

Registration, Broadcast, Cache, Transaction Reversal and Security

Telecommunications and Networks Group
IIT Madras

Deepti Kumar
deepti@lantana.tenet.res.in

2nd December 2009

- Registration Process
 - Banks
 - MPP
- Broadcast Query Protocol
 - Algorithm
 - Analysis
- Transaction Reversal
 - Customer Initiated
 - Beneficiary Initiated
- Security

Registration Process

Registration with Bank

- Banks should have a system of registration before commencing mobile based payment service to a customer
- Enabling the option of mpayment services (via Internet, in person, etcetera)
 - Registration of default account/MPP
 - Procedure for changing default account

Registration of Default Account/MPP

- Mobile subscriber N gets a bank account in bank B1
- A/c holder N registers **only one account number** as his Default Bank Account
- N selects a Default MPP M1 from the list of the bank's MPPs
- Bank stores details & sends to the default MPP
- Bank B1 broadcasts a message to other MPPs/banks
<N's mobile number, time of registration T1>
 - This broadcast can be sent by default MPP on behalf of the banks

- Every other MPP receives the message sent by the MPP M1
- MPP M2 checks if it has any entry for the mobile number N which has been marked as default
- If so, the following happens:
 - Rule 1: if $T1 \geq T2$, then M2 cancels its default registration and informs the Customer by SMS
 - Rule 2: If $T1 < T2$, then M2 sends a message containing $\langle T2 \rangle$ to the originating MPP M1. This results in M1 canceling its default status by Rule 1



Procedure for changing Default Account/MPP

- Request the Bank/MPP with the default account to cancel the registration
- The Bank/MPP cancels the registration and informs the account holder
- The account holder registers a new default using the procedure above

Registration with the MPP

- The account holder may register with several MPPs as follows:
 - A/c holder contacts the default MPP by downloading the MPP software (or as described by the MPP)
 - A/c holder gets authentication credentials (such as a pin number) from MPP
 - The number of digits in m-Pin is left to the respective bank / MPP's discretion
 - Max length is 8 characters

tenet

Broadcast

- Payment Type 1:
 - Payment is made by entering the details of both parties
 - For each transaction `<party's name, mobile number, bank name, bank account number, MPP Id, amount>` is entered
- Payment Type 2:
 - The details that need to be entered are the **mobile number** of the 2nd party and the **amount**
 - Other details to be looked up by a special mechanism

Broadcast Query Protocol

- System must be able to automatically locate the account details (bank, MPP and account number) given a mobile number
 - Accomplished using **Default account** and a **Default MPP** which owns that account
- This default account for a specified mobile number is located using a broadcast query protocol

- Initiating MPP broadcasts the 2nd party's mobile number to all other MPPs
- MPP which owns the default account number responds with its MPP identity
 - Other MPPs ignore the request
- RBI authorised agency will maintain a website with a list of MPPs including <MPP name, MPP id, IP address, port number for connecting with other MPPs, CA signed digital certificate>



Analysis of Broadcast Protocol

- Unfairness
- Scalability with respect to subscriber population
- Scalability with respect to MPP Population
- Server Processing Capacity

- **Broadcast Miss**
 - Occurs when an MPP receives a request which is not meant for it
 - MPP is not the default MPP of the mobile number
- **Broadcast Hit**
 - Request received by an MPP that is meant for it
 - MPP is the default MPP
- **Overhead Ratio = Broadcast Miss/Broadcast Hit**

- Defined as the deviation of the overhead from the ideal case
 - Unfairness in the system when the subscriber population is unequally divided amongst the MPPs
- Zero, if all MPPs are equal in size
- Low
 - if only one large MPP and the others are small
- High
 - if two or more MPPs in the system are large

To improve performance
Staggered Broadcast is suggested



Scalability w.r.t Subscriber Population

- As subscribers increase, load at each MPP increases
 - Transactions per second increase

Subscriber Population	10K	1M	100M
Number of MPPs	5	10	20
No. of Transactions/Cust/10 hr	0.2	1	5
Transactions/Second Received by an MPP	0.04	25	13194.44

After 500,000 subscribers & 10 MPPs
Central DB mechanism should be adopted



Scalability w.r.t MPP Population

- Calculated in terms of the extra messages that the MPP server will have to process when the number of MPPs in the system increase
- As the number of MPPs grow query traffic increases, broadcast probability increases, probability of a Broadcast Miss increases

Number of MPPs	5	10	50
Prob of Bcast Miss at an MPP	0.48	0.72	0.95

Server Processing Capacity

- Server capacity is defined by the number of database lookups the server is able to perform per second
- With 100K subscribers, entire DB fits easily in RAM
- Assume, each lookup in the DB in the memory will take less than 1 ms
- **An inexpensive 3 GHz quad-core processor will suffice for the load**

tenet

Cache

- To reduce broadcast traffic and response time, the initiating MPP stores the `<mobile number, MPP identity, last accessed timestamp, creation time>` of the 2nd party in a local cache
- This cache is used in subsequent transactions
- The refresh period or age of the cache must be no more than 24 hours
 - Assuming that it will take 24 hours to complete a request for changing default MPP

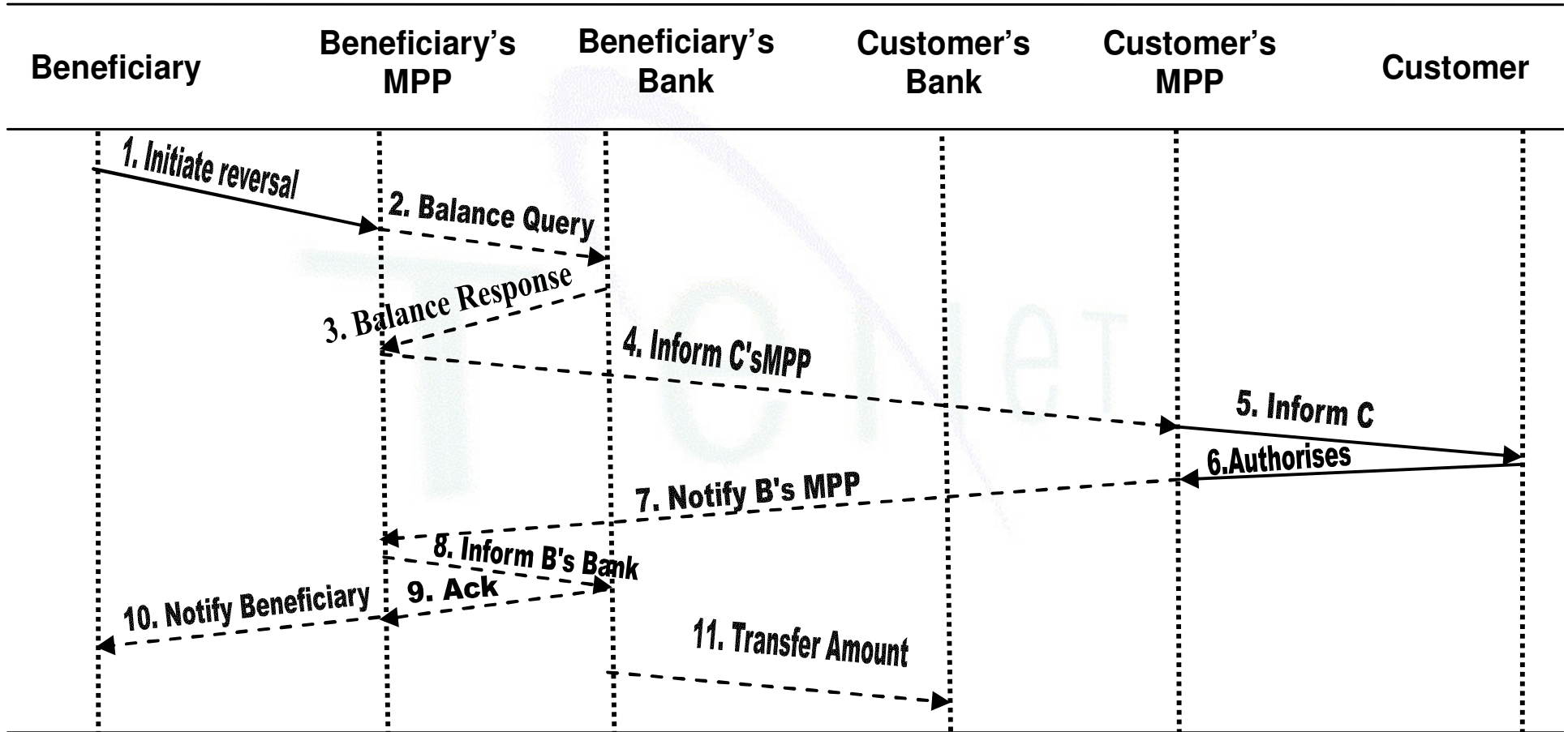
Updating the time stamp

- Whenever an MPP receives a broadcast reply, the entry is stored in the cache
 - If the entry corresponding to the A/c Number, MPP id and creation time already exists, update the **last accessed time**
 - If the entry does not match with creation time: cache entry stale, discard it

Transaction Reveal

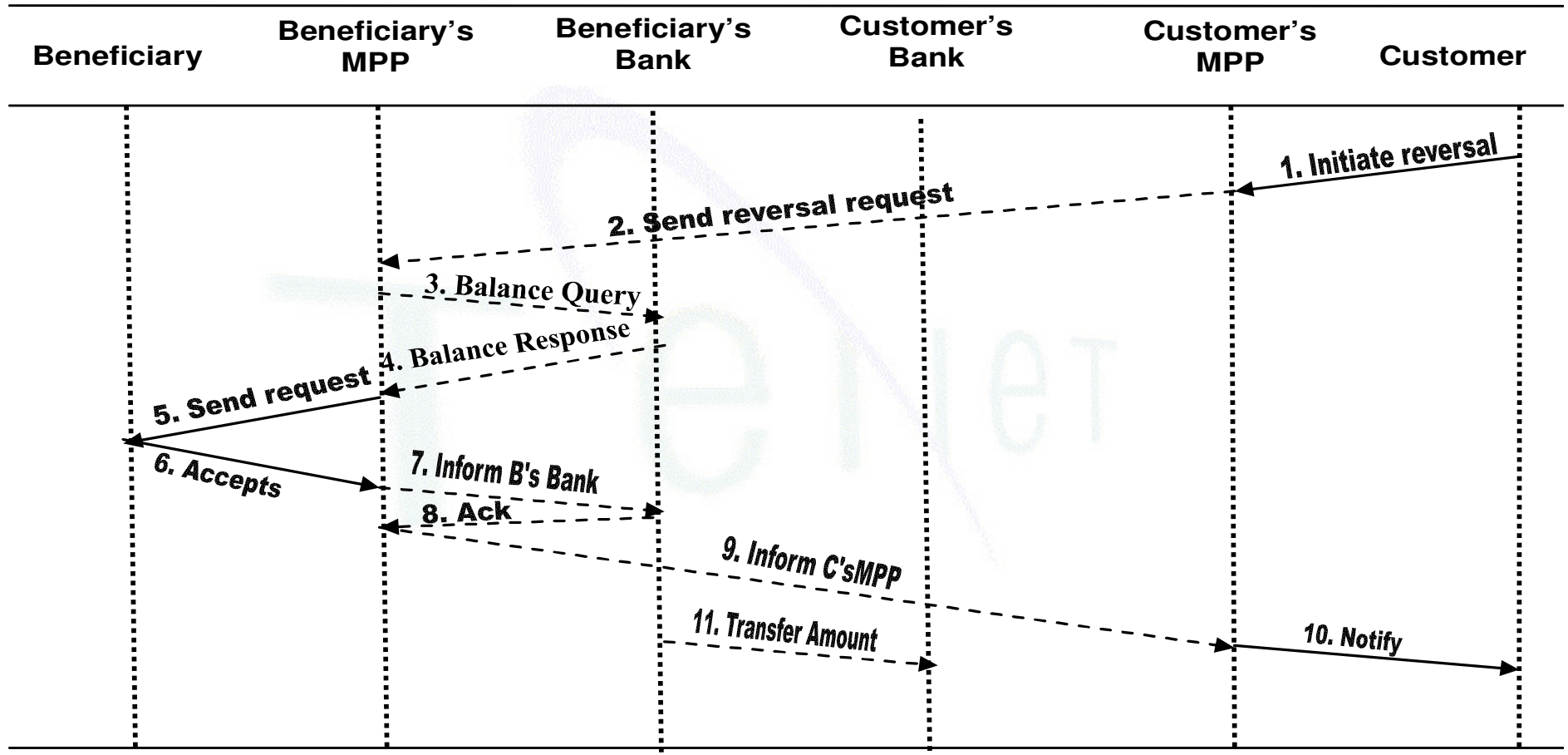


Transaction Reversal



Reversal of transaction (Beneficiary Initiated)

Transaction Reversal



Reversal of Transaction (Customer Initiated)

- Backend
 - SSL/TCP is used for an encrypted channel from source to destination
 - CA certified SSL
 - IDRBT can act as a CA and provide a set of certificates to the closed group involved in mobile payments
 - Use of bidirectional certificate checks: both client and server authenticate each other
- MPP-Customer
 - Two-factor authentication: e.g. phone number and m-PIN
 - Communication to be encrypted (method not in the standard)

- Users must register one *default* bank a/c and MPP
 - Choice with multiple banks+a/c supported
- Default account for broadcast query protocol
 - Provides ease of use: *enter only digits*
- Use of *cache* to reduce
 - broadcast traffic
 - response time
- Transaction Reversal
 - *Beneficiary* and *Customer* initiated supported
- Security
 - Back-end: CA certified SSL/TCP
 - MPP-Customer interface: two factor authentication