Multiparty Micropayments for Ad Hoc Networks

Hitesh Tewari & Donal O’Mahony
Networks and Telecommunications Research Group
Dept of Computer Science
University of Dublin, Trinity College
Ireland
Next Generation Wireless Networks

- WiFi/Wireless LANs
- Core IP Network
- Access Network
  - IP Router
  - Location Mgt Server
  - Broker
  - Web Server
  - Gateway

NAIMN – joe@ls.net

Mobile Ad Hoc, PAN and Sensor Networks

http://ntrg.cs.tcd.ie
Ad Hoc Networks

- Infrastructureless mobile networks
  - Consist of groups of nodes that communicate with each other using multihop wireless links

- Each node acts as a router to forward packets for other nodes in the network
  - May be selfish nodes in the network which do not forward packets to conserve their battery life

- Need an incentive based scheme to stimulate packet forwarding in the network

- We present a real-time micropayment scheme which enables a node to join an existing ad hoc network and allows it to pay each node that relays packets on its behalf
Design Goals

• **Real-Time Payment**
  - Need to be able to choose any route and pay each node along the path to forward packets to the destination

• **Off-line Operation**
  - Intermediate nodes should not be required to have an on-line connection to a trusted third party (TTP) to verify the payment instrument

• **Minimize Fraud**
  - The effort required to steal value from the system should be far greater than the rewards
    • Post-fact detection should pinpoint the culprit(s) who can then be disqualified from the network
Lightweight Cryptographic Techniques

• We make use of hash chains for payment and minimal use of cryptographic keys in the system

\[
P_0 \quad P_1 \quad P_{N-1} \quad P_N
\]

Anchor \quad Hash# 1 \quad Hash# N-1 \quad Secret Root

• UOBT
  - Not possible to store long hash chains on mobile devices
  • Need to store only the 'tree root' to generate all sub-chains

Unbalanced One-Way Binary Tree (UOBT)
Micropayments Using Hash Chains

- Allow for repeated small valued payments at a single vendor
  - E.g. one-tenth of a cent in single transaction

To pay multiple hash tokens one can just attach the correct hash value up the chain.
Broker Commitment

- Payment chains can be purchased from a broker in advance of knowing the actual recipients
  - Allows flexibility in choosing the best route

For a 40x40 UOBT the broker commitment is (40*168) ~7Kbytes. For a 100x100 UOBT it is ~17Kbytes

http://ntrg.cs.tcd.ie
Endorsement Distribution

- Broker signed endorsement values prevent a valid smart card from accepting falsely generated or stolen chains

Charge Request \{A, B, N, R, X\}

Source requests charging information for a destination

Charge Reply \{A, X, [(B, 1)\text{Sig}_B, \text{Cert}_B], [(N, 1)\text{Sig}_N, \text{Cert}_N], [(R, 2)\text{Sig}_R, \text{Cert}_R]\}\n
Intermediate nodes return their charge for packet forwarding

Endorsements \{[B, (\text{Endorsement1})\text{PK}_B], [N, (\text{Endorsement2})\text{PK}_N], [R, (\text{Endorsement3, Endorsement4})\text{PK}_R]\}\n
Encrypt individual endorsements with public key of each recipient

- Alternative to avoid attaching large certificate chains is to buy payment chains from a local broker
  - Nodes in the area will already have the broker certificate
Payment for Packet Forwarding

- No need to protect hash tokens using additional cryptographic procedures
  - Quick verification of payment information at each node and fast relaying of packets

- Smart card module has to be compromised to obtain endorsement values
  - Expiry date associated with the chain prevents a compromised chain from being reused indefinitely

http://ntrg.cs.tcd.ie
Change in Route - New Path

- No requirement to contact a broker to pay nodes along a new route
  - Switch to new set of sub-chains of the UOBT and immediately start paying nodes to forward packets

Charge Request\{A, L, N, R, X\}

Charge Reply\{A, X, [(L, 2)\text{Sig}_L, \text{Cert}_L], [(N, 1)\text{Sig}_N, \text{Cert}_N], [(R, 2)\text{Sig}_R, \text{Cert}_R]\}\}

Endorsements\{[L, (\text{Endorsement5})\text{PK}_L]\}\}

\{P_{52}, P_{231}, P_{422}\} \rightarrow (H(H(P_{52}))=P_0? \rightarrow H(P_{231})=P_{230}? \rightarrow (H(H(P_{422}))=P_{420}? \rightarrow \{P_{520}, P_{240}, P_{440}\} \{P_{240}, P_{440}\} \{P_{440}\}

Distribute new set of endorsements to keep session alive
Redeeming Tokens & Broker Clearing

• Periodically a node will contact the broker and deposit payment tokens that it has collected

User L

Redeem Token\{L, P_5, (Endorsement5)PK_{Broker}\}Sig_L

Deposit highest received hashes in each payment chain

Broker

Receipt\{L, P_5, Amount\}Sig_{Broker}

Broker verifies hashes and credits users account

• There can be multiple brokers in the system
  - Which can have accounting relationships to settle user accounts
Discussion

- Use of micropayments and off-line verification allows the solution to be efficient and scalable
  - Asymmetric key algorithms are only used during call setup and endorsement distribution

- We make use of tamper resistant devices for providing some of the bank functionality
  - However we do not place total trust in the hardware modules and associate an expiry date with each chain

- Hash chains are of a finite length and there is a possibility that a node may run out of hash values during a call
  - We can make use of more efficient hash chain storage and computational techniques as proposed by Jakobsson et al.
Conclusions

• A method for compensating nodes in real-time for packet forwarding has been outlined

• The protocol allows routers to charge per-packet and adapts to dynamic routing changes
  - No requirement to contact a TTP to verify payment

• A node discovers one or more routes along with a secure and verifiable charge for packet forwarding
  - Allows for the node to choose the cheapest route

• Use of lightweight cryptographic techniques
  - Means that there will minimum delay in the relaying of datagrams by intermediate nodes
Thank You – Questions?