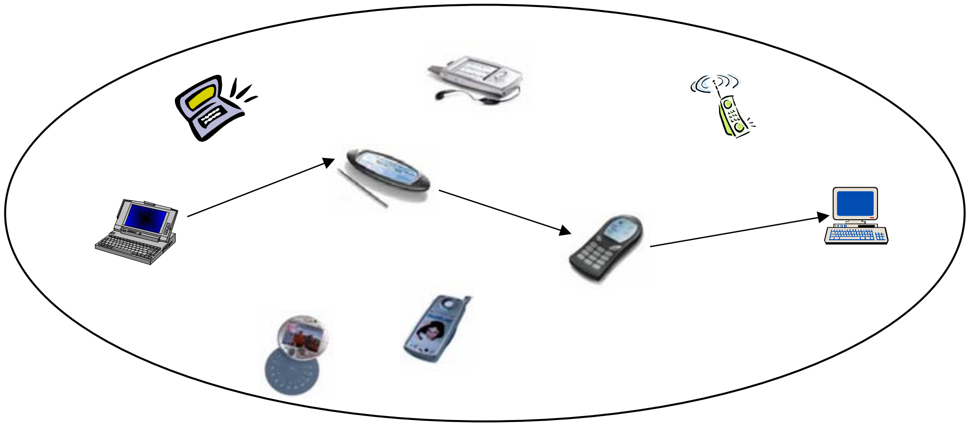
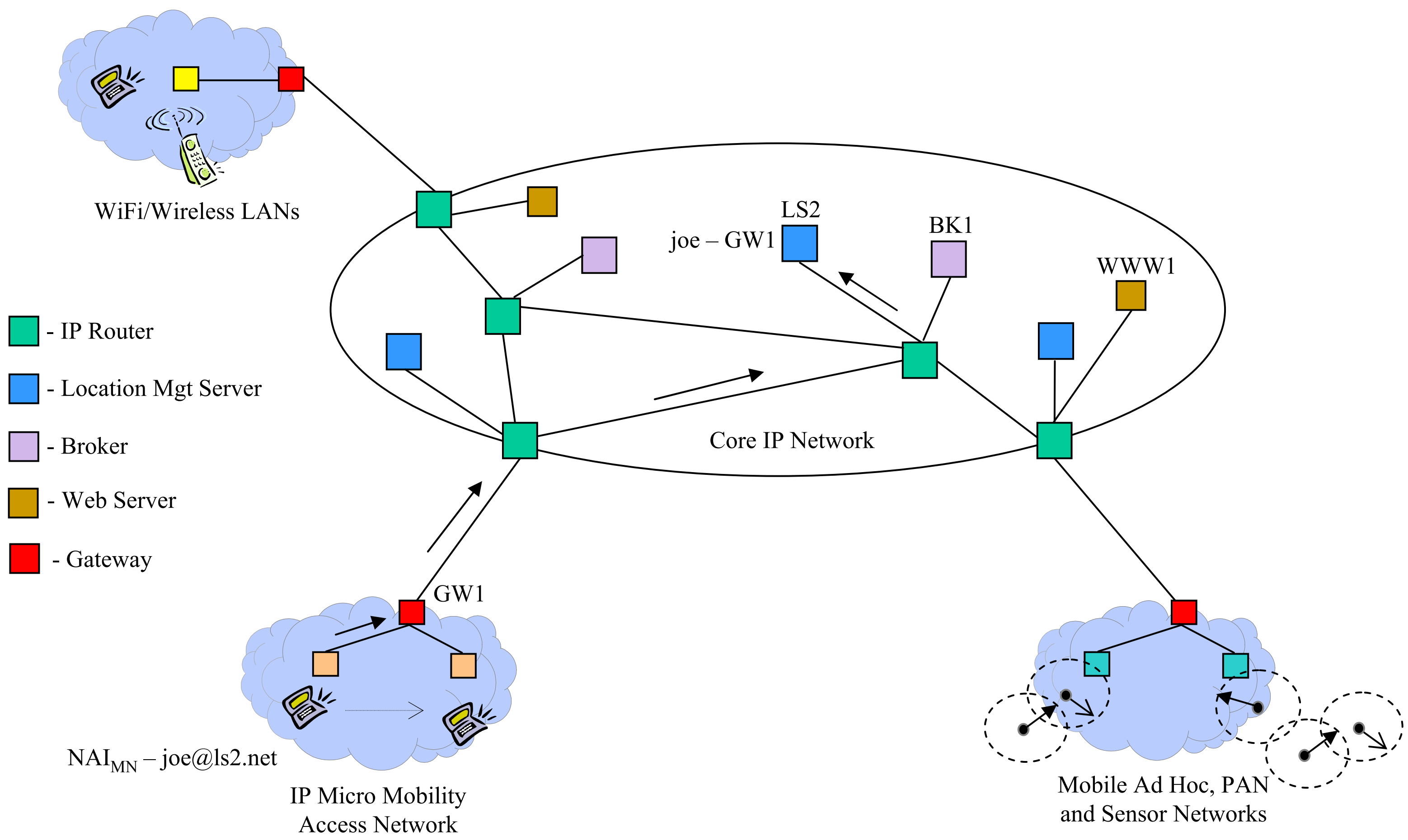


Multiparty Micropayments for Ad Hoc Networks

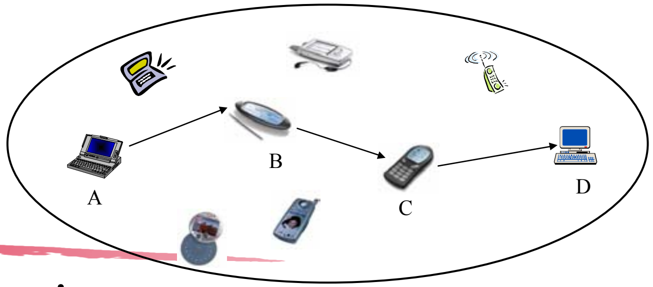
Hitesh Tewari & Donal O'Mahony
Networks and Telecommunications Research Group
Dept of Computer Science
University of Dublin, Trinity College
Ireland

http://ntrg.cs.tcd.ie

Next Generation Wireless Networks



Ad Hoc Networks



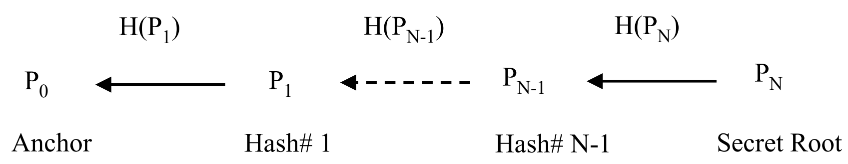
- Infrastructureless mobile networks
  - Consist of groups of nodes that communicate with each other using multihop wireless links
- Each node acts as a router to forward packets for other nodes in the network
  - May be selfish nodes in the network which do not forward packets to conserve their battery 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

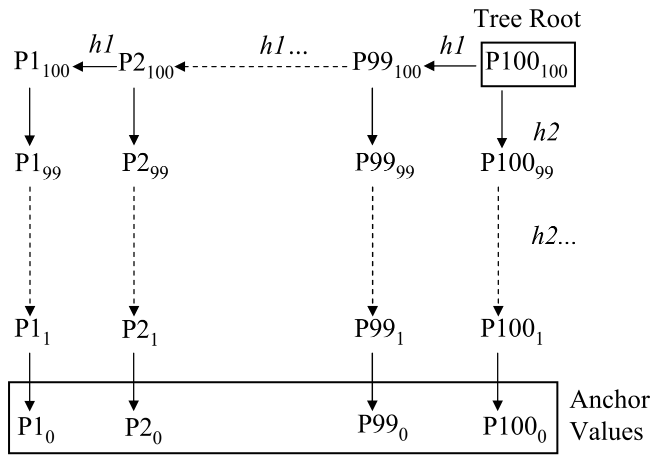
- Real-Time Payment
  - Need to be able to choose any route and pay each node along the path to forward packets to the destination
- Off-line Operation
  - Intermediate nodes should not be required to have an on-line connection to a trusted third party (TTP) to verify the payment instrument
- Minimize 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



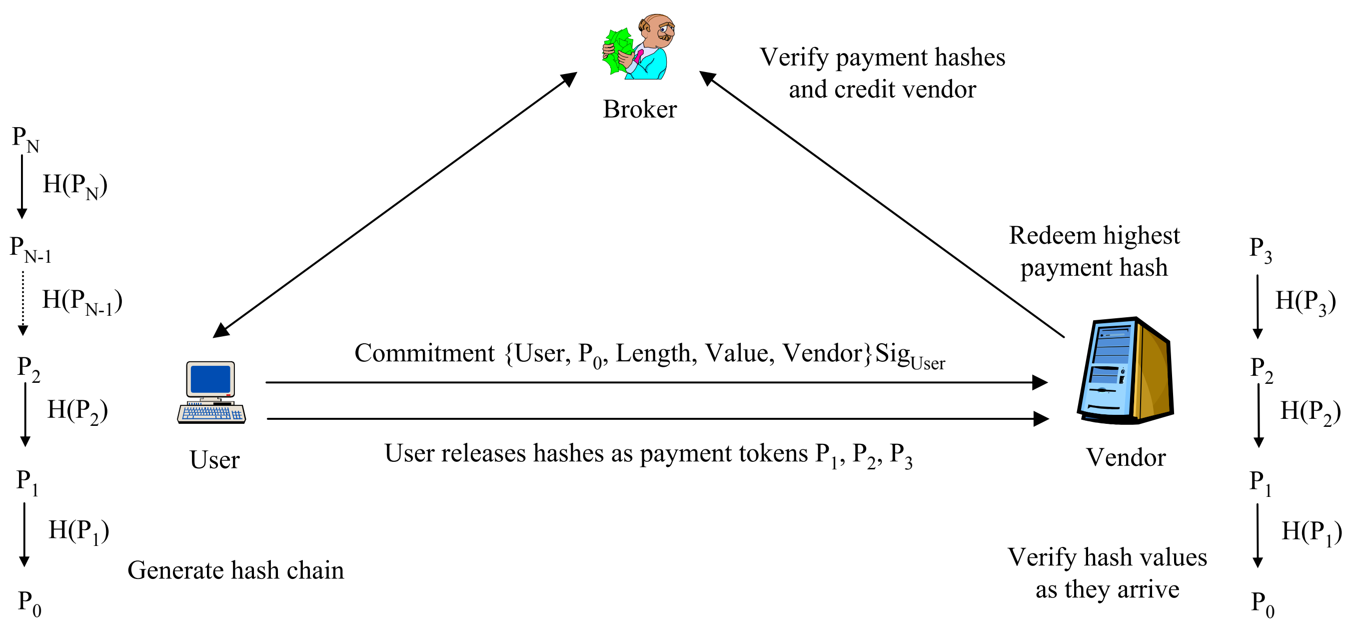
- UOBT
  - Not possible to store long hash chains on mobile devices
    - Need to store only the 'tree root' to generate all sub-chains



Unbalanced One-Way Binary Tree (UOBT)

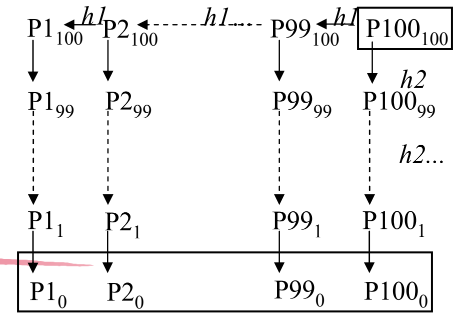
Micropayments Using Hash Chains

- 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

(PK_A, SK_A)

User A

{[A, (P1$_0$, P2$_0$, ... P39$_0$, P40$_0$), Length, Value, Macropayment]Sig_A, $Cert_A$}PK_{Broker}

UOBT anchor values to be signed by broker

(PK_{Broker}, SK_{Broker})

Broker

Broker generates secret endorsement values {E1, E2, … E39, E40}

Commitment

Endorsement1	Endorsement2	Endorsement3	……….	Endorsement39	Endorsement40

P3$_0$	E3	Length	Value	User_ID	Expiry

Sig_{Broker}

Size of each endorsement = 40+128 bytes

{Commitment}PK_A	Receipt

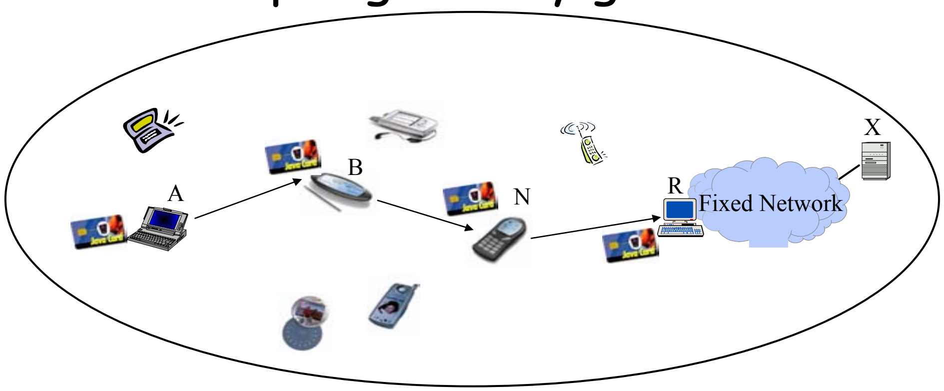
Broker returns a commitment which consists of the set of endorsements encrypted with the public key of the recipient and a signed receipt

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

Receipt = {A, (P1$_0$, P2$_0$, … P39$_0$, P40$_0$), Length, Value, Expiry}Sig_{Broker}

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)Sig_B, $Cert_B$], [(N, 1)Sig_N, $Cert_N$], [(R, 2)Sig_R, $Cert_R$]}

← Intermediate nodes return their charge for packet forwarding

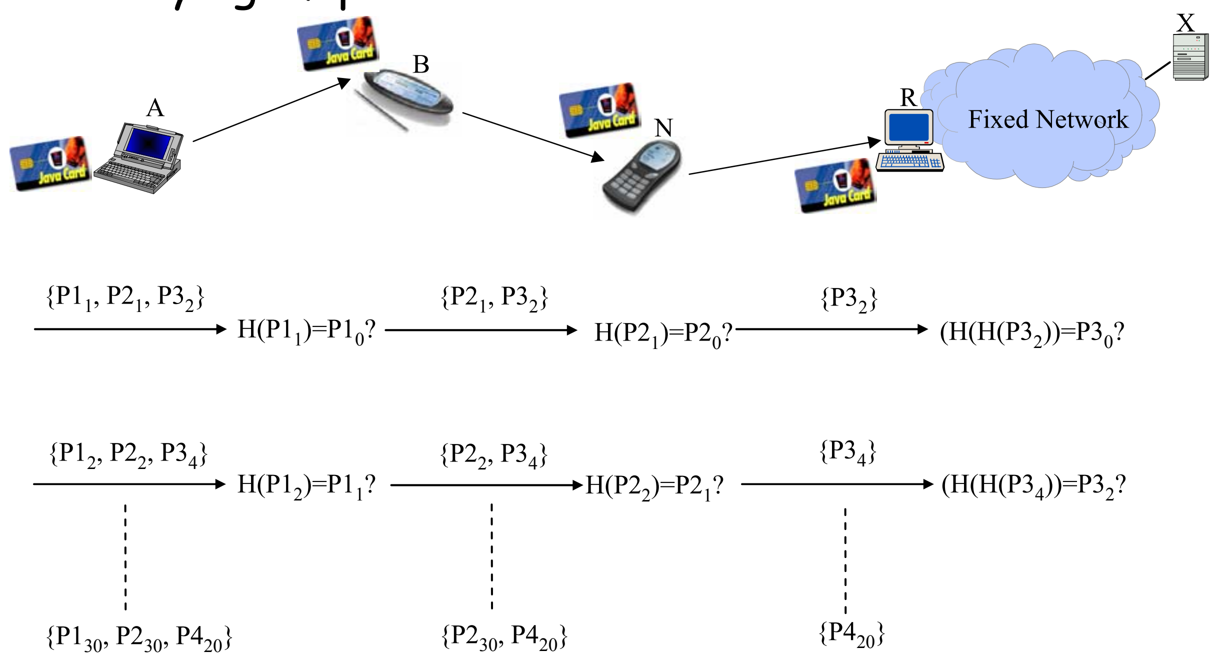
Endorsements{[B, (Endorsement1)PK_B], [N, (Endorsement2)PK_N], [R, (Endorsement3, Endorsement4)PK_R]}

→ 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

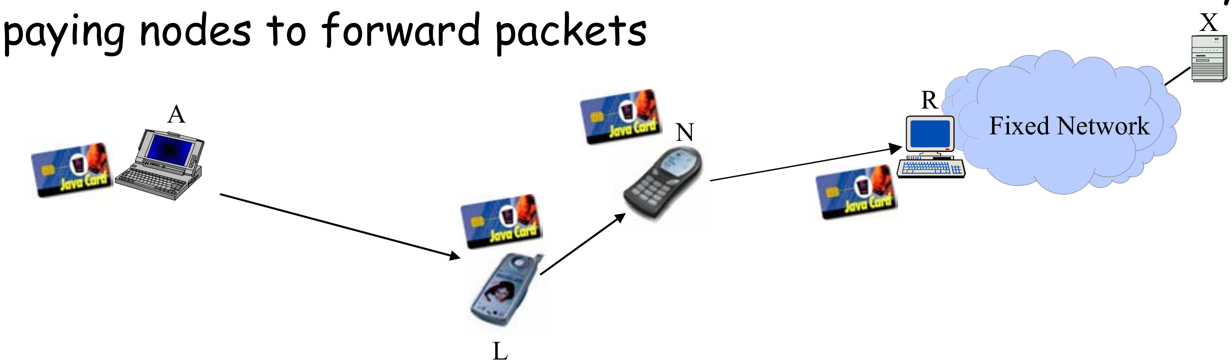
- No need to protect hash tokens using additional cryptographic procedures
  - Quick verification of payment information at each node and fast relaying of packets

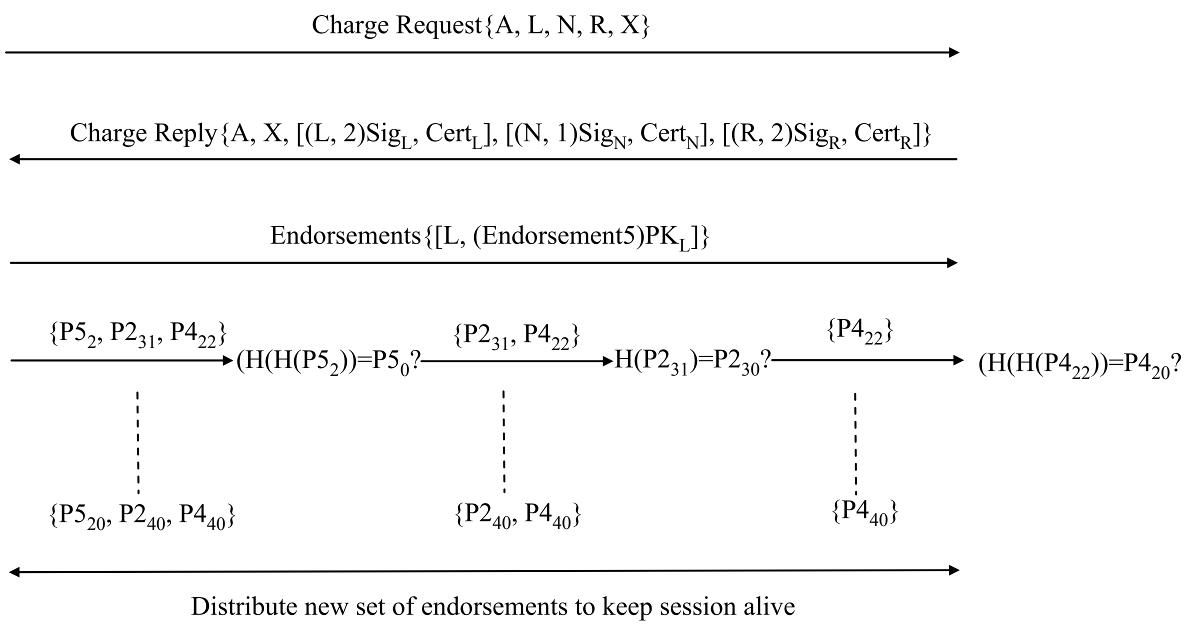


- Smart card module has to be compromised to obtain endorsement values
  - Expiry date associated with the chain prevents a compromised chain from being reused indefinitely

Change in Route - New Path

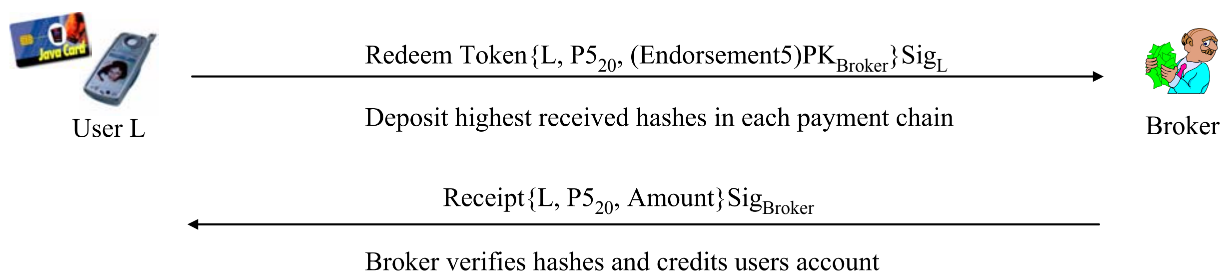
- No requirement to contact a broker to pay nodes along a new route
  - Switch to new set of sub-chains of the UOBT and immediately start paying nodes to forward packets





Redeeming Tokens & Broker Clearing

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



- 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 a 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?