Real-Time Payments for Mobile IP

Hitesh Tewari & Donal O'Mahony
Dept of Computer Science
Trinity College Dublin
Ireland

NTRG
networks that work

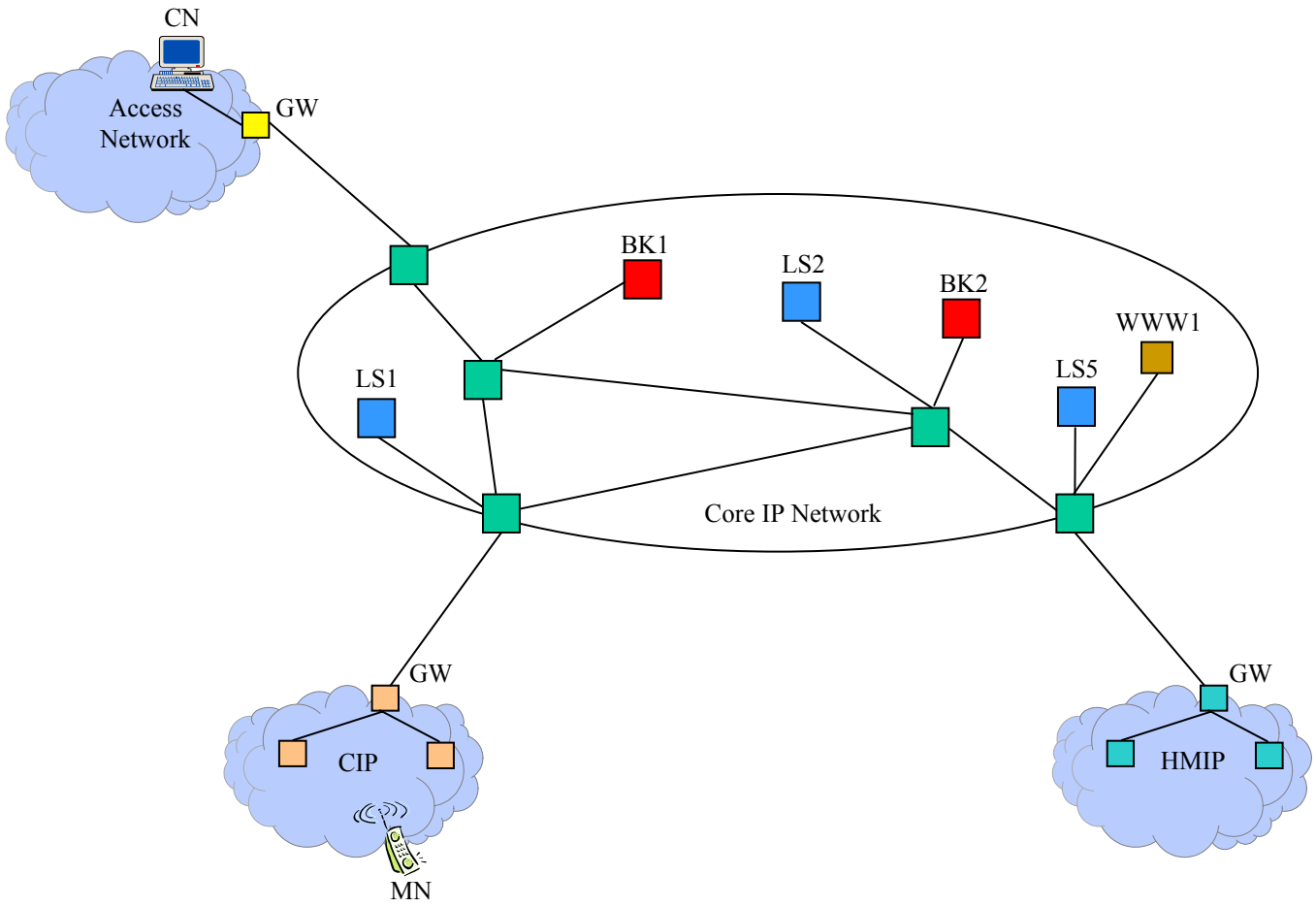
Protocol Goals

- Real-time payment
  - For network usage and location hosting by a mobile node (MN)
- Pay As You Go
  - Eliminate the need for long lived contracts between the users & network operators
- Authenticated signaling exchanges
  - Between MN and specialized nodes in the network
- Lightweight cryptographic procedures
  - Minimize computation & storage requirements on MN and network nodes

Protocol Goals 2

- Single unique global identity e.g. user@realm
  - "Personal Mobility" - independent of user terminal
- Eliminate the requirement for a "Home Network"
  - No need to contact a HA to update/obtain location info for MN
- Route Optimization
  - No "triangular routing"
- Location Privacy
  - Minimize traffic analysis by end-users and routing nodes to obtain location details of a mobile

Network Model



- IP Router
- Location Server
- Broker
- Web Server

We envisage a core network to which are connected numerous access networks that support micro mobility. These access networks can be operated by independent network operators and service providers (“micro-ISPs”)

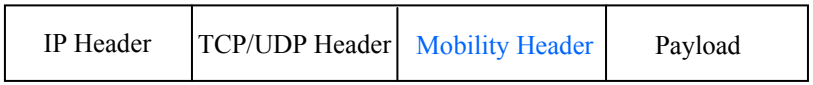
System Overview

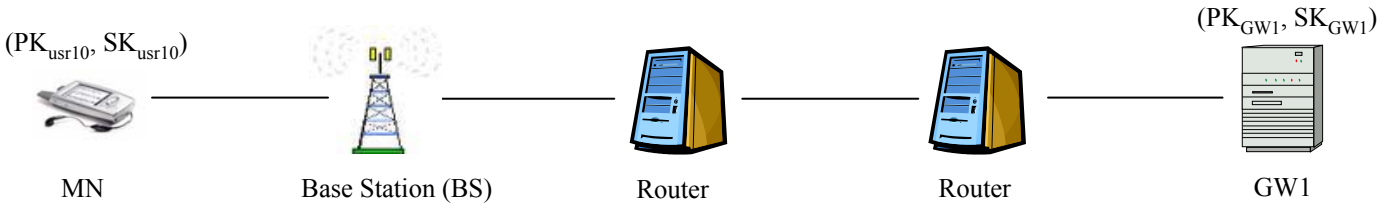
- Brokers in the system endorse and validate payment chains
  - A mobile node has an accounting relationship with a broker
- The MN also has an association with a LS for hosting its care-of address information
  - The LS issues a public-key certificate to the MN
- MN registers with GW node in the access network
  - Obtains a network address which is used as the CoA
- MN buys hash chains from a broker
  - Hash chains are specific to a access network or a LS and can only be spent with the same

System Overview 2

- MN pays the LS at periodic intervals to keep CoA info alive
  - Eliminates the need for a long lived contract between the two and allows for authenticated updates
  - Criteria for choosing a LS could be the cost associated with hosting the CoA info or geographical proximity
- MN also releases payment tokens periodically in the access network
  - Allows for payment for network usage & authentication of signalling messages
    - Intermediate routing nodes are able to securely update their routing caches
- The GW relays packets from the MN to a CN and vice-versa

Registration in Access Network





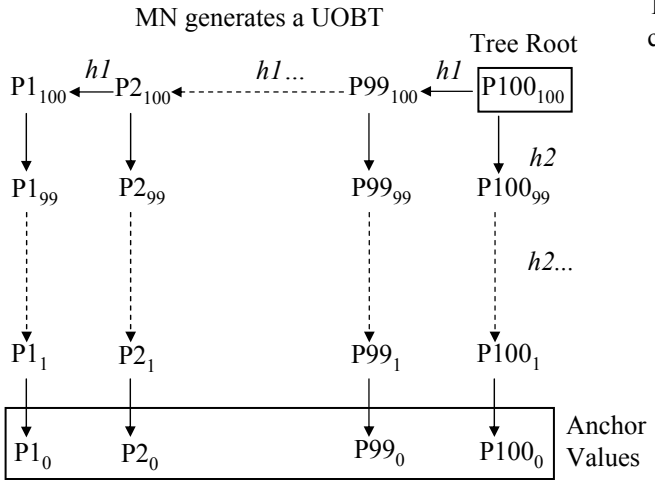
NAI_{MN} – usr10@ls2.net

{0, GW1, Registration-Request, (NAI_{MN}, Timestamp)Sig_{usr10}, $Cert_{usr10}$}

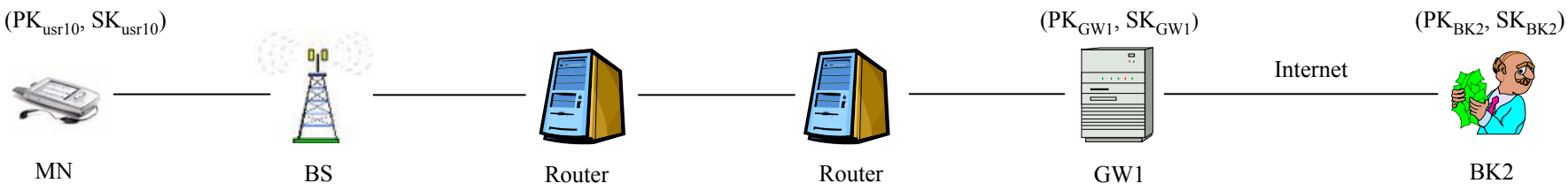
MN presents its authenticated identity (NAI) and requests a network address from the GW node. Uses 0.0.0.0 as its initial source address

{GW1, 1, Registration-Response, (MN, NAI_{MN}, Charge-Details)Sig_{GW1}, $Cert_{GW1}$}

The gateway returns a unique network address for the mobile node along with charge details for network usage in the access network, signed with its private key



Payment Chains & Broker Commitment



{MN, GW1, Payload 1}

MN requests its broker to commit the payment chains which are specific to the access network

Payload 1 – (Purchase-Request, BK2, (Payment Details)Sig_{usr10}, (Macropayment)PK_{BK2})

Payment Details – (NAI_{MN}, GW1, $UOBT_{ID}$, {$P1_0$ … $P100_0$}, Length, Value)

Payload 2 – (Broker-Commitment, (Comm)Sig_{BK2}, $Cert_{BK2}$)

Comm – (NAI_{MN}, GW1, $UOBT_{ID}$, {$P1_0$ … $P100_0$}, Length, Value, Expiry)

Auth – (MN, NAI_{MN}, $UOBT_{ID}$, $P1_0$, 1, 0, {$P1_0$ … $P100_0$}, Length, Expiry)

{GW1, BK2, Payload 1}

GW intercepts the request, marks it as pending and forwards it to the broker

{BK2, GW1, Payload 2}

Broker returns a signed commitment. Binds the anchor of the payment chains to the identity of the GW node by digitally signing the message

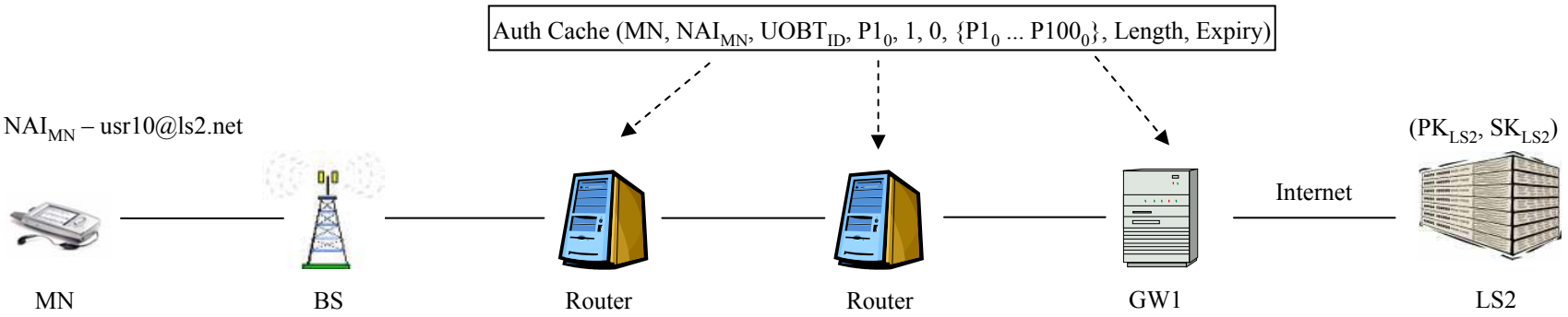
{GW1, MN, Payload 2}

GW returns the signed broker commitment to the MN

{GW1, 1, Gateway-Authorization, (Auth)Sig_{GW1}}

GW broadcasts the payment details in the access network

Location Update



{MN, LS2, Data, UOBT$_{ID}$, P1$_1$, 1, 1, Payload}

MN sends a location update message to its location server LS2 via the gateway node

{MN, LS2, Payload}

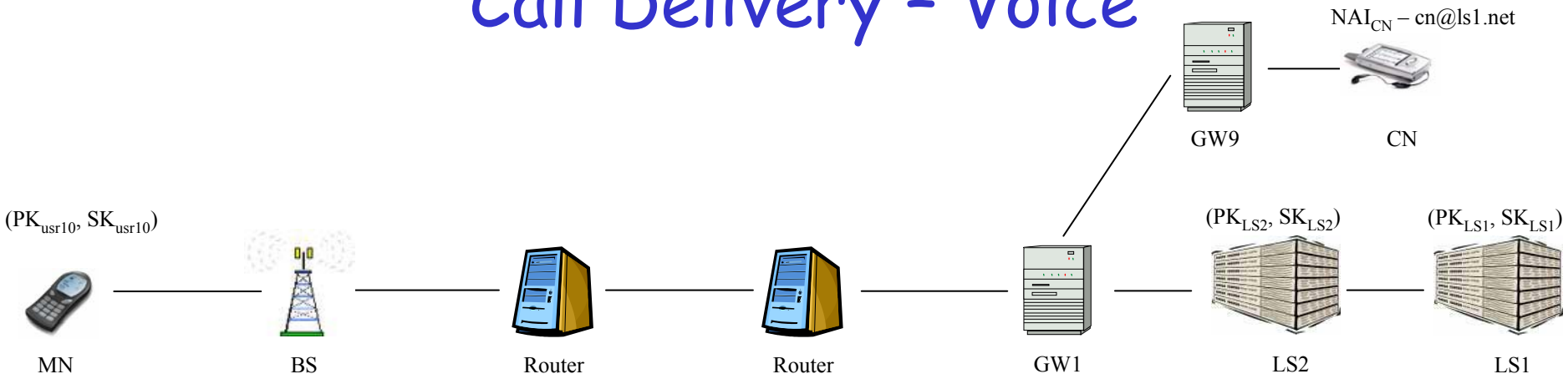
GW removes the mobility header and forwards IP datagrams across the Internet. LS2 authenticates the payment tokens and updates its CoA entry for the MN

MN uses a different UOBT with the LS

Payload – (Location-Update, NAI$_{MN}$, MN, UOBT$_{ID}$, P32$_5$, 32, 5)PK$_{LS2}$

CoA Hash Value Sub-chain# Hash#

Call Delivery – Voice



{MN, LS2, Data, UOBT_ID, P1$_2$, 1, 2, Payload 1}

MN request the network address of the remote node from its LS. Uses the CNs NAI as an identifier

{MN, LS2, Payload 1}

{LS2, LS1, Payload 2}

The location servers may have a micro or macro payment relationship with each other

{LS1, LS2, Payload 3}

{LS2, MN, Payload 4}

The mobile node's location server forwards the signed reply from the remote server encrypted with the public key of the MN

{LS2, MN, Payload 4}

The MN caches the network address of the correspondent node

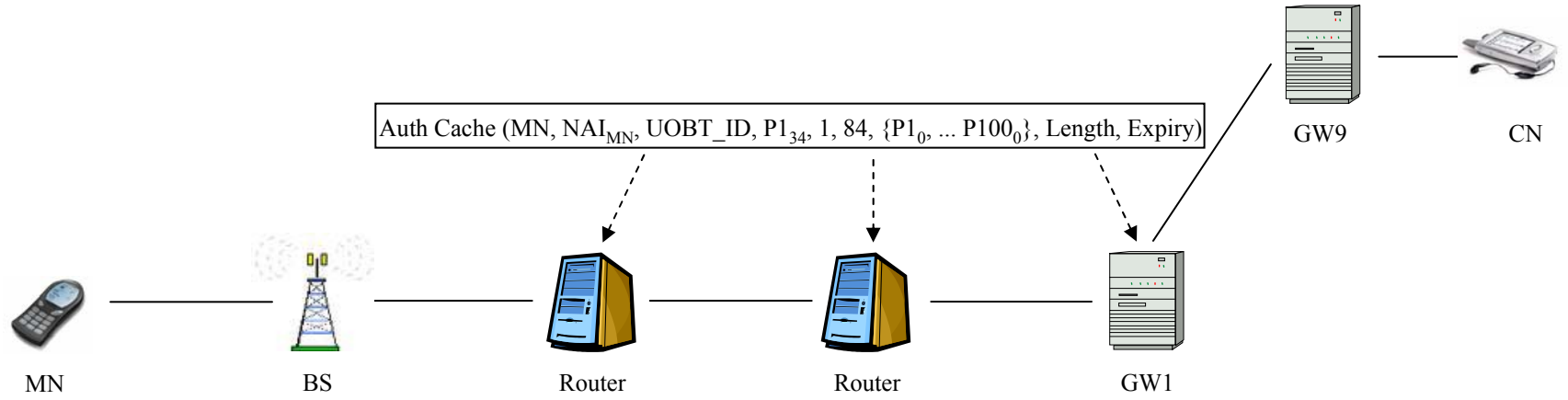
Payload 1 – (Location-Request, NAI$_{MN}$, NAI$_{CN}$, UOBT_ID, P32$_{10}$, 32, 10)PK$_{LS2}$

Payload 2 – (Loc-Req, NAI$_{CN}$, Payment)PK$_{LS1}$

Payload 3 – (Location-Response, (NAI$_{CN}$, CN)Sig$_{LS1}$)PK$_{LS2}$

Payload 4 – ((Location-Response, (NAI$_{CN}$, CN)Sig$_{LS1}$)PK$_{MN}$, Cert$_{LS1}$)

Call Delivery - Voice



{MN, CN, Voice, UOBT_ID, P1$_3$, 1, 3, Payload }

MN attaches next hash token with each datagram. Allows for updating of local route entries and payment for network usage in the access network

{MN, CN, Payload }

Payload – (NAI$_{MN}$, Voice Data)

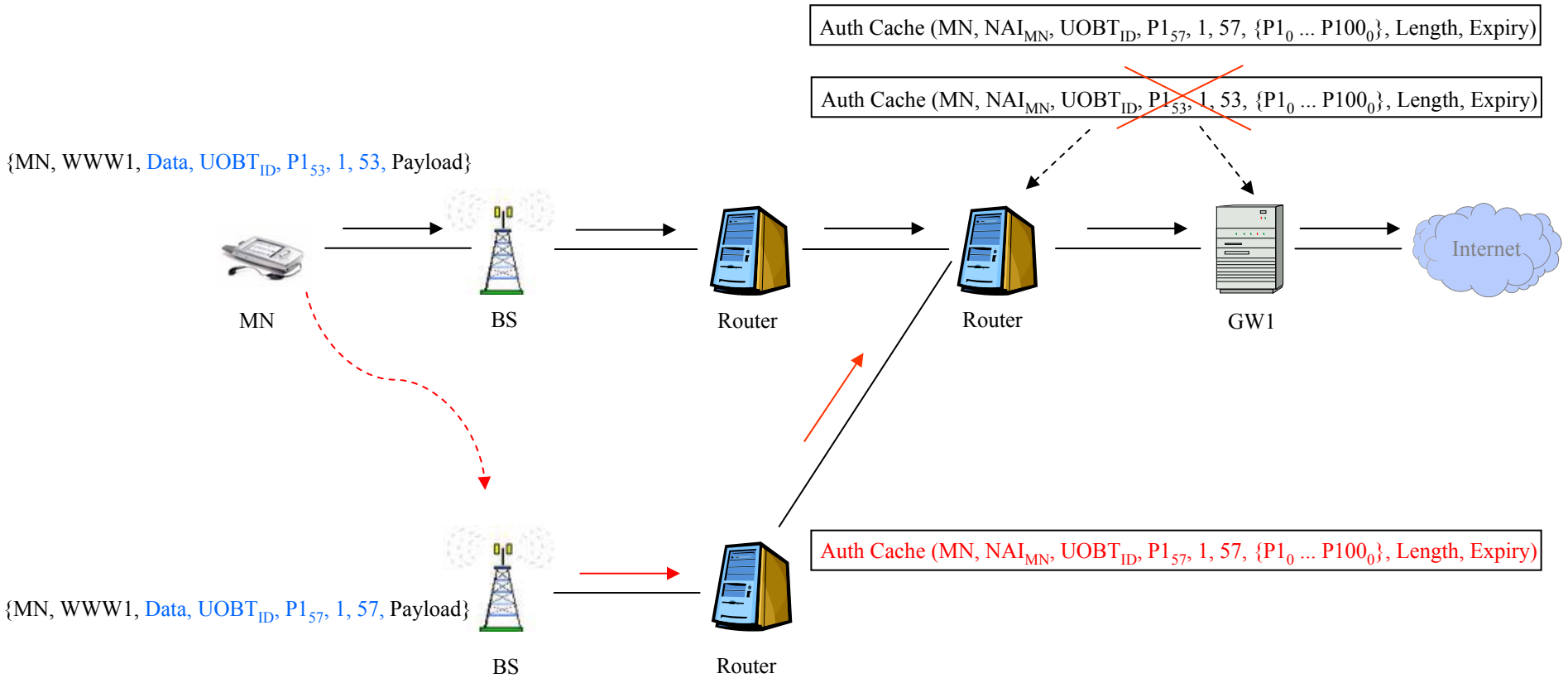
{MN, CN, Voice, UOBT_ID, P1$_{84}$, 1, 84, Payload }

The payload consists of the identity of the caller and the voice data

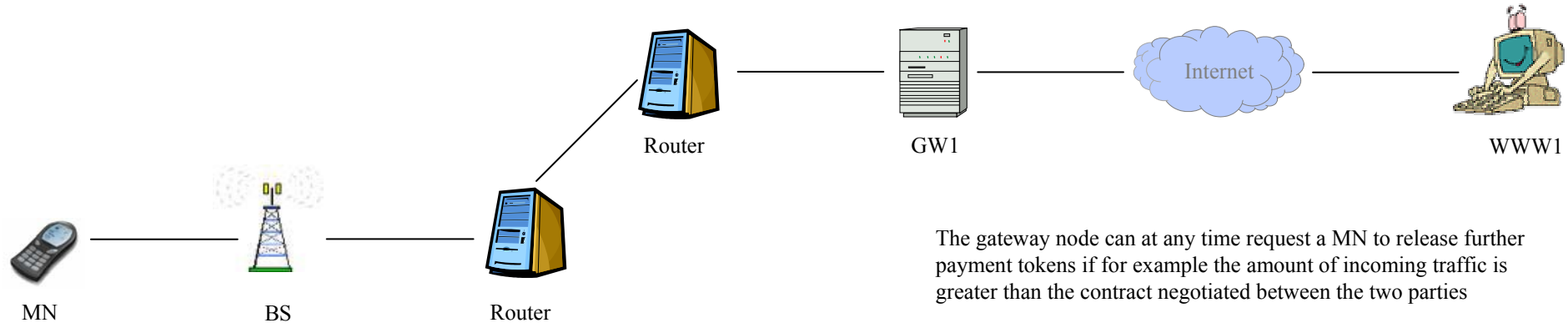
{MN, CN, Payload }

Cannot identify the recipient from the datagram

Fast Handover & Authentication



Call Delivery - Data



The gateway node can at any time request a MN to release further payment tokens if for example the amount of incoming traffic is greater than the contract negotiated between the two parties

{MN, WWW1, Data, UOBT_ID, $P2_8$, 2, 8, Payload}

The MN performs a DNS lookup on the fixed host (WWW1) to obtain the network address for the server. It then sends its request via the gateway node which removes the mobility header and forwards the packet into the core network. Allows us to make use of existing UDP/TCP based applications

{MN, WWW1, Payload}

The packet that travel across the core network and is treated as a regular IP datagram by intermediate IP routers

{WWW1, MN, Payload}

Regular IP packets are sent back in response

{WWW1, MN, Payload}

Complete location privacy is guaranteed for data calls

Broker Clearing

GW1

BK1

BK2

{GW1, BK1, Redeem-Token, BK2, ((Payment-Details)Sig_{GW1})PK_{BK2}, $Cert_{GW1}$}

Deposit highest received hashes in each payment chain from MN with own broker

{BK1, BK2, Redeem-Token, BK_2, ((Payment-Details)Sig_{GW1})PK_{BK2}, $Cert_{GW1}$, $Cert_{BK1}$}

BK1 forwards the request to BK2 who verifies the hashes

Payment-Details (NAI_{MN}, GW1, UOBT_ID, $P1_{85}$, 1, 85, $P2_8$, 2, 8)

Payment-Receipt (NAI_{MN}, GW1, UOBT_ID, $P1_{85}$, 1, 85, $P2_8$, 2, 8, Amount)

{BK2, BK1, Broker-Receipt, ((GW1, Amount)Sig_{BK2})PK_{BK1}, ((Payment-Receipt)Sig_{BK2})PK_{GW1}, $Cert_{BK2}$}

BK2 indicates that BK1 should credit the access network for the specified amount. The brokers in the system maintain an accounting relationship

{BK1, GW1, Broker-Receipt, ((Payment-Receipt)Sig_{BK2})PK_{GW1}, $Cert_{BK2}$}

BK1 forwards a receipt to the gateway node

Concluding Remarks

- We attempt to address the twin problems of authentication and accounting in Mobile IP based access networks
  - Our protocol is independent of any access network technology such as CIP, HAWAII or HMIP
- We try to minimize any changes to the IP datagram format
  - All packets sent across the core network appear as normal IP datagrams
  - Protocol changes required to the MN and GW nodes to be able to interpret the mobility headers
  - Require sufficient amount of network addresses in the access network. May need to move to IPv6

Concluding Remarks 2

- Use of the Network Access Identifier (NAI)
  - Uniquely identify a user
  - Fits in better with our model than assigning a permanent IP address to a node
- Binding the gateway identifier into the payment chain means that a MN can only spend the hash tokens in the specified access network
  - No fraud in the system
- Can use smart cards for personal mobility
  - Store security keys and payment information

Problems/Issues

- Calls will be dropped when a MN roams from one access network to another
  - Requires an update at the LS and address in the new network as well as payment tokens
  - A number of people have also proposed "vertical handovers"
- A MN may be required to keep a number of payments chains for different access networks that it may use
  - May also run out of chains during a call – applicable to all "pay as you go" type systems