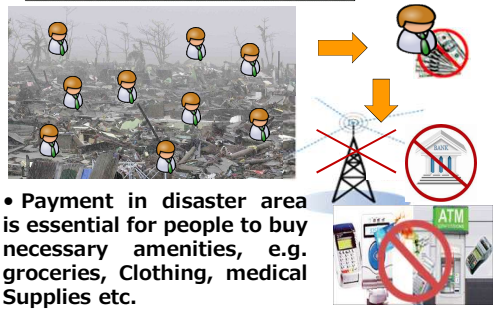
An Endorsement Based Mobile Payment System for a Disaster Area

Babatunde Ojetunde†1, Naoki Shibata†1, Juntao Gao†1, Minoru Ito†1

†1 NAIST

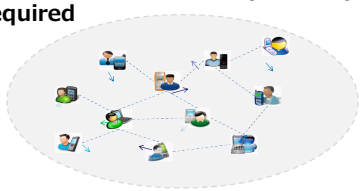
Background



- Payment in disaster area is essential for people to buy necessary amenities, e.g. groceries, Clothing, medical Supplies etc.
- Network infrastructure is not available
- People have no access to
  - Their bank account
  - Electronic transaction
- Existing payment systems require communication infrastructures

Payment System in MANETs

- An infrastructureless Payment System is required

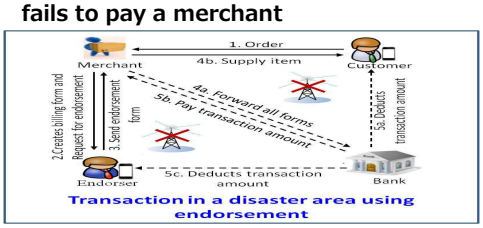


Payment System Challenges in MANETs

- Non-availability of network infrastructure
- Dynamic change topology due to mobility
- Fraudulent transactions
  - Authentication Issues
  - Impersonation
  - Double Spending
  - Resetting Phone

Proposed Mobile Payment System

Endorsement: An endorser agrees to pay for a customer in case customer fails to pay a merchant



Transaction in a disaster area using endorsement

Payment System Obstacles

i. Authentication and Security
ii. Users Colluding (Customer and Endorser)
iii. Double Spending
iv. Confirming Transaction Location Source
v. Reset and Recovery attacks
vi. Availability of Endorsers

Proposed Method

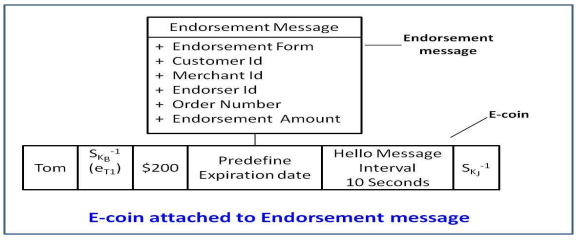
Schemes Securing Endorsement Based Mobile Payment System

i. Solution 1: Digitally Signed Picture

- ◊ Digitally signed picture used for authentication
- 1. The system can use another kind of biometric authentication method
- ◊ Messages are digitally signed and encrypted

ii. Solution 2: E-coin Balance Checking

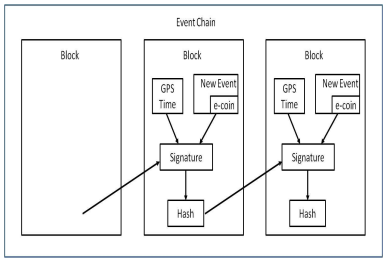
- ◊ Colluding can be avoided by checking whether an e-coin is attached to the endorsement message

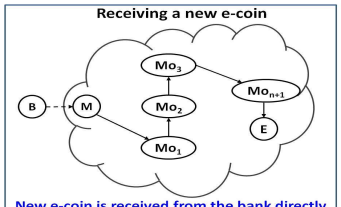


E-coin attached to Endorsement message

iii. Solution 3: Preventing Double Spending with Event Chain

- ◊ Endorser creates an event chain for recording all transaction logs





New e-coin is received from the bank directly or relayed to the endorser through the users available within radio range

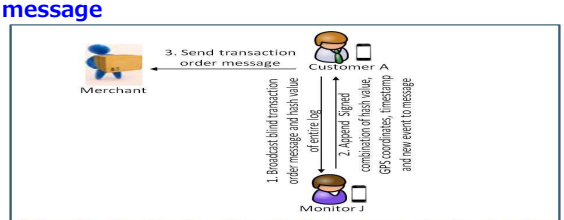
- ◊ Other users can check event chain to verify whether e-coin is double spent

iv. Solution 4: Location Information Based Monitoring

- ◊ Endorsers exchange Hello message with other users
- ◊ Other users monitor endorsers transaction location by
  1. Comparing endorser's entire log of event chain with the event chain at end of the Hello message previously exchanged
  2. Comparing the Hello message interval in the e-coin with the one in the Hello message

v. Solution 5: Blind Signature and Event Chain

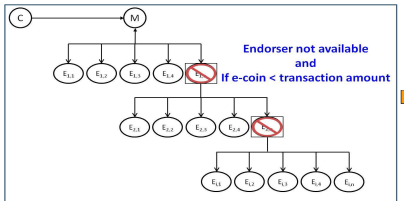
- ◊ Blind signature ensures anonymity of broadcast message
- ◊ Event chain prevents users from using previously used message



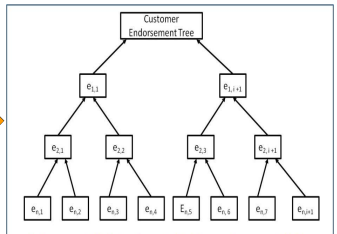
Merchant checks the entire event chain to see if predefined time has passed before a new event is added

vi. Solution 6: Chains of Endorsers

- ◊ Many endorsers can be used
- ◊ Endorsers are rewarded to stay honest
- ◊ Reduced endorsers liability



Merchant obtains level two endorsers information from the endorsement tree header



Endorsement chain-tree is created to form endorsement chain

Assumptions

1. Most of the users in the system are trustable
   - ◊ Do not change location often
   - ◊ Most of the users do not power off the phone very often
2. All users are in the disaster area except the bank
3. No more than two parties will collude to do fraud in the system
4. Enough number of monitoring nodes are available at most of the time.

Evaluation

The following goals can be achieved for mobile payment system in disaster area

- ◊ Feasibility: Suit limitation of mobile payment in disaster area like non-availability of network etc
- ◊ Authentication
- ◊ Anonymity
- ◊ Confidentiality
- ◊ Integrity
- ◊ Reliability

Reference

Z. Hu, Y. Liu, X. Hu, and J. Li, "Anonymous micropayments authentication (AMA) in mobile data network," in *INFOCOM 2004. Twenty-third Annual/Joint Conference of the IEEE Computer and Communications Societies, vol. 1, March 2004, pp. 53.*