Terminodes: Principles and Challenges

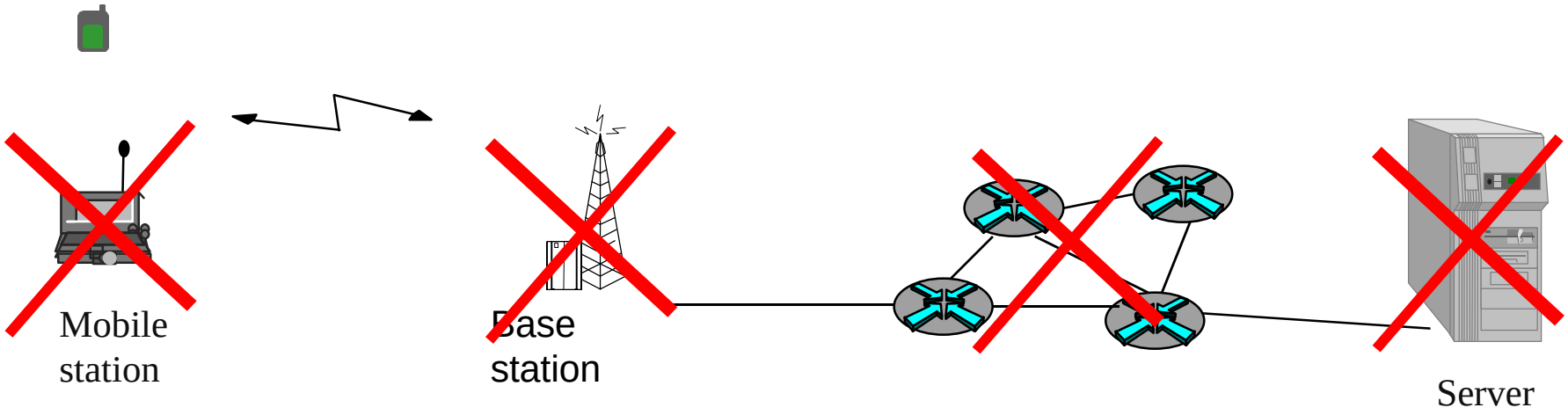
Mobile Information and Communication Systems

Prof. Jean-Pierre Hubaux

http://icawww.epfl.ch

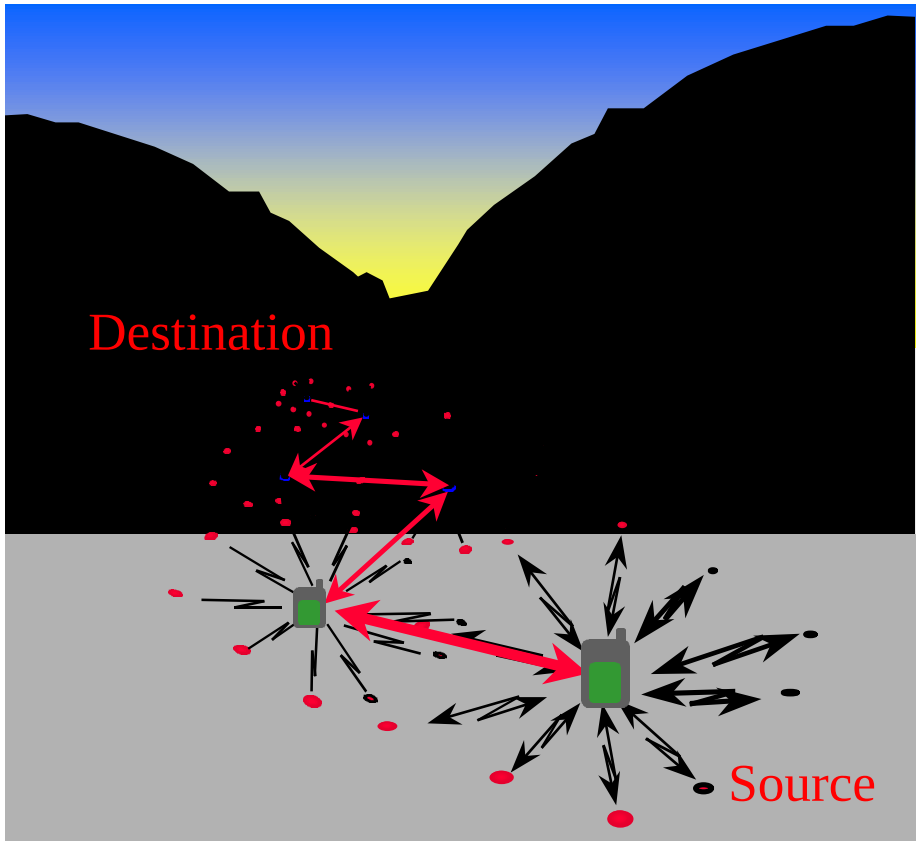
http://dscwww.epfl.ch

Self-Organized, Mobile, Infrastructureless WANs



Terminal + Node = Terminode

- All **network functions** (packet forwarding, flow control, error control,…) and **terminal functions** (coding/decoding, A/D and D/A, storage, ciphering,…) are embedded in the terminode
- All terminodes are potentially **mobile**
- A communication must be **relayed** by intermediate terminodes
- The **route** followed can be different for each packet
- A terminode is able to discover its own **environment** and to react accordingly
- The network is **self-organized**: no human intervention to define the addressing plan etc.



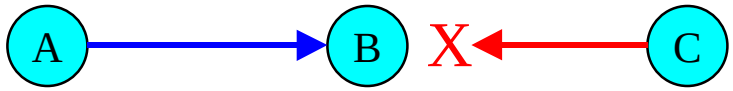
What are Terminodes?

- A societal/political vision
  - **Purpose**: make IT an instrument for democracy and economic development; empower citizens with communication facilities even in hostile environments
  - **Example**: *How would infrastructureless mobile communications foster economic development in remote or poorly equipped areas?*
- An intellectual fantasy
  - **Purpose**: stimulate creativity in order to identify new research challenges
  - **Example**: *What would be a formal model for fair exchange?*
- A technical challenge
  - **Purpose**: make innovative contributions in the area of self-organized mobile ad-hoc networks
  - **Example**: *What is the best way to track the terminals in such a network?*

Reminder: Packet Radio

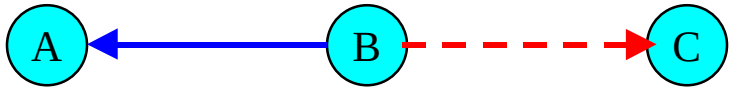
- Research started in the 70's, essentially with military applications in mind
- Unlike with cellular networks, the allocation of the transmission resource is decentralized (no base stations, no cells)
- Two typical problems:

The hidden terminal



- A is sending to B
- C is out of the range of A's transmitter
- C wants to send to B (or someone near to B); a collision occurs in B
- A is ***hidden*** from C

The exposed terminal



- B is sending to A
- C is in the range of B's transmitter
- C wants to send, but will wait; if A is out of the range of C, then C waits needlessly
- C is ***exposed*** to B

Upper Bound for the Throughput of Packet Radio Networks

If we have:

- n identical randomly located nodes

- each capable of transmitting W bits/s

Then the throughput $l(n)$ obtainable by each node for a *randomly chosen* destination is

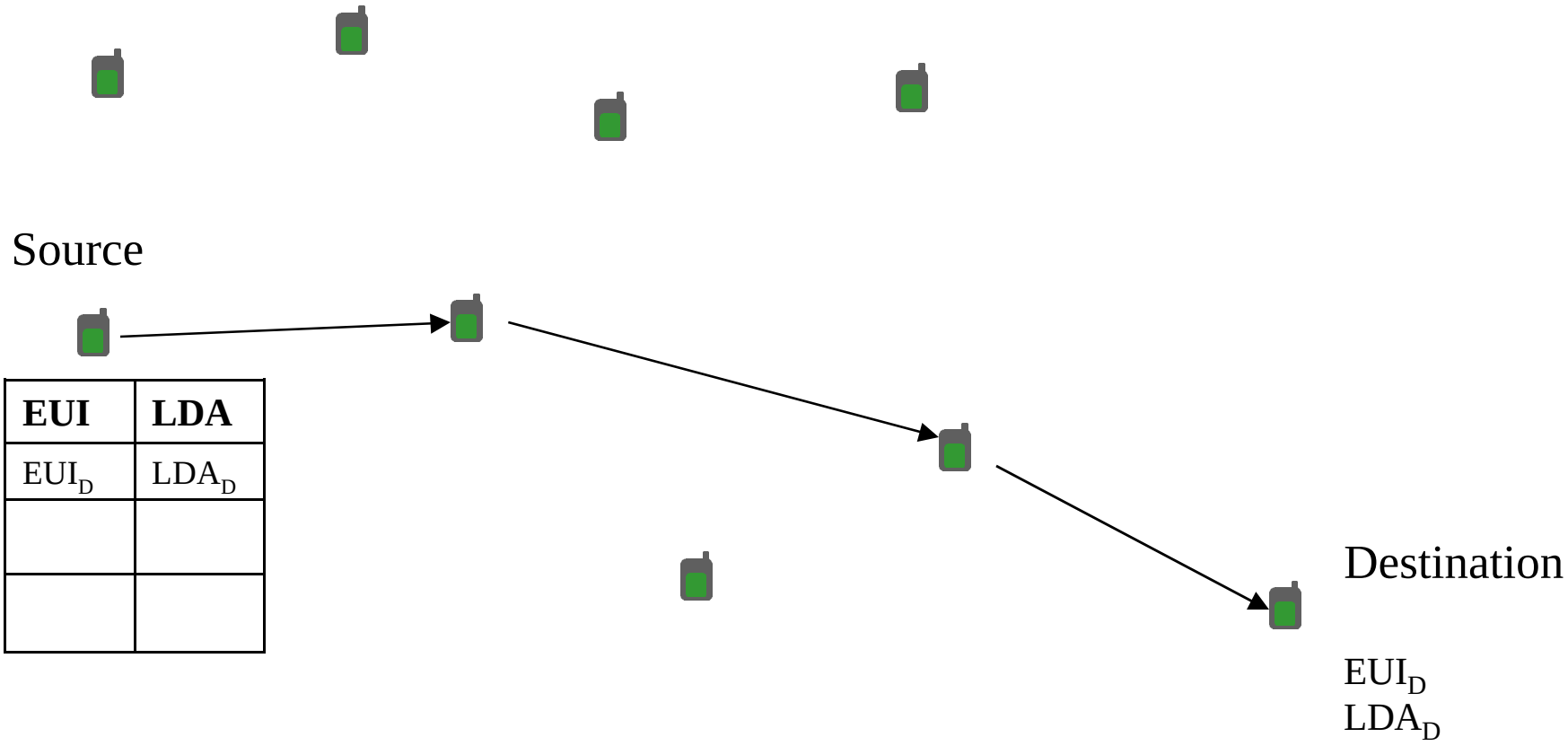
$$l(n) = \Theta\left(\frac{W}{\sqrt{n \log n}}\right)$$

Ref: P. Gupta, P. Kumar, ***The Capacity of Wireless Networks***
IEEE Transactions on Information Theory, March 2000

Technical Issues covered by this Talk

- Basic mechanism for terminodes: packet forwarding, location awareness
- Mobility management of terminodes
- Incentive to collaborate for terminodes

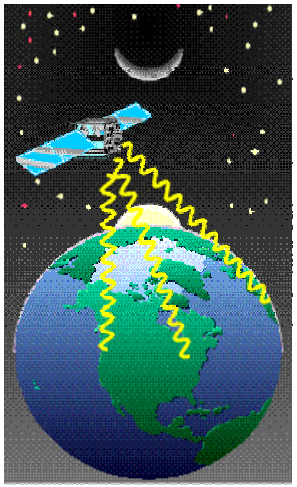
Packet Forwarding in Terminodes

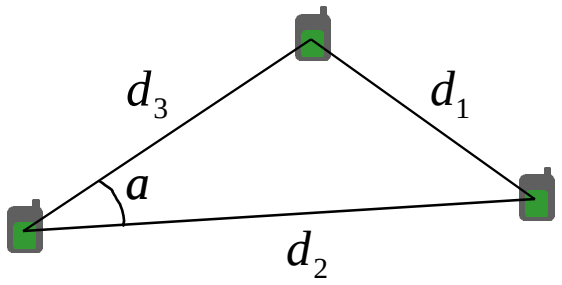


EUI	LDA
EUI_D	LDA_D

EUI: End-system Unique Identifier (64 bits)
LDA: Location-Dependent Address: (longitude, latitude, height) (approx. 48 bits for 10m accuracy)

Location Awareness



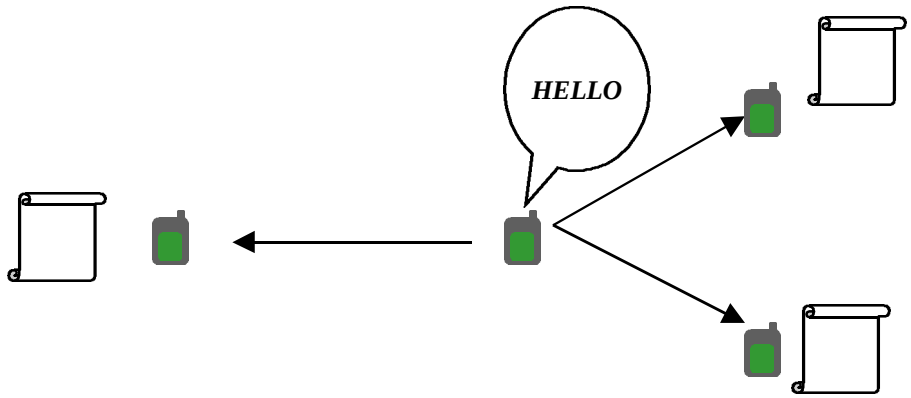


$$\cos a = \frac{d_1^2 - d_2^2 - d_3^2}{2 d_2 d_3}$$

If GPS is available: Each node is aware of its own Location-Dependent Address (LDA) via GPS (Global Positioning System).

If GPS is not available: computation of relative positions based on Time of Arrival.
Major Pb: *Non-Line-of-Sight*

Neighborhood Awareness

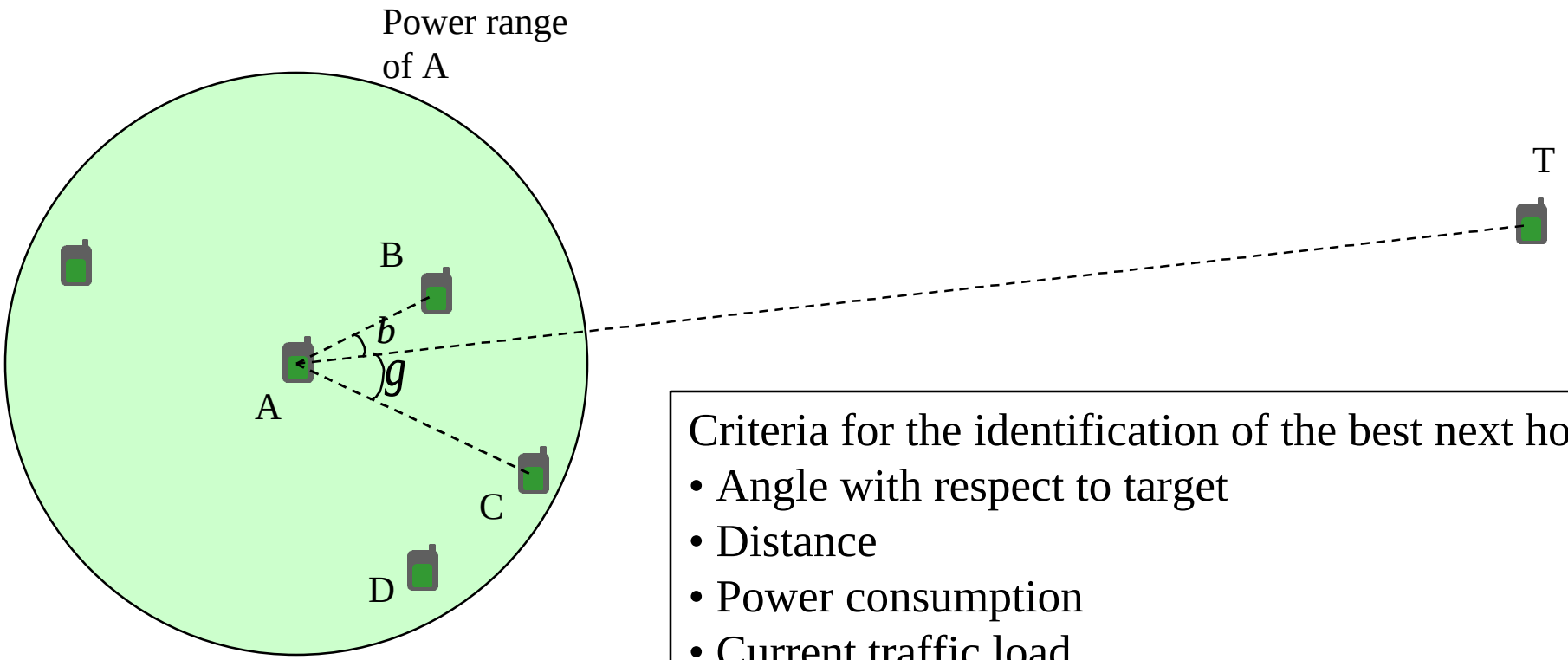


Periodic Broadcast of *Hello* Messages with current position of the sender.

Applications:

- Code negotiation (for spread spectrum)
- Power control
- Establishment of pairwise security keys

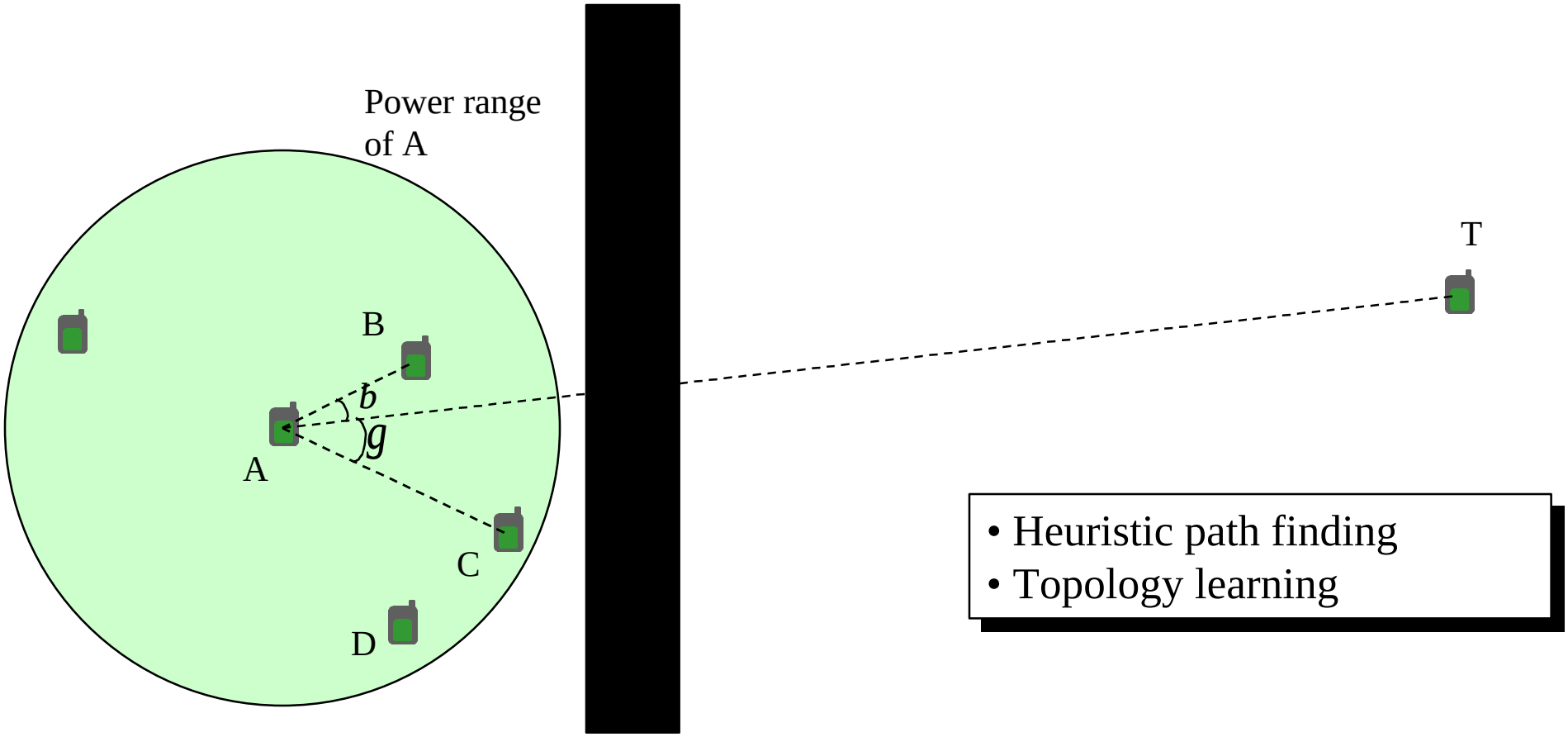
Directional Packet Forwarding



Criteria for the identification of the best next hop:

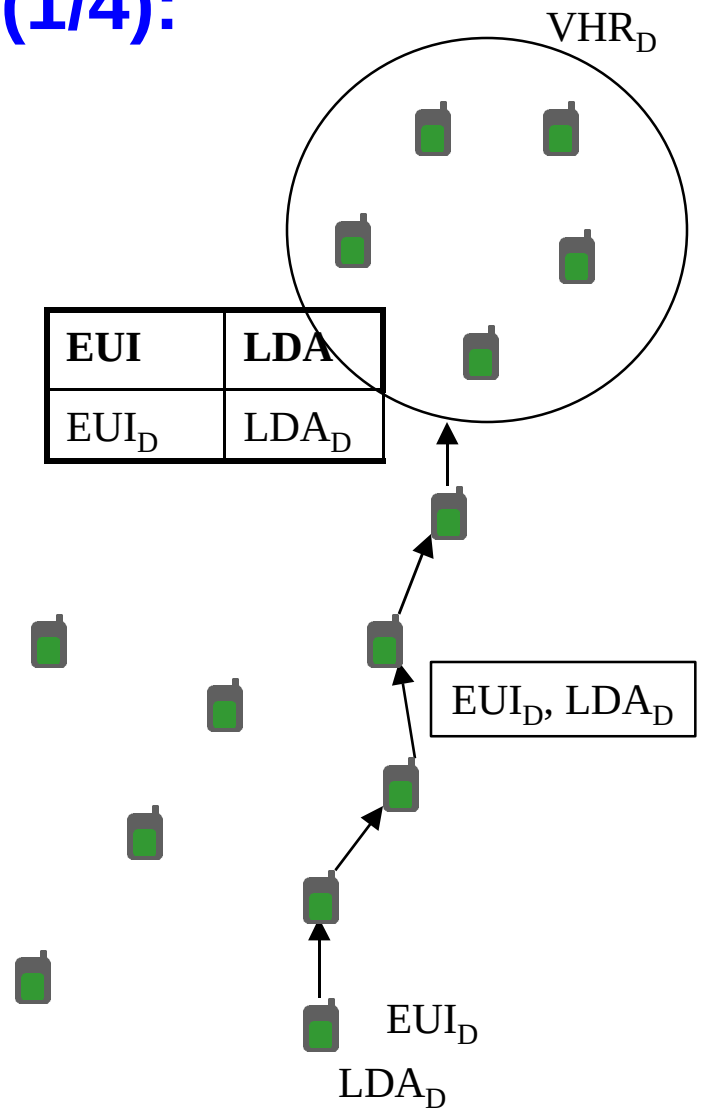
- Angle with respect to target
- Distance
- Power consumption
- Current traffic load
- …

Obstacle Avoidance



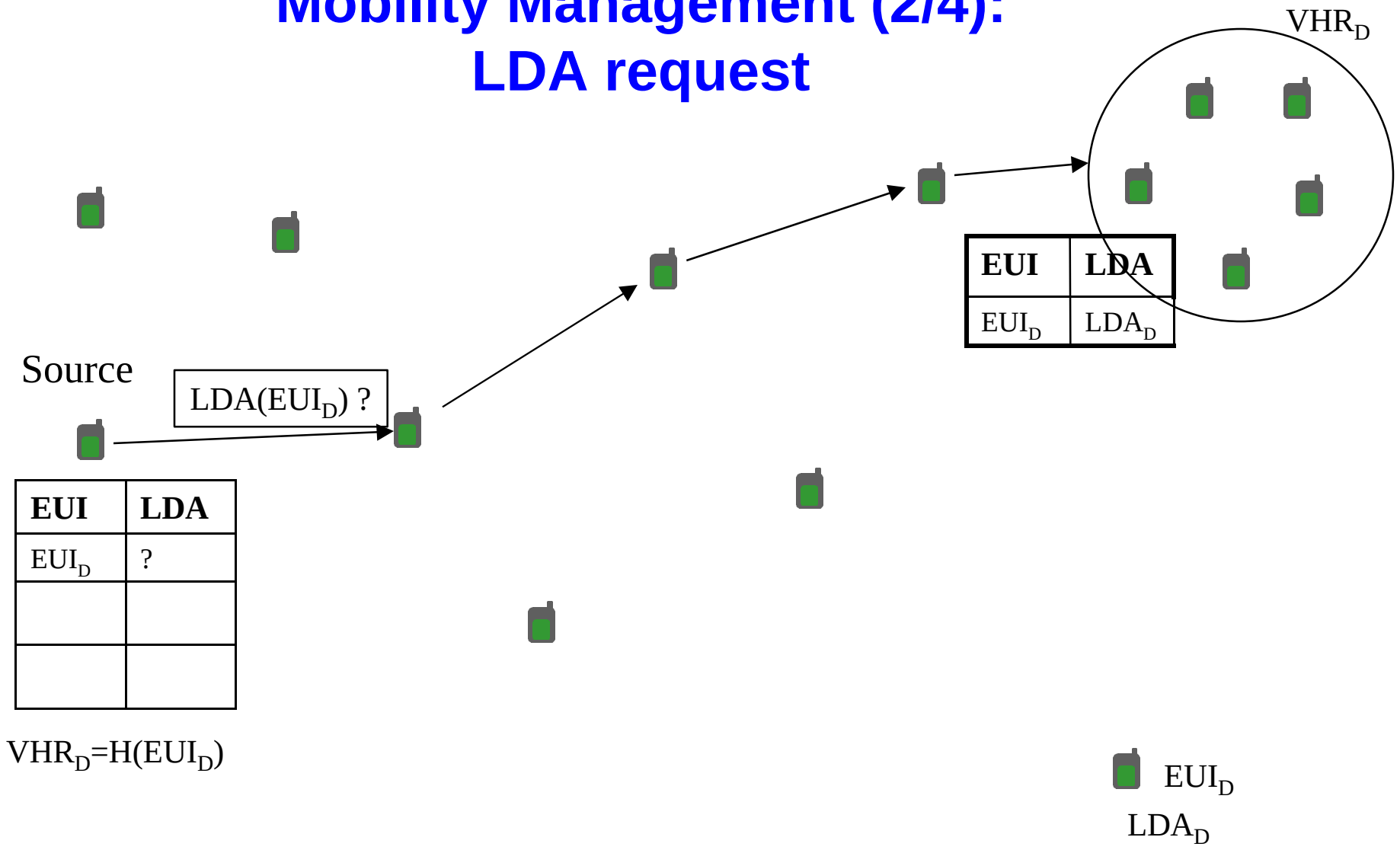
- Heuristic path finding
- Topology learning

Mobility Management (1/4): LDA storage



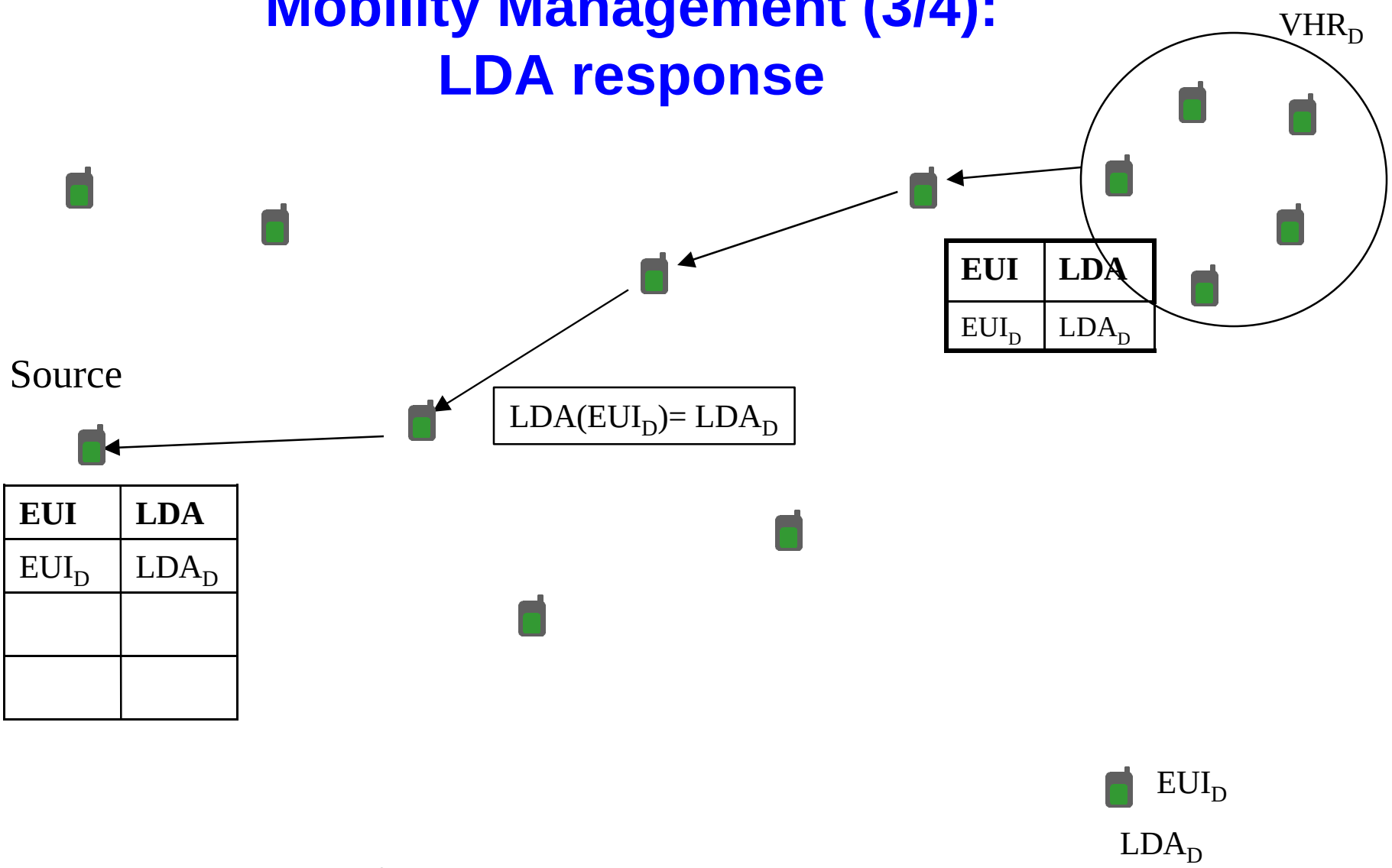
EUI: End-system Unique Identifier
LDA: Location-Dependent Address
VHR: Virtual Home Region

Mobility Management (2/4): LDA request



EUI: End-system Unique Identifier
LDA: Location-Dependent Address
VHR: Virtual Home Region

Mobility Management (3/4): LDA response

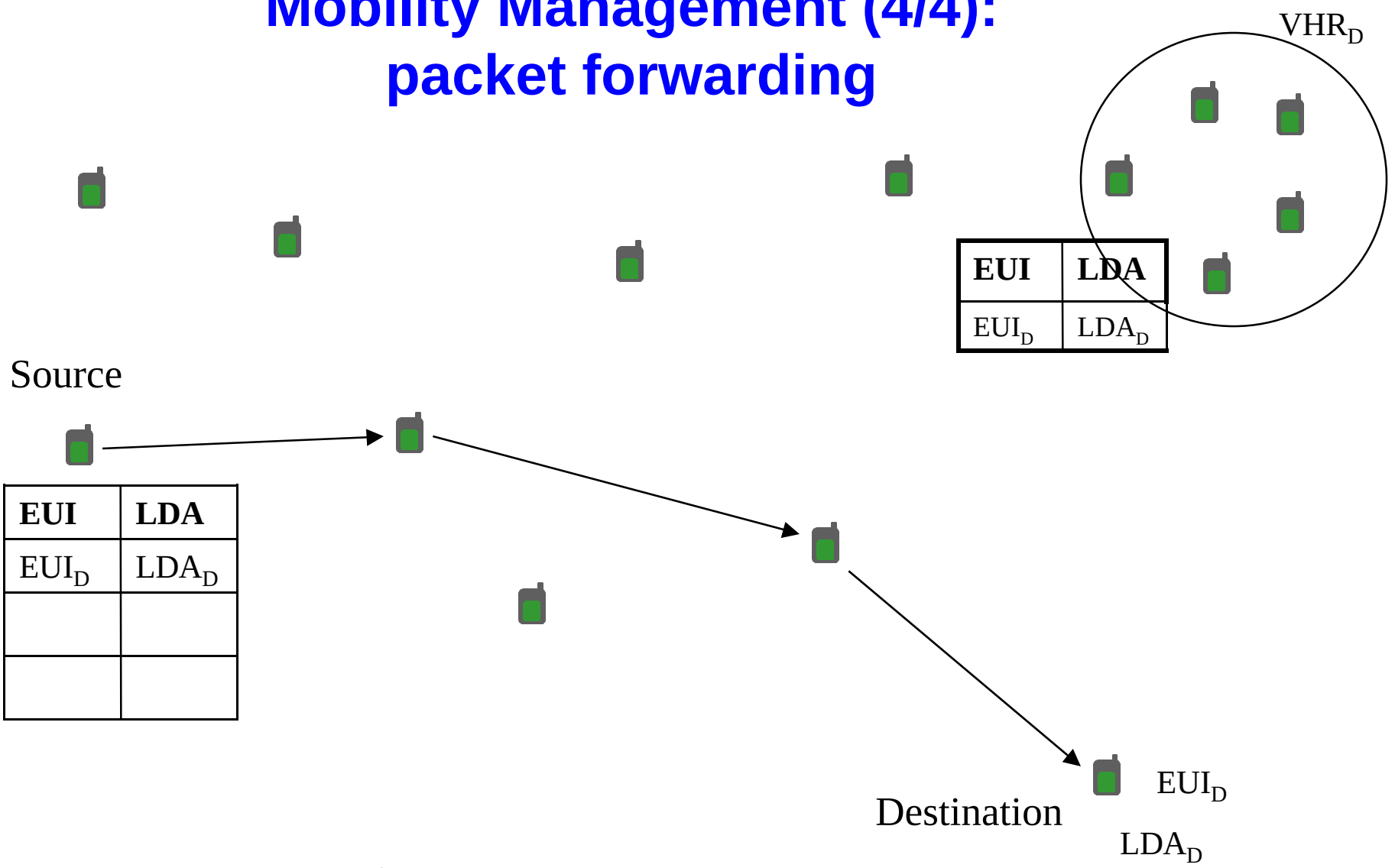


EUI	LDA
EUI$_D$	LDA$_D$

EUI	LDA

EUI: End-system Unique Identifier
LDA: Location-Dependent Address
VHR: Virtual Home Region

Mobility Management (4/4): packet forwarding

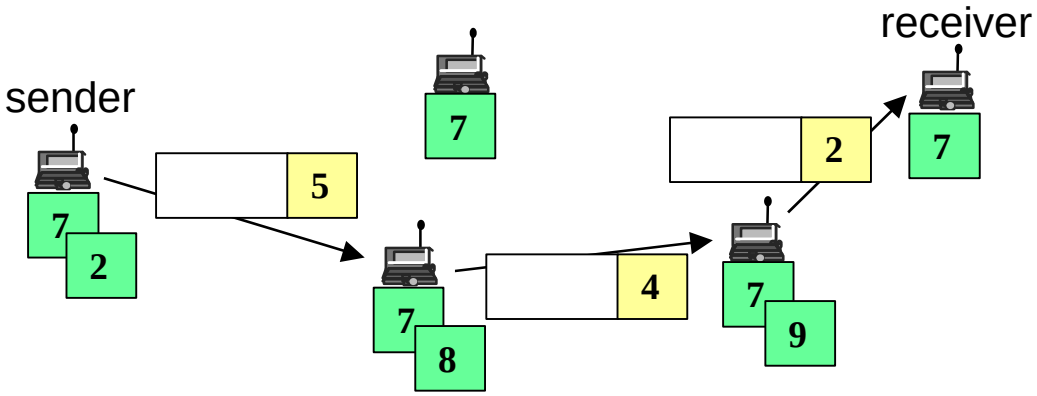


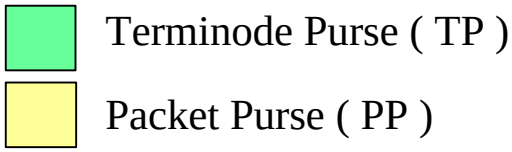
EUI: End-system Unique Identifier
LDA: Location-Dependent Address
VHR: Virtual Home Region

Incentive to cooperate and to prevent congestion

- Mechanism required to:
  - Encourage end-users to let their terminode **act as a relay** (keep them turned on and not tamper with them)
  - Discourage end-users from **overloading** the network; in particular, limit the number of long distance communications
- 2 models
  - Packet Purse Model (payment by the sender)
  - Packet Trade Model (payment by the receiver)

Charging the sender: Packet Purse Model (PPM)



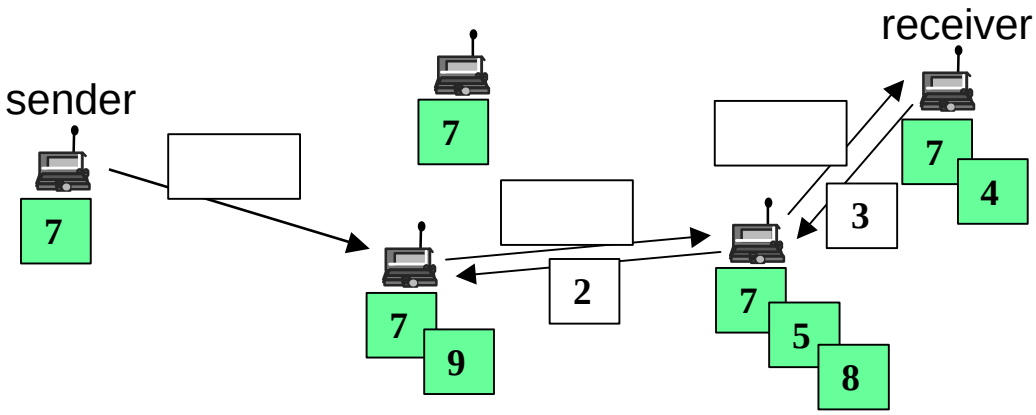


$$PP_r(p_k) = PP_s(p_k) - \sum_{i=1}^{n} C_i(p_k)$$

Problems to be solved include:

- **Nugget forgery** should be prevented
- **Nugget robbery** should be prevented
- Each packet should **indeed** be forwarded
- The packet purse should be **bundled** to its packet

Charging the receiver: Packet Trade Model (PTM)



Terminode Purse (TP)

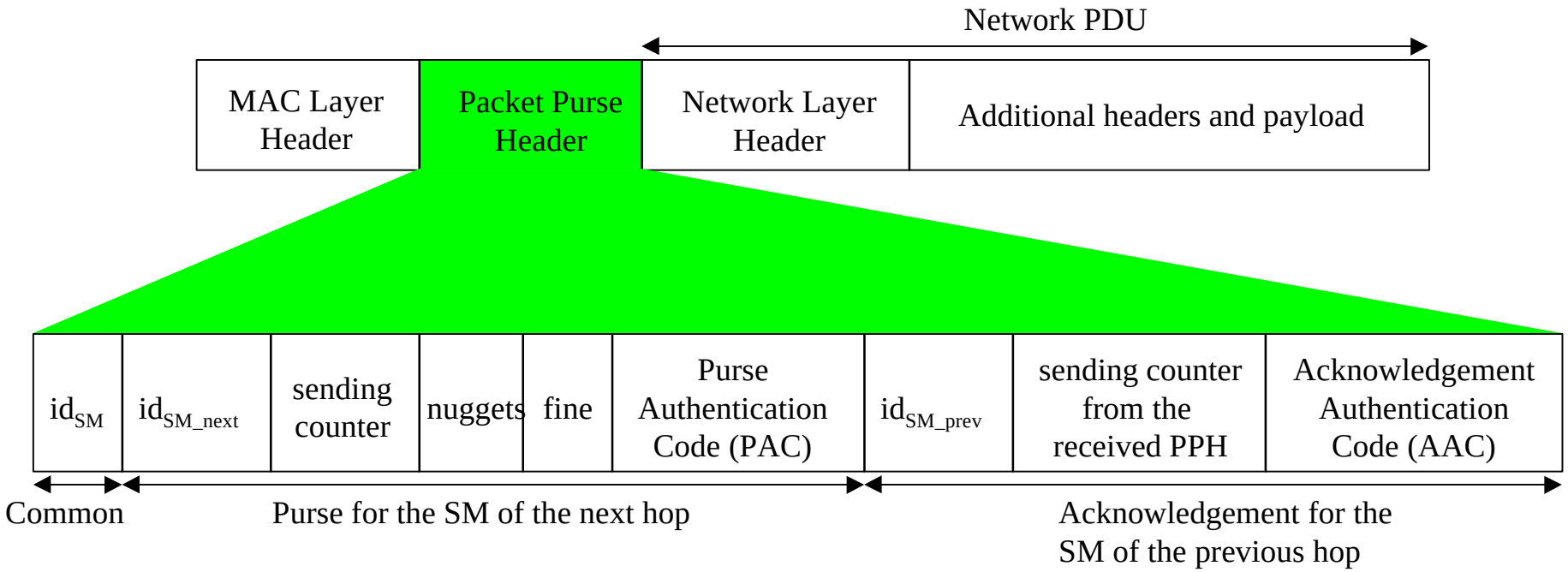
$$TP(r) := TP(r) - \sum_{i=1}^{n} C_i(p_k)$$

- Advantages
  - The sender does not need to know the **amount of nuggets** that is necessary to send a packet
  - Intermediaries are **interested** in forwarding the packet after having bought it
  - Charging for **multicast** communications is easier
- Drawback
  - There is no direct incentive to refrain from overloading the network

Implementation: Assumptions

- Tamper resistant **security module** in each device, which is used for the management of nuggets and cryptographic keys
- **Public key infrastructure** that can be used by the security modules to authenticate each other and establish secure communication links
- Neighborhood changes **slowly** (at least compared to the speed of the packets)
- **Reliable, bidirectional communication** between neighbors
- **Pricing** mechanism
- Terminodes are **greedy** and they always want to increase their number of nuggets

Implementation of PPM: Packet Purse Header (PPH)

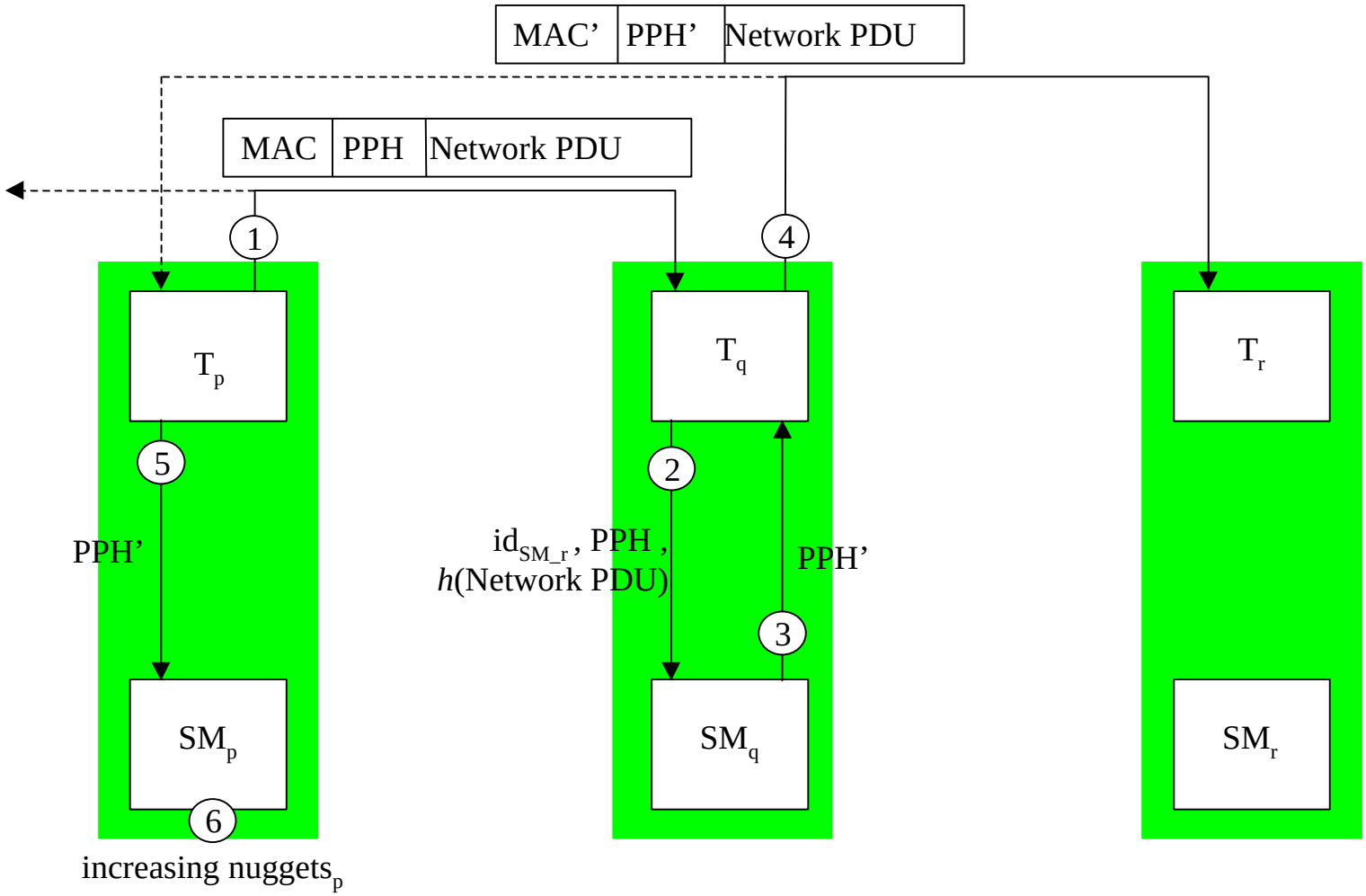


$PAC = g(k_{SM,SM\_next}; id_{SM}, id_{SM\_next}, \text{sending counter, nuggets, fine, } h(\text{Network PDU}))$

$AAC = g(k_{SM,SM\_prev}; \text{received PPH})$

g is a publicly known keyed cryptographic hash function
h is a publicly known cryptographic hash function

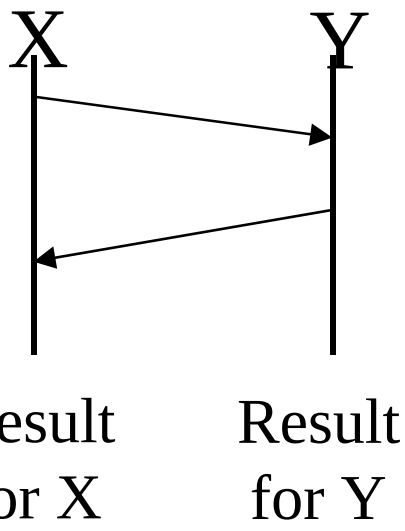
Implementation of PPM: Packet forwarding protocol



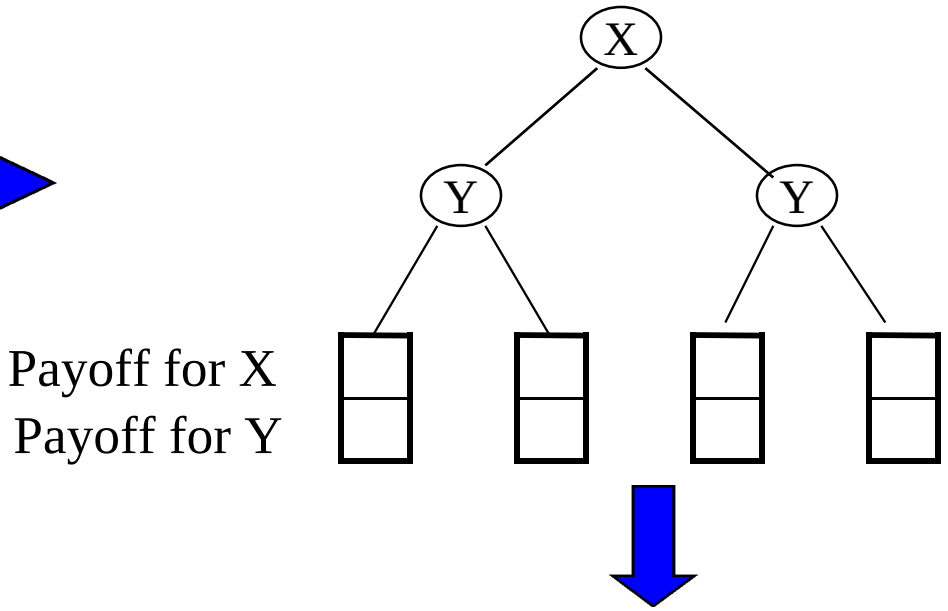
PPH: Packet Purse Header

Modeling exchange protocols using game theory

1. Protocol Design



2. Modelling as a game tree



3. Analysis of the payoffs

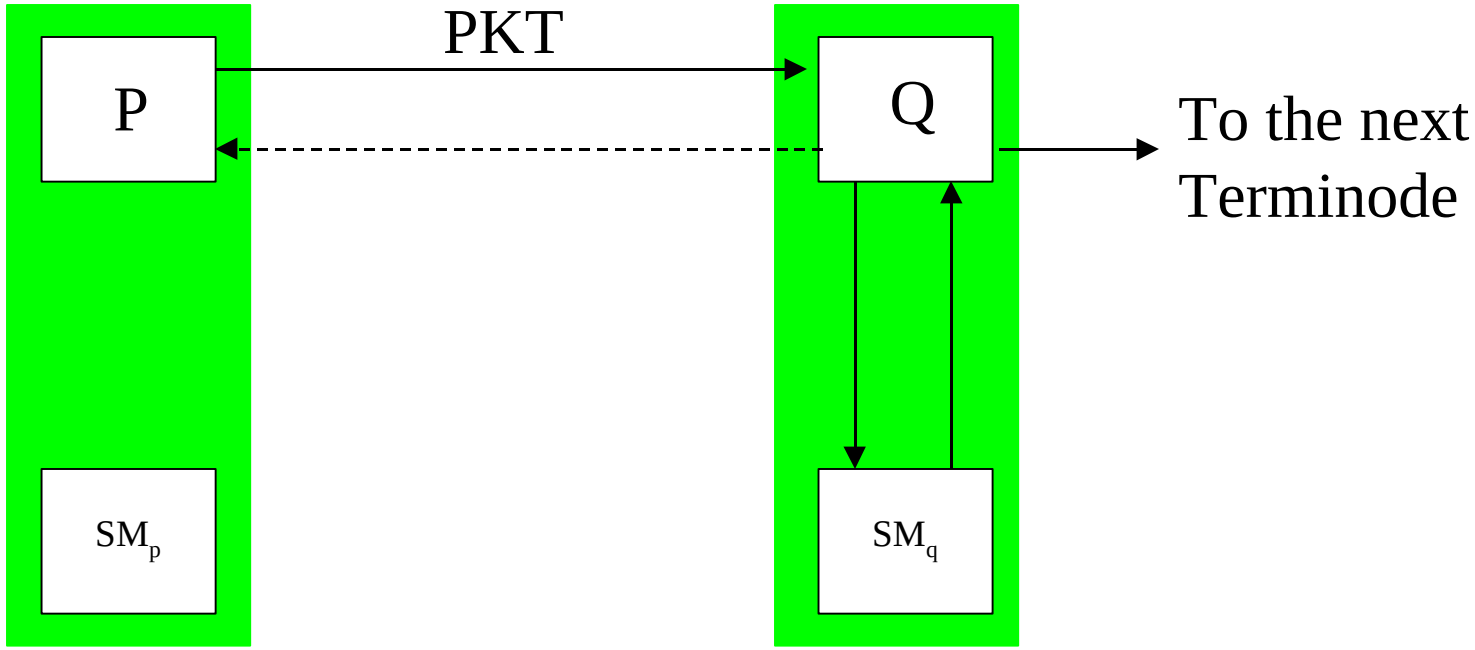
X strategies \ Y strategies			
Payoffs for X and Y			

4. Identification of the properties

- Fairness
- Incentive for desirable behaviours

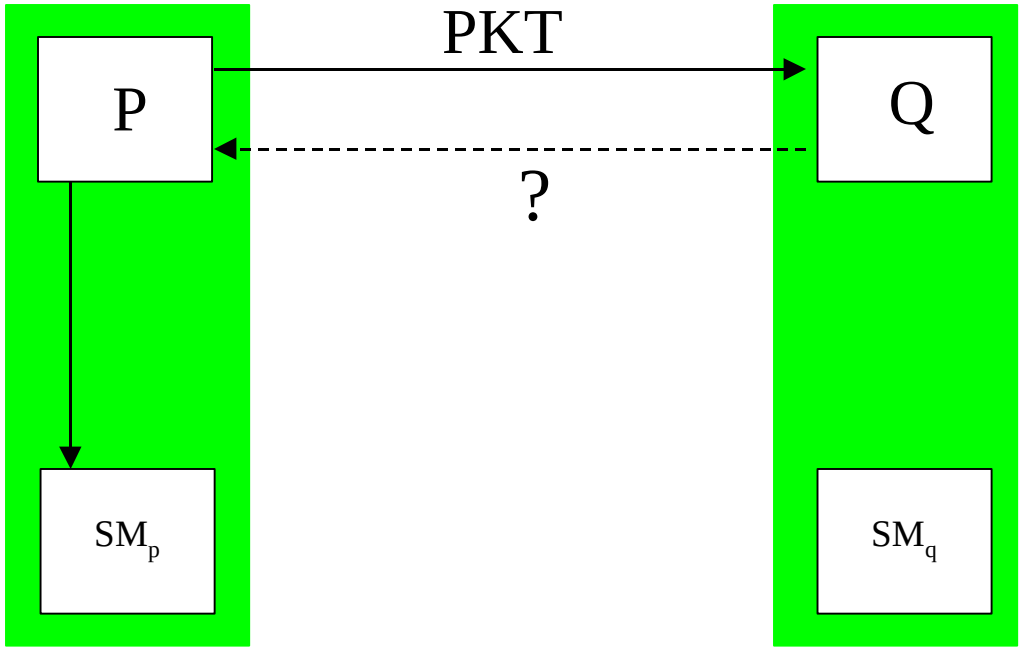
Example of practical usage:
- Fine tuning of the parameters

Modeling packet forwarding as a game: Q's behavior

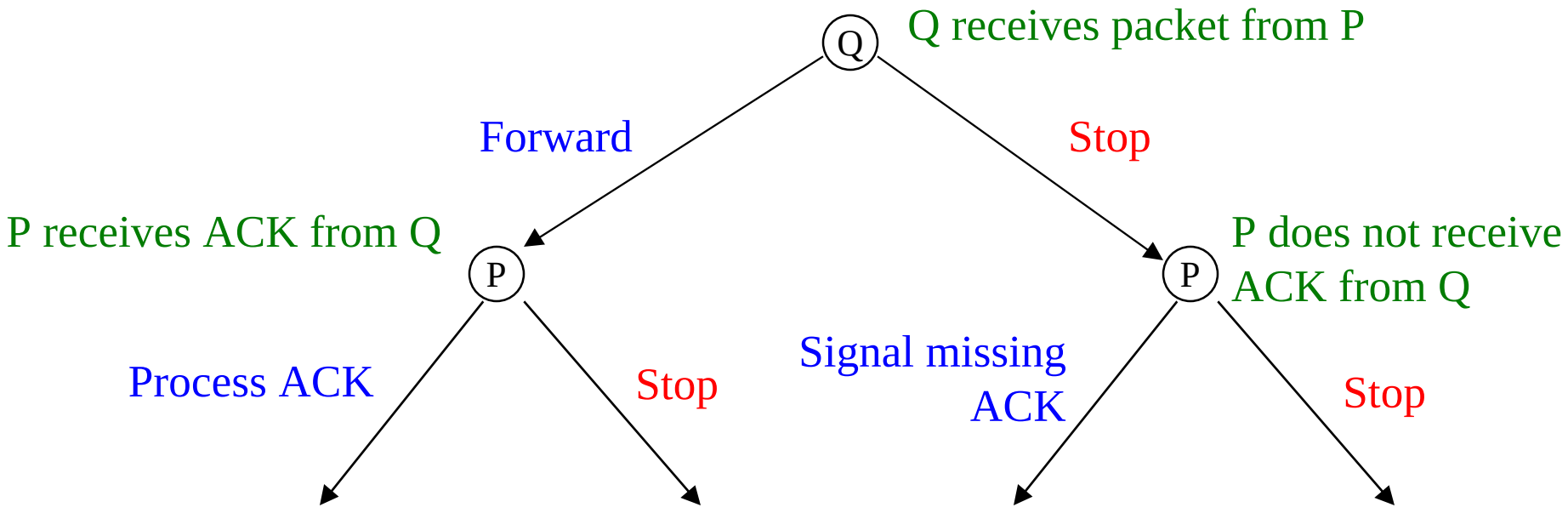


Modeling packet forwarding as a game: P's behavior

Process ACK
or
Report missing ACK
(in order to inflict fine)



Payoff for each player in packet forwarding



	P	Q
Earned nuggets	1	$h-1$
Energy	$-c$	$-c$

P	Q
0	$h-x\,f$
$-c$	0

P	Q
1	$-x\,f$
$-c$	0

P	Q
0	0
$-c$	0

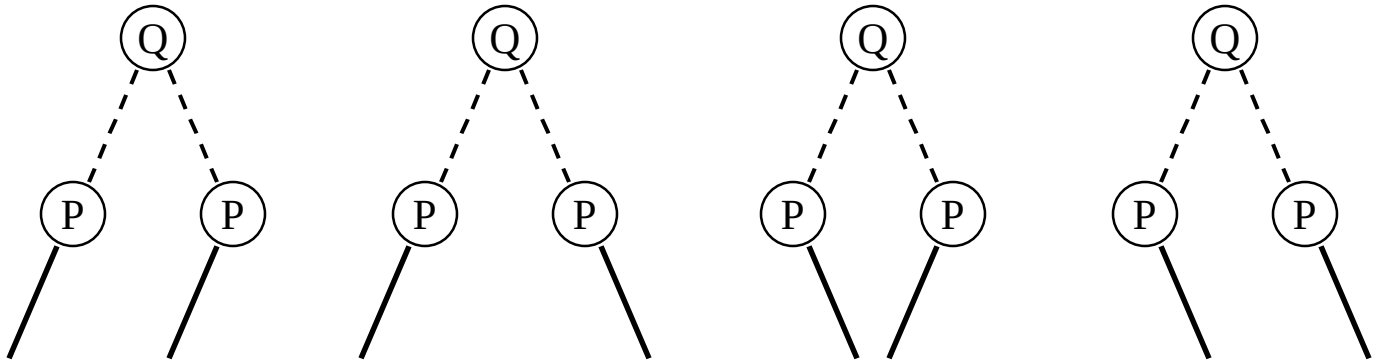
c : cost

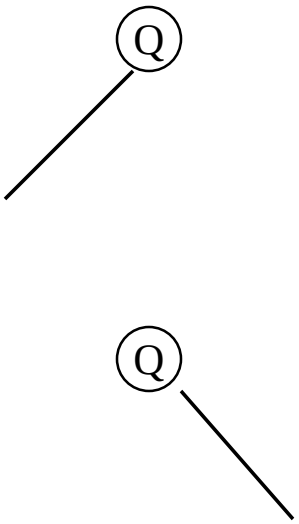
f : fine

h : probability that Q will eventually receive payment from R

x : probability that the fine will eventually be inflicted to Q

Identification of the strategies





Payoff for P and Q			

Analysis of the strategies

Q \ P	Process ACK/ Signal missing ACK	Process ACK/ Stop	Stop/ Signal missing ACK	Stop/ Stop
Forward	P: 0 Q: $h-1$	P: 0 Q: $h-1$	P: -1 Q: $h-x\,f-1$	P: -1 Q: $h-x\,f-1$
Stop	P: -1 Q: $-x\,f$	P: -1 Q: 0	P: -1 Q: $-x\,f$	P: -1 Q: 0

A

B

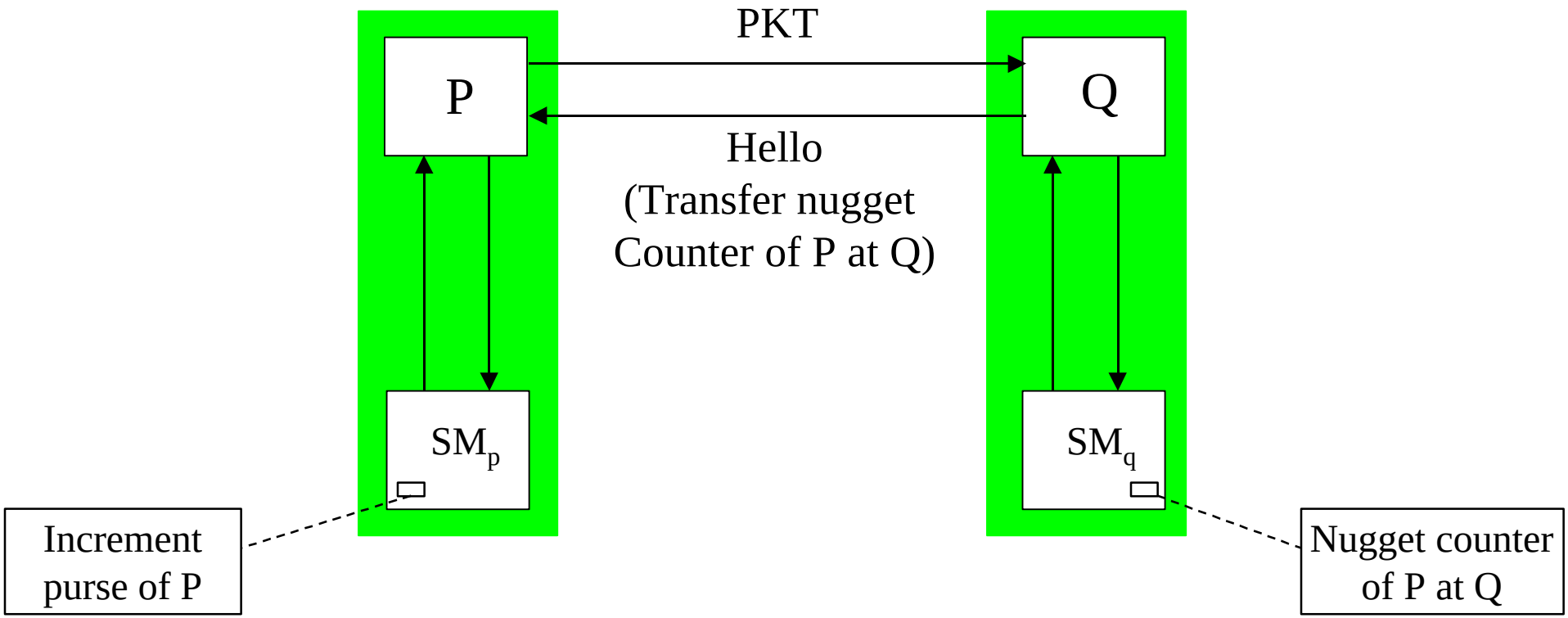
Weakly dominated by the two left columns

$$h-1>-x\,f \Rightarrow f>\frac{1-h}{x} \qquad (1)$$

A : desired Nash equilibrium

B : undesired Nash equilibrium

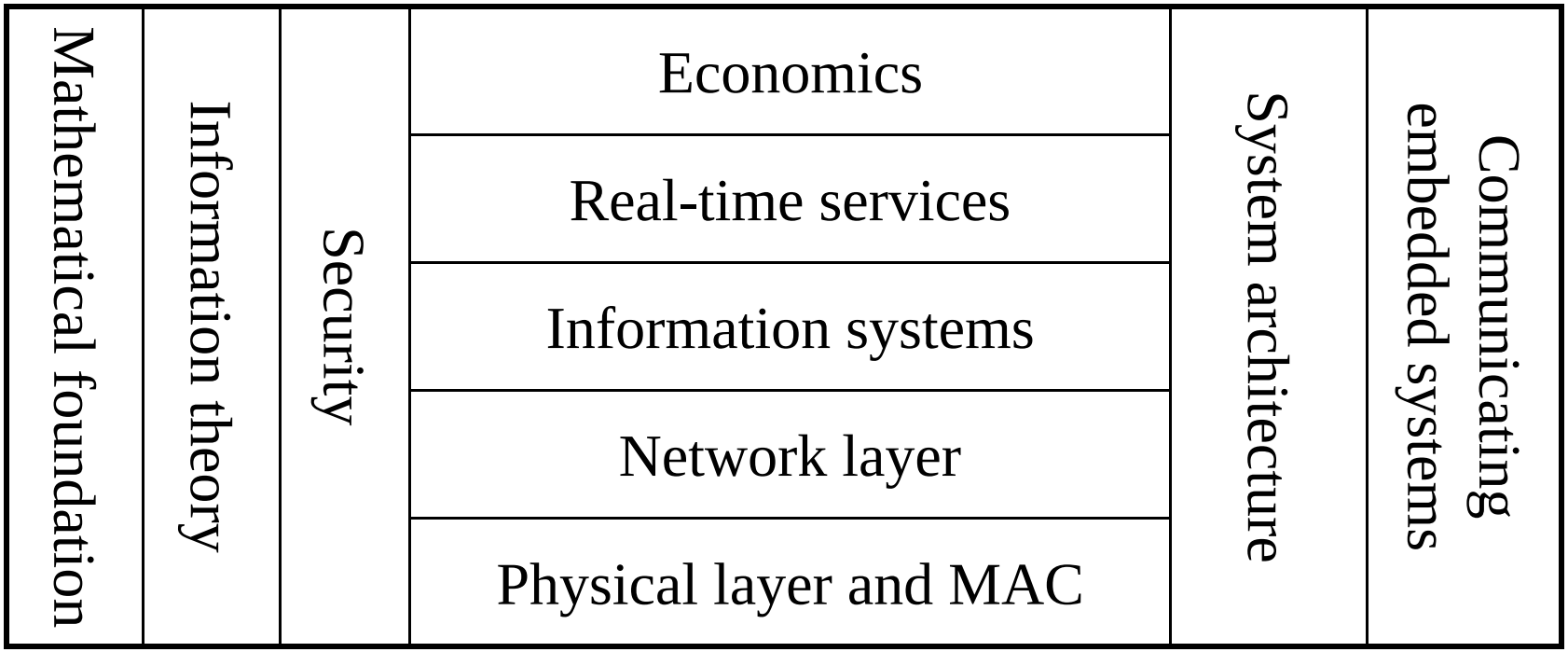
Alternative solution
(non real-time increase of the Terminode Purse)



Conclusion on the incentive to cooperation

- In self-organized mobile ad hoc networks, the **cooperation mechanisms** have to be carefully scrutinized
- Some form of **funny money** (nuggets) can be introduced to incentivate cooperation
- **Game theory** can be used to study the properties of exchange protocols
- **Future work**:
  - Reduce the overhead (statistical mechanisms?)
  - Get rid of the assumption of communication bidirectionality

Main challenge and benefit : Working accross layers



Related Projects

- Carnegie-Mellon: Monarch
  - Testbed
  - Routing protocols (proposal: Dynamic Source Routing Protocol)
- MIT/LCS: Wireless Network of Devices (WIND)
  - Energy-efficient routing
  - Intentional Naming System
- Cornell Univ./EE Dept
  - Zone Routing Protocol (ZRP)
  - Mobility management with Uniform Quorum Systems (UQS) and Randomized Database Group (RDG)
- Georgia Tech/School of ECE: Associativity-Based Routing (ABR)
- SUN: Ad Hoc on Demand Distance Vector Routing (AODV)
- UCLA/CS Dept: Clustering
- Univ. of Texas at Dallas/CS Dept: Clustering
- IETF: MANET Working Group
- …

References on the Project

- ***Terminodes: Toward Self-Organized Mobile Wide Area Networks***
  JP Hubaux,
  Technical Report SSC/1999/022, June 3, 1999
- ***The Terminode Project: Towards Mobile Ad-Hoc WANs***
  JP Hubaux, JY Le Boudec, S. Giordano, M. Hamdi,
  IEEE Mobile Multimedia Conference, San Diego, November 1999 (MOMUC'99)
  Technical Report SSC/1999/031, Nov. 99
- ***Toward Mobile Ad-Hoc WANs: Terminodes***
  JP Hubaux, JY Le Boudec, M. Vojnovic, S. Giordano, M. Hamdi, L. Blazevic, L. Buttyan
  Technical Report SSC/2000/006, February 2000
- ***Enforcing Service Availability in Mobile Ad-Hoc WANs***
  L. Buttyan, JP Hubaux
  Technical Report SSC/2000/025, April 2000; accepted for publication at MobiHoc'00

- ***Toward a Formal Model of Fair Exchange - a Game Theoretic Approach***
  L. Buttyan, JP Hubaux
  Technical report No. SSC/1999/039, December 1999

All documents available at http://dscwww.epfl.ch. See also http://www.terminodes.org