

# Managing Credits in Mobile Ad Hoc Networks

Fabio Martinelli, Marinella Petrocchi, Anna Vaccarelli

Istituto di Informatica e Telematica  
National Research Council  
IIT-CNR  
Pisa, Italy

Wednesday 5 May 2004

UK Ubinet 04 - Cambridge

## Scenario

Mobile Ad Hoc Networks (MANETs):

are kept connected by the mobile hosts  
may be not governed by a single authority

MANETs need:

Cooperative behaviour,  
*e.g.*, forwarding each other's packets

⇒ A node may misbehave by agreeing  
to forward packets and then failing to do so

- *overloaded*
- *malicious*
- *broken*
- *selfish*

## Related Work

*Reputation systems &  
award-based systems*

may be used to provide incentives to forward packets.

Marti *et al.*, 2000, and CONFIDANT, 2002, use watchdogs, pathraters and neighborhood monitoring.

*Nuglet* is a virtual currency (Buttayan & Hubaix 2002).

⇒ pay when sending packets

being paid when forwarding packets

## Local Management of Credits & Debits

Each node locally maintains a Credit Table

⇒ With  $S$  = packet source

Credits = packs that  $S$  has forwarded for  $A$

Debits = packs that  $A$  has forwarded for  $S$

Authenticated proof of delivery. *Cryptographic extension* at routing level – included as additional data in DSR-like specifications.

Credits cannot be spent over all available routes

⇒ *Credit transferring*

$A$  = *first-hand* debtor of  $S$

$B$  = *second-hand* debtor of  $S$

⇒  $A$  securely transfers debits to  $B$

## Identity Management

Nodes may re-enter the network in disguise:

- *misbehaving users are punished*
- *new users are granted to have an initial amount of packets forwarded*

Source of inspiration  $\Rightarrow$

out-of-band mechanisms to bootstrap authentication in wireless networks

The Resurrecting Duckling – Stayano & Anderson

Location-Limited Channels – Balfanz *et al.*

First: “*achievement of a credential in a non forgeable way*” – univocal device identification

Then: At any time, devices do not possess more than one valid certificate

## What's different from...

?? Neighborhood monitoring

?? Virtual currency

?? Central authority awarding & charging nodes  
(free in multi-hop cellular networks)

Work partially supported by CNR project:

**“Trusted e-services for dynamic coalitions”**