Enforcing Service Availability in Mobile Ad-Hoc WANs

***Levente Buttyan et al** (Swiss Federal Institute of Tech.)*

1st IEEE/ACM Workshop on
Mobile Ad Hoc Networking and Computing

October 28, 2002

Uichin Lee
CA-LAB CS KAIST

Agenda

- Introduction
- Rewarding the packet forwarding
- General Assumption
- Implementing the models
- Analysis
- Conclusion

Introduction (1/2)

- ***Terminodes*** Project
  - Research on *mobile ad-hoc wide area network*
  - ***Terminode***
    - A small, portable device
    - Autonomous
    - Large size of the network; a *terminode* network
    - Communication based on packet switched, multi-hop, wireless communication of voice and data
      - ***Packet forwarding*** mechanism lets each of the *terminodes* located on the route of a given packet compute the "best" next hop toward the final destination

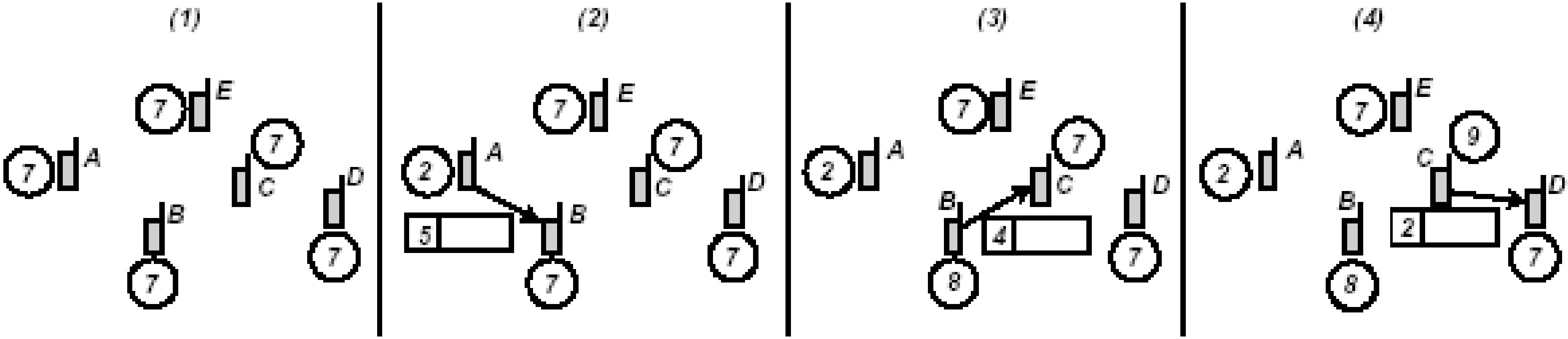
Introduction (2/2)
- Availability of services in terminode network

- Two aspects of ***availability*** in *terminode* networks
  - Stimulation for cooperation
    - Dearth of energy makes users have little interest in ***service provision***, so they are not cooperative each other
    - Short term and cooperative env.(an ad-hoc network) vs long term and uncooperative env.(a *terminode* network)
  - Prevention of overloading
    - Overloading the network with a malicious denial-of-service attack or a user sending too much information
    - Need a mechanism that makes DOS attacks expensive and discourages users from flooding

Rewarding Packet Forwarding

- How to stimulate a cooperative behavior and prevent congestion?
  - The concept of money and service charges
  - If a *terminode* wants to use a service (sending a message), then it has to pay for it in nuggets and vice versa
- A *terminode* currency called ***nuggets***
- Models to reward the packet forwarding service
  - The Packet Purse Model (PPM)
  - The Packet Trade Model (PTM)

Rewarding Packet Forwarding
- The Packet Purse Model

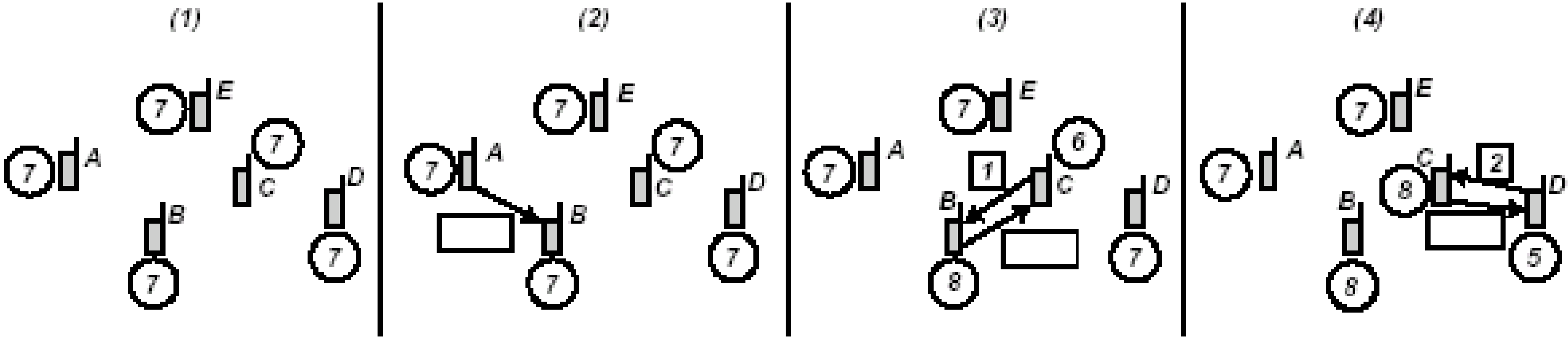


⑦ Stock of nuggets at the *terminode*

$\boxed{5}$ Number of transferred nuggets

- Estimation of number of nuggets to reach a destination
  - Over vs. under estimation

Rewarding Packet Forwarding
- The Packet Purse Model



⑦ Stock of nuggets at the *terminode*

$\boxed{5}$ Number of transferred nuggets

- No need to know in advance the number of nuggets to deliver the packet
- Could not deter users from ***flooding*** the network
    - Allow each *terminode* to decide whether to buy a packet or not
    - Thus it provides a sort of "***back pressure***" mechanism

Rewarding Packet Forwarding
- Problems

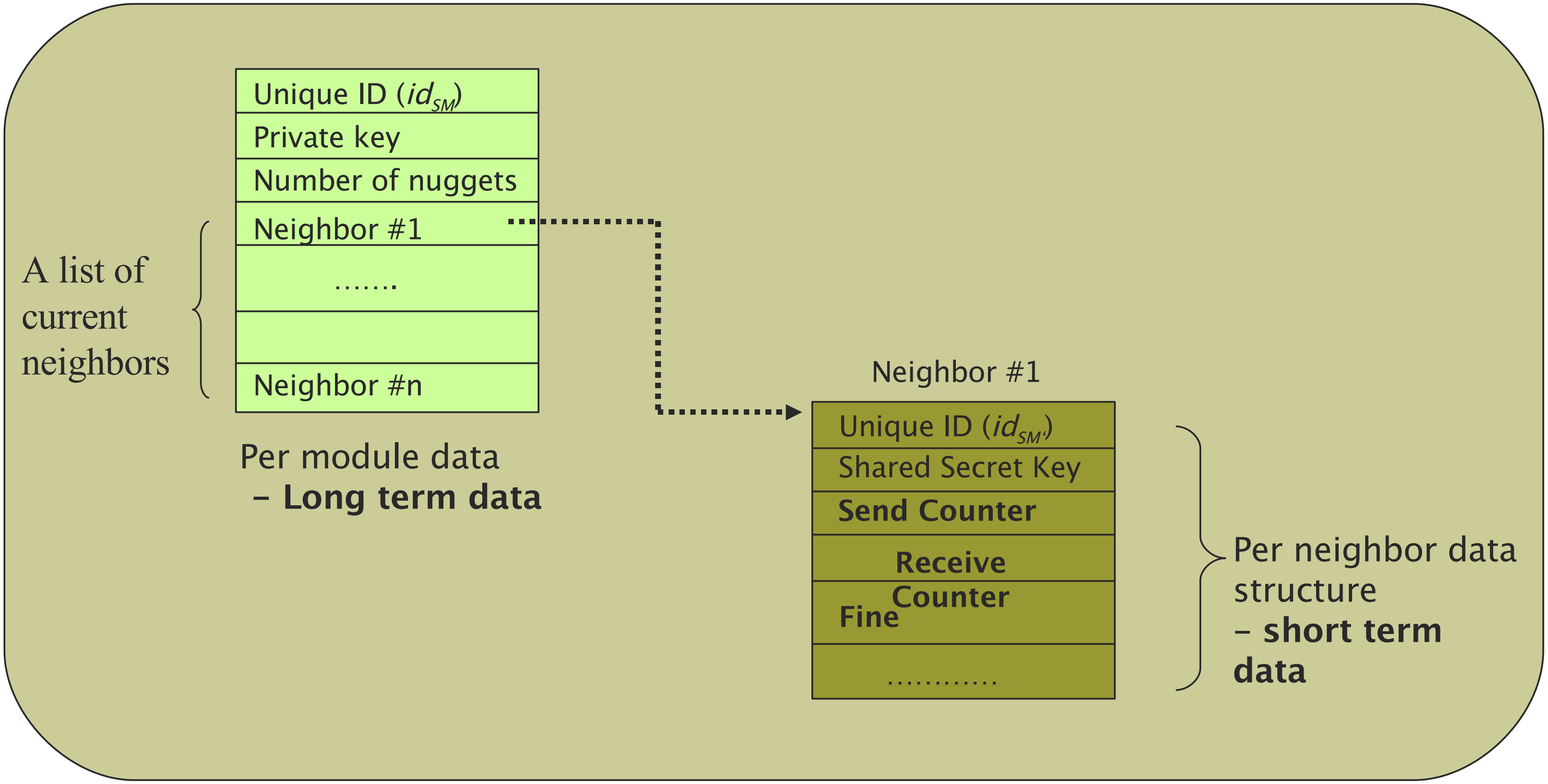
- Nugget forgery and re-use
- Replay
- Packet Purse Model
  - Packet robbery; taking nuggets out of the packet illegally
  - Taking nuggets and then exact forwarding
- Packet Trade Model
  - Fairness of the exchange

Rewarding Packet Forwarding
- Assumptions

- Tamper resistant security module (SM)
- Public key infrastructure (secure com links)
- Slowly changing neighborhood
- Omni directional antennae
- Symmetry of the neighbor relationship
- Reliable communication between neighbors
- Pricing
- *Terminodes* are greedy
- No network operator

Implementation of Models
- A Security Module in each terminode

- The tamper-proof Security Module (SM)



A list of current neighbors

Unique ID (id_{SM})

Private key

Number of nuggets

Neighbor #1

....

Neighbor #n

Per module data
– **Long term data**

Neighbor #1

Unique ID ($id_{SM'}$)

Shared Secret Key

Send Counter

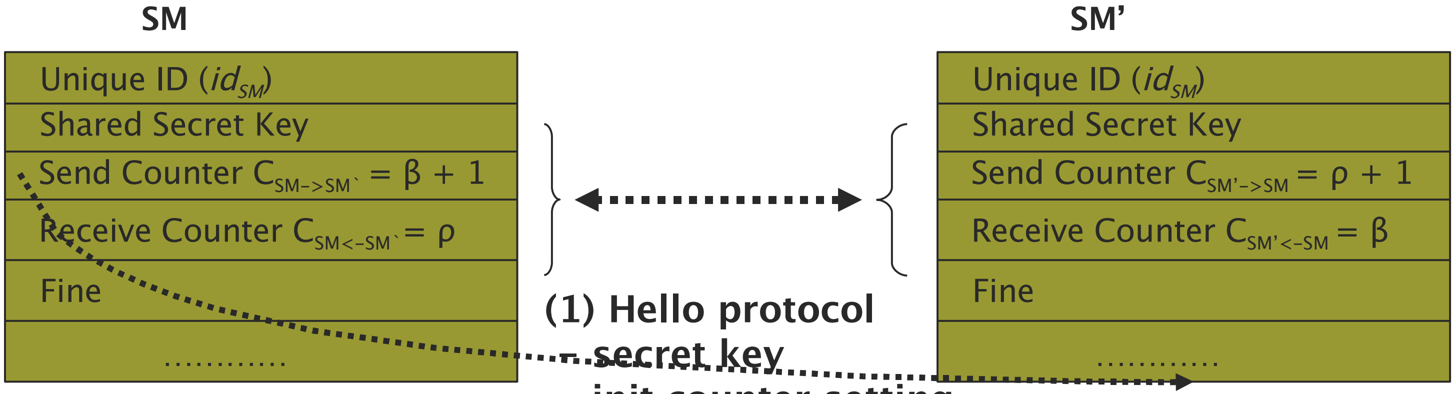
Receive Counter

Fine

....

Per neighbor data structure
– **short term data**

Implementation of Models
- How to Prevent "Replay"?



SM

Unique ID (id_{SM})
Shared Secret Key
Send Counter $C_{SM->SM`} = \beta + 1$
Receive Counter $C_{SM<-SM`} = \rho$
Fine
…………

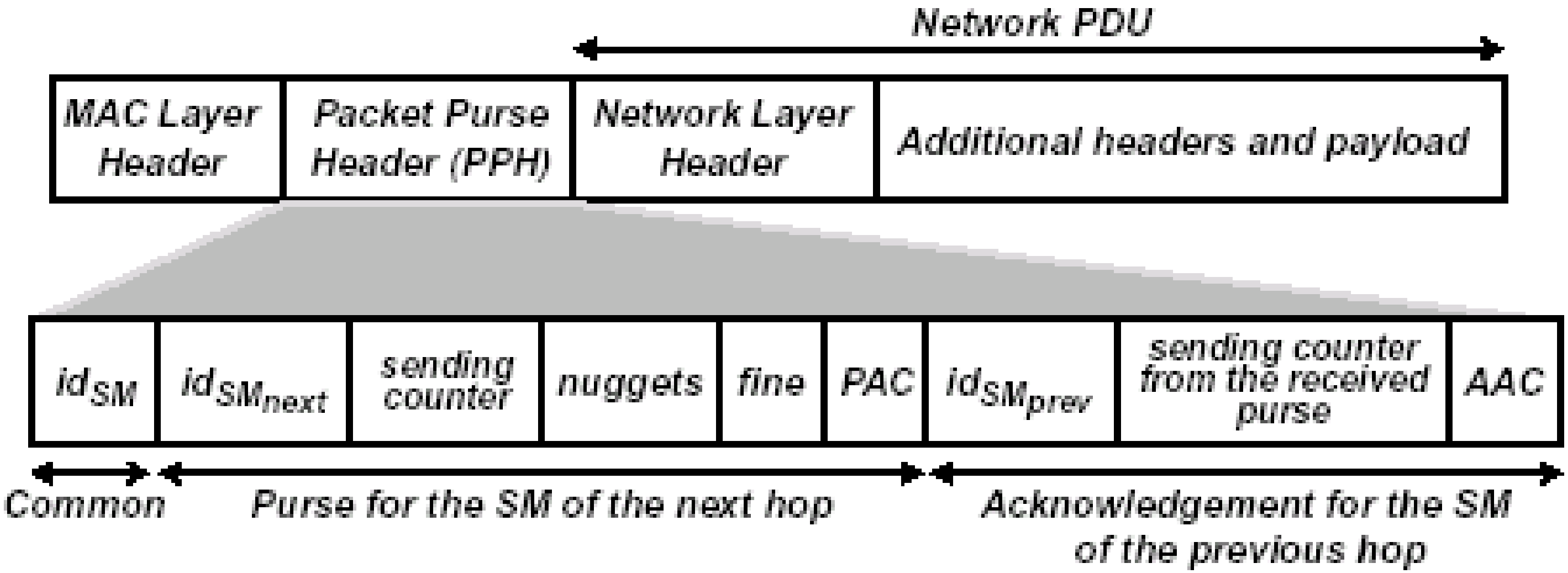
SM'

Unique ID (id_{SM})
Shared Secret Key
Send Counter $C_{SM'->SM} = \rho + 1$
Receive Counter $C_{SM'<-SM} = \beta$
Fine
…………

(1) Hello protocol
 – secret key
 – init counter setting
 (ρ and β are randomly selected)

(2) Sending a Message, SM => SM'
 – SM: send c to SM' and then c++
 – SM': receive and compare it with receive counter
  * if c <= r, then discard
  * else accept and increase r++

Implementation of Models
- Packet Purse Header



Network PDU

MAC Layer Header	*Packet Purse Header (PPH)*	*Network Layer Header*	*Additional headers and payload*

id_{SM}	$id_{SM_{next}}$	*sending counter*	*nuggets*	*fine*	*PAC*	$id_{SM_{prev}}$	*sending counter from the received purse*	*AAC*

Common

Purse for the SM of the next hop

Acknowledgement for the SM of the previous hop

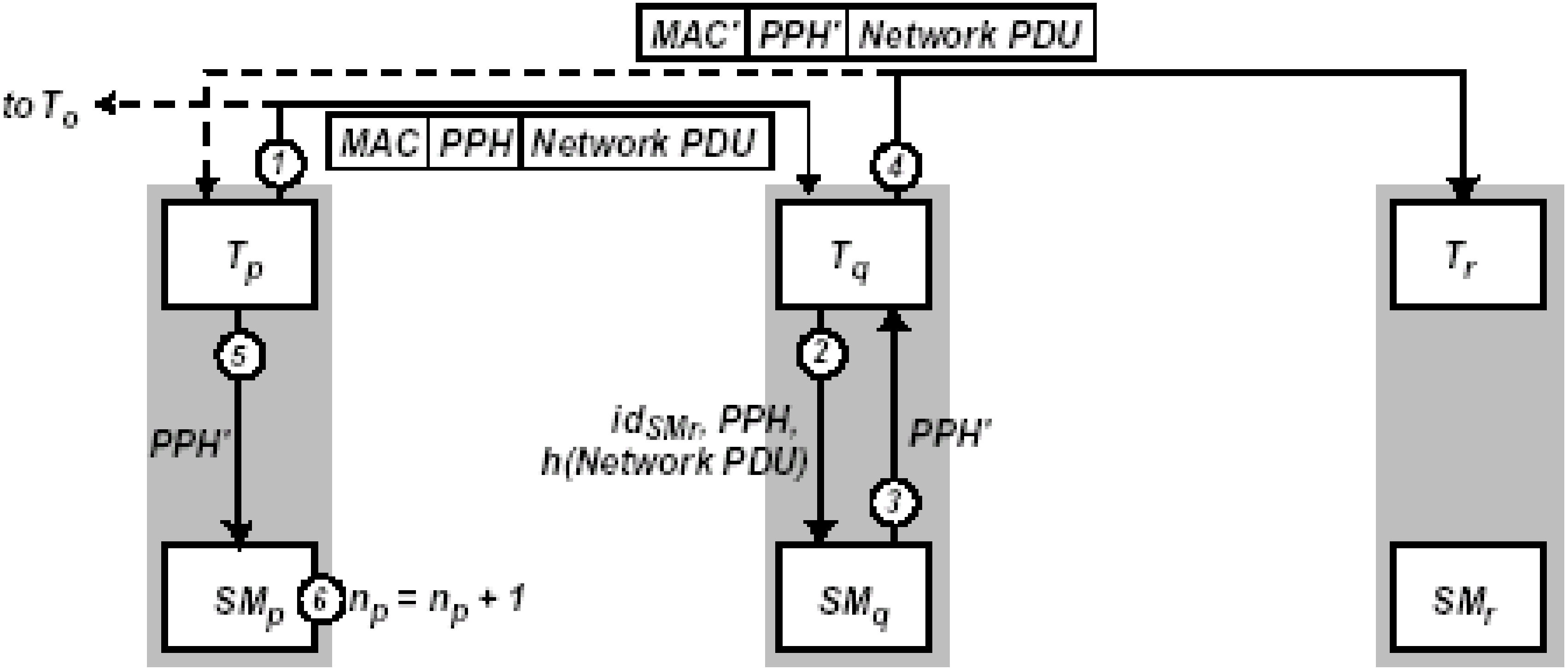
PAC - Purse Authentication Code

PAC = $g_{k_{SM,SMnext}}(id_{SM}, id_{SM_{next}},$ *sending counter, nuggets, fine, h(Network PDU))*

AAC - Acknowledgement Authentication Code

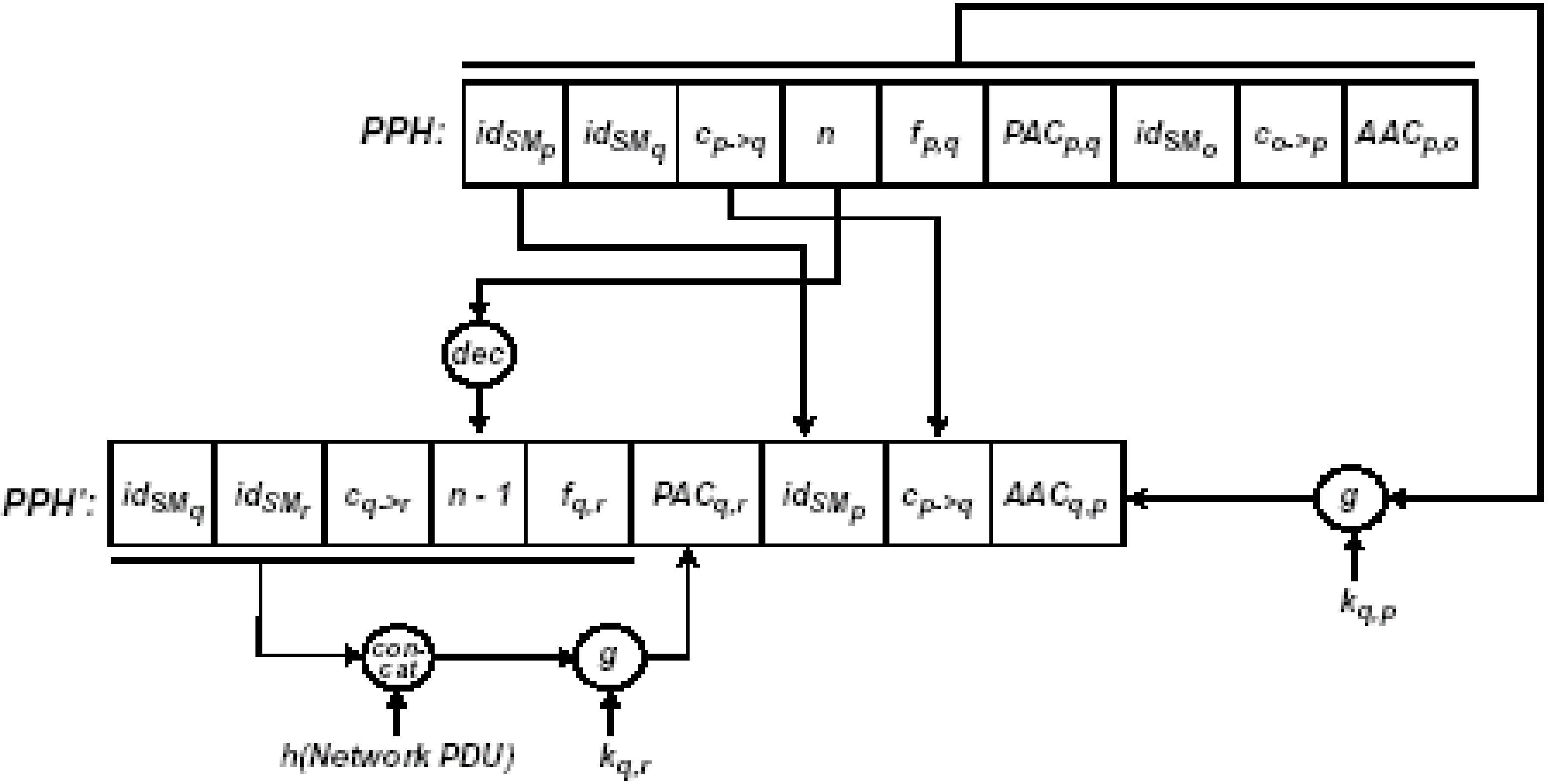
AAC = $g_{k_{SM,SMprev}}$*(received PPH)*

Implementation of Models
- Packet Forwarding Protocol



Implementation of Models

- Re-computing the Packet Pulse Header



Implementation of Models
- Packet Trade Model

- Instead of the number of nuggets, it contains the price of the packet
- The SM of each forwarding *terminode*
    - decreases its nugget counter by the price in the PTH (buying)
    - increases the price by one when re-computing the PTH
    - Increases its nugget counter by the new price when ack arrives (selling)

Analysis

- Simulation for cooperation and prevention of overloading and efficient
- Robustness
  - Illegitimate increase of the nugget counter
    - Assumption; a tamper-proof security module
  - Generation of fake packet purses or acks
    - Using cryptographic checksums (i.e., the Purse Authentication Code and the Ack Authentication Code)
  - Replay
    - Counter of each module
  - Fair exchange
    - Nash equilibrium fairness
    - A misbehaving party may cause some damage to a correctly behaving one, but it also loses something or at lease cannot gain anything (apart from malicious joy) with the misbehavior

Conclusion

- Addressed the problem of service availability in *terminode* networks (mobile ad-hoc WANs)
- A secure mechanism to stimulate end users, and prevent DOS attacks
- Mainly motivated by the experience of chargeable cellular networks
- Also has other purposes
  - Communication and Information Services
  - Converting nuggets to real currency