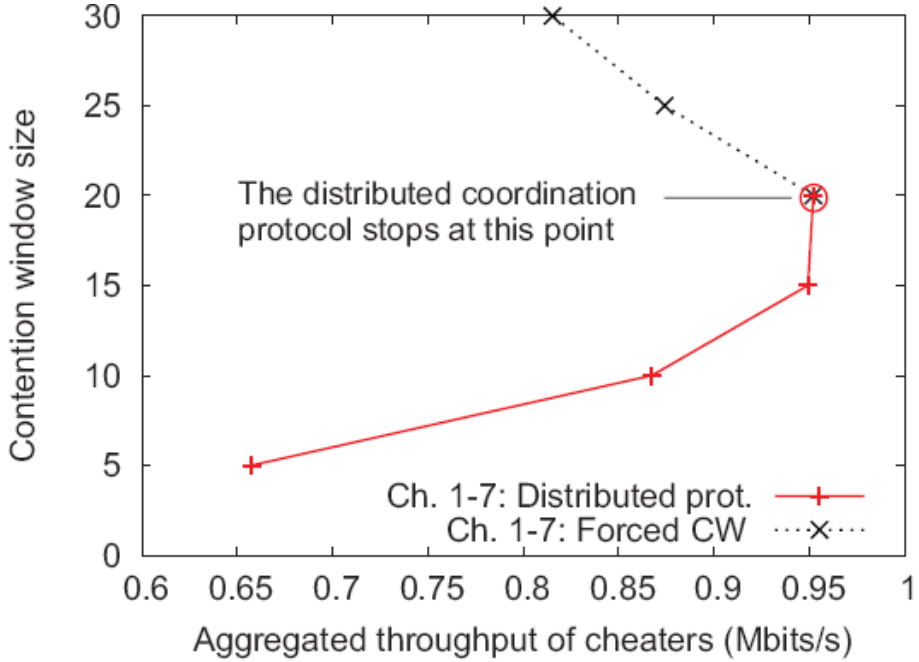
- Penalized cheater: disable the timer and use the adaptive strategy

- system will stabilize, when $W_i^{init} = W_i^{init} + \gamma$ for all.

- Then, every cheater compares her new throughput with previous:
- if a decrease in throughput: terminate the search for W*
- Otherwise: increase her W by γ.

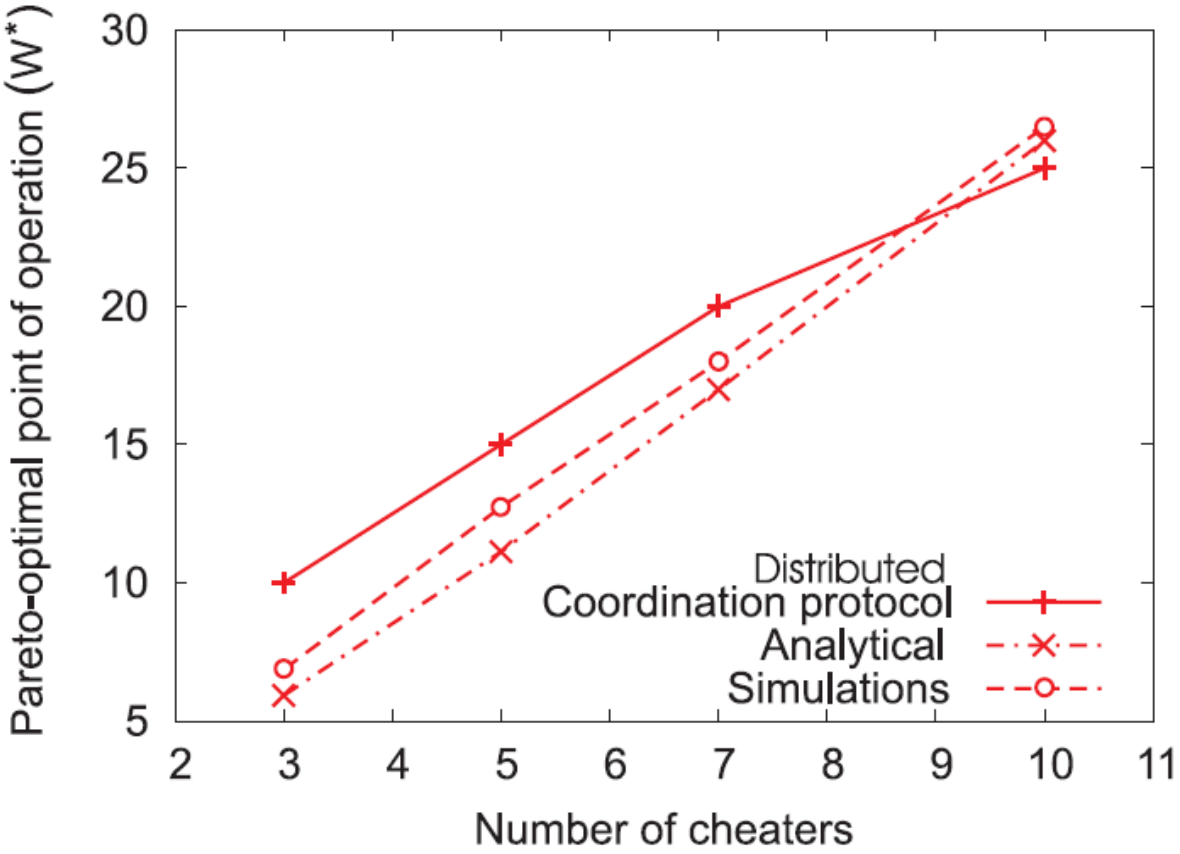
Fully Distributed Implementation





- 7 cheaters
- step size = 5

Fully Distributed Implementation



Summary of Section 9.3

- Addressed the Problem of cheating in single collision domain CSMA/CA networks
- Formalism for the systematic study of rational cheating in CSMA/CA ad hoc networks
- Single cheater as well as several cheaters acting without restraint
- Transformation of the Pareto optimal point into a Subgame Perfect Nash Equilibrium (repeated games)
- Smart cheaters can collectively find this point

Conclusion on Chapter 9

- Selfish behavior is relatively easy to implement at the MAC layer
- Upcoming technologies such as cognitive radios will further facilitate this kind of misbehavior
- In the case of IEEE 802.11, we have shown how to thwart it, both from the engineering and the analytical points of view.