Multi-Party Payments for Mobile Services

Michael Peirce, Donal O'Mahony

Networks & Telecommunications Research Group,
Department of Computer Science, Trinity College Dublin.

{Michael.Peirce | Donal.OMahony}@cs.tcd.ie

Abstract

As mobile communications become increasingly sophisticated and ubiquitous, traditional mobile billing with its implicit trust relationships, will no longer be adequate. With a large number of mobile networks, a huge variety of value added service providers, and many millions of roaming users, it is desirable to remove any unnecessary trust in order to increase security and to provide incontestable charging. We present a multi-party micropayment scheme that allows all parties involved in a call to be paid in real-time. A pricing contract is used to allow dynamic tariffs for each leg of the call route and to prevent fraud. During a call a mobile user releases a stream of micropayment tokens into the network in exchange for the requested services. We discuss the problems of mobile billing, refer to related work in micropayment technology, and outline the design goals of the protocol before presenting the details of our solution.

1 Billing in Mobile Networks

In the fixed network a *call detail record (CDR)* or *toll ticket* is created for each call. This typically contains details about the call source, destination, duration and route. The CDRs are forwarded to a central database where periodically prices are applied to generate a customer's bill. Basic CDR billing has been extended to mobile networks where authentication with a home location register (HLR) is used to identify the call source. If the user roams into another mobile network then the CDRs created while placing calls must be transported back to the home network. The visiting network operator will bill the home network operator, who in turn bills the user. Billing based on CDRs cannot guarantee incontestable charging or payment for any of the parties involved.

To ensure payment some mobile operators have introduced prepaid solutions. These are based on temporary prepaid accounts at the HLR. The CDRs are examined immediately, a process known as *hot billing*, to allow automatic call termination when the account value reaches zero. Those that do allow roaming are based on a call back service through the home network.

2 Micropayments

A roaming user is likely to use many different network operators and value added service providers. Therefore it is desirable to be able to make efficient repeated payments of small amounts, called *micropayments*, to all the parties involved in a call as the services are used. Secure use of credit cards, electronic checks, and digital cash have been proposed to pay for services across a network [1]. However each of these *macropayment instruments* have a minimum transaction overhead, which make them unsuitable for repeated transactions of small amounts. In contrast micropayment systems minimize the communications and computational overhead.

Micropayment research has concentrated on repeated payments to a single vendor. Many of these schemes are based on the use of one-way hash functions to generate chains of hash values, including Pederson's phone ticks[2], PayWord[3], NetCard[4] and iKP micropayments[5]. The ESPRIT project CAFE[6] used Pederson's scheme to pay a single network operator for a phone call. Later, the ACTS project ASPECT[7] used the same scheme to pay a VASP for additional services. Our solution is novel in that it is the first time hash chains have been used to pay multiple parties at the same time.

3 Multi-party micropayments for mobiles

Future mobile systems will involve a large number of different public and private network operators. Through these users will be able to access a variety of on-line services provided by an even larger number of competing value-added providers (VASPs). A mobile user might arrive in a new network, place calls that are routed through several independent networks, and use the services of both local and remote value-added providers. Such a scenario is illustrated in Figure 1.

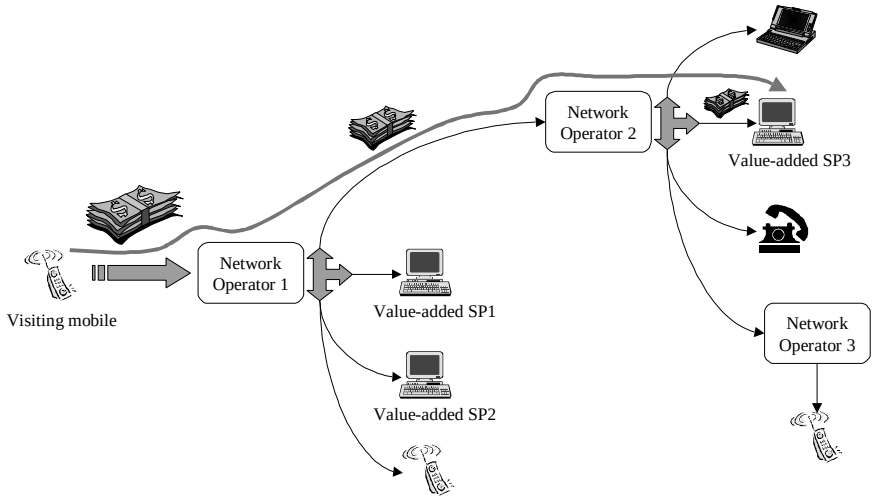

Figure 1. Multi-party real-time payment

3.1 Protocol Goals

The protocol was designed to solve the problems that CDR billing will face in future mobile networks and has the following goals:

- Real-time payment anywhere. A mobile user should be able to pay all parties involved in a call in real-time without need for authentication or contact with a distant home location register.
- Remove user accountability. Since mobile users are the greatest number of entities within the system they should be trusted the least. Unlimited credit with post-fact punishment is too open to abuse in a global system with hundreds of millions of users. The use of blacklists with stolen identities and equipment does not scale well.
- No user digital signatures. Use of digital signatures implies the existence of a public key infrastructure (PKI) with at least one certificate per signer. In addition the validity of a certificate must be checked in order to verify a digital signature. With millions of users, maintaining such a PKI is a huge task. A signature from a random roaming user, of which there are millions, will still not guarantee payment.
- Prevent inter-operator fraud. CDRs can be forged and it should not be possible for NOs to receive payment for services which were not used.
- Remove roaming agreements for billing. A negotiated bi-lateral agreement between operators should not be necessary for a roamer to make calls from a foreign network.
- Verifiable dynamic tariffs. A call charge should be able to be fixed depending on the service requested and current network conditions, and the mobile user should be able to verify that charge before payment begins.

3.2 Purchase of a Payment Chain

A mobile user buys prepaid tokens, through their phone or terminal, from a third party broker, using an existing macropayment system. The user nominates any specific service provider, called the *enforcer*, through whom the tokens will be spent. The mobile user initially creates the tokens by repeatedly applying a one way hash function, such as the Secure Hash Algorithm (SHA), to a root value P_X to generate a payment hash chain. The chain has no monetary value until *committed to* by a broker. To obtain this commitment the mobile user makes a macropayment to the broker, sending along the final hash (P_0), the chain length, the desired total value of the chain, and the identity of the enforcer through whom it must be spent. The broker commits to the hash chain, or promises to honor its value, by digitally signing the payment chain commitment ($Comm_P$):

$$Comm_P = \{P_0, \text{Length}, \text{Chain\_value}, \text{Enforcer}\}Sig_{Broker1}$$

The commitment shows that each *payment hash value* from the chain represents pre-paid value, redeemable at the broker. The value of a single payment hash is later fixed, on a per call basis, by the enforcer. This allows the *same hash value* to be used to pay all parties. The user is given $Comm_P$ which is stored with the secret P_X.

3.3 Pricing Contract

To make a call the mobile user must have a payment chain commitment for *any one* of the NOs or VASPs involved in the call. Figures 2 and 4 show the same call being made but with payment chains for different enforcer SPs along the route. In Figure 2 the local network operator is the enforcer. In Figure 4 the payment chain must be spent through VASP3. For example this could be a voicemail provider.

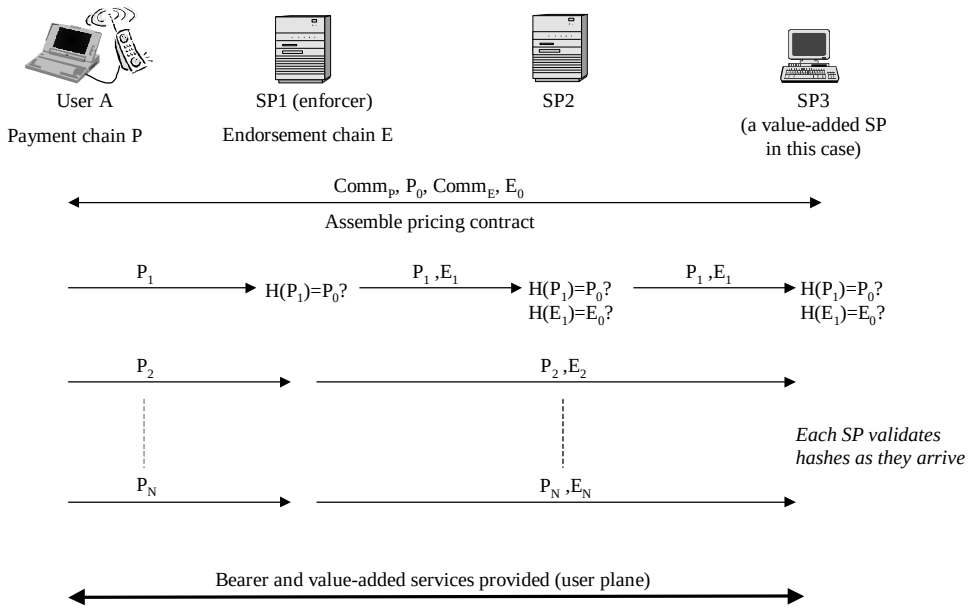

Figure 2. Mobile pays all SPs with same payment hash, with SP1 as enforcer

The user sends the call details and the payment chain commitment to the enforcer. A signed pricing contract, shown in Figure 3, is then generated by the SPs involved in the call. Its purpose is to allow verifiable dynamic tariffs, fix the starting hash in the payment chain, create a record of the call, and link a single payment commitment to multiple SPs for the call. The important fields are:

- SPs. The identity of each NO and VASP involved in the call.
- Charge. Charging mechanism and tariff rate for each SP.
- $Comm_{Pay\_chain}$. Payment chain commitment spendable through the enforcer.
- P_{Start}. Starting payment hash from the chain. For a new chain this will be P_0. For a partially spent chain this will be the last spent hash value.
- Start. Position of that hash in the chain.
- P_value. The value per payment hash for the duration of the call, fixed by the enforcer.
- $Comm_{Endorse\_chain}$. An endorsement chain commitment, created and signed by the enforcer SP. This is used to prevent double spending of payment hashes.
- Redeeming brokers. Each SP fixes the broker through whom they will redeem payment hashes for this call.

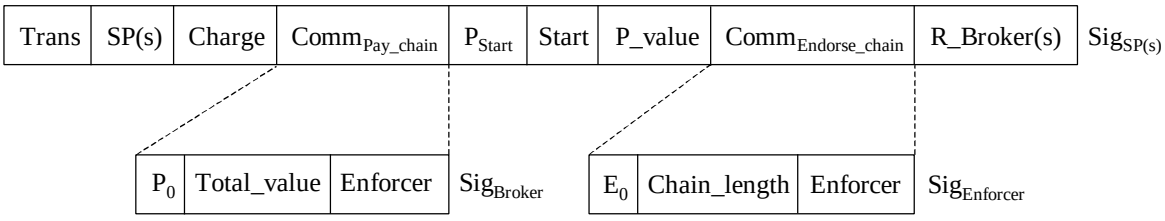

Figure 3. Contents of a pricing contract, payment and endorsement commitments

The enforcer is responsible for ensuring that the pricing contract is constructed correctly using a three-way handshake protocol. The pricing contract is presented to the user for agreement before the call is setup.

3.4 Releasing Payments during a call

Payment is *ongoing*, with the user releasing payment hashes at regular intervals. For a voice call this might be every second. In return for a valid payment the SPs continue to provide the service they agreed to in the pricing contract. If the user does not receive these services he can terminate the call by not releasing any more hashes. The total call cost per unit time, or per data unit transmitted, is the sum of each SPs tariff rate in the pricing contract. The enforcer fixes each payment hash to be worth the total cost per charging unit. For example in Figure 2 each SP might charge 1, 5 and 2 cents per second respectively. The enforcer assigns each payment hash to be worth 8 cents in the pricing contract.

Every second the user releases a payment hash, in this case starting with P_1 from a new payment chain. The enforcer verifies that the payment is valid by performing one hash function on it to obtain the previous payment hash, in this case the starting hash P_0. The enforcer forwards the payment hash and his own endorsement hash to the other SPs. Each SP independently verifies both the payment hash and the endorsement hash. Since the hash function is one way, payment hashes cannot be forged, and knowledge of the payment hash is proof of payment. When the SPs redeem P_{40}, the 40^{th} payment hash, they will be paid 40, 200, and 80 cents respectively.

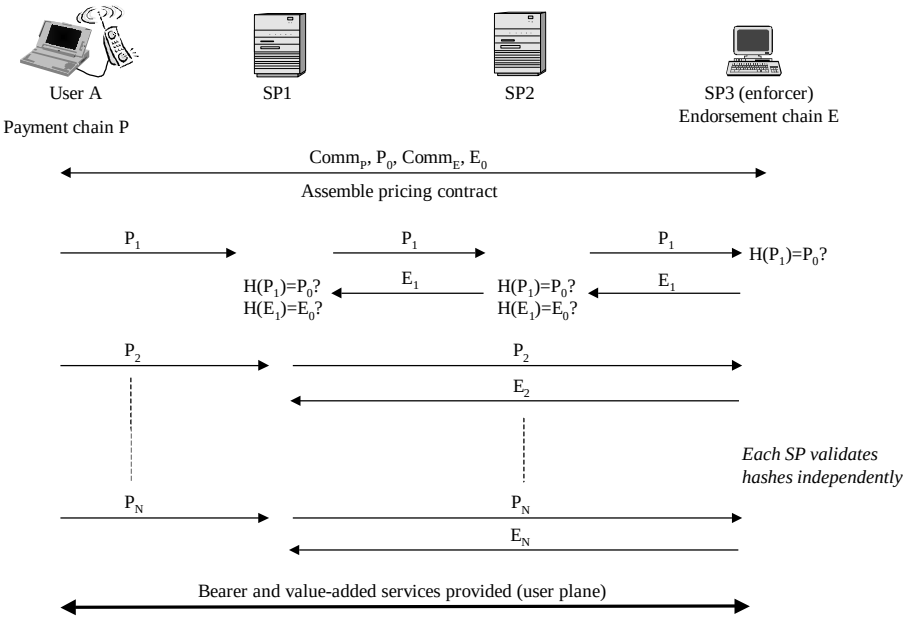

Figure 4. Mobile pays all SPs with same payment hash, with SP3 as enforcer

The enforcer keeps a record of how much of a payment chain has been spent and prevents *double spending* of payment hashes. The purpose of the endorsement chain is to prevent SPs from redeeming parts of a payment chain to which they are not entitled. A valid endorsement hash from the enforcer gives a SP, identified in the corresponding pricing contract, the right to redeem a valid payment hash. Unspent hashes can be spent later on a different call, using different SPs, through the same enforcer.

3.5 Redeeming Payment Hashes

At the end of the day each SP will redeem the highest spent payment hash from the call with their preferred broker. The broker will only accept a payment hash from an identified SP if a corresponding endorsement hash and pricing contract accompany it. Only the redeeming broker, fixed in the pricing contract by each SP, will redeem the hashes. The broker knows how much to pay each SP from the contents of the pricing contract. To verify the payment the broker will perform N hash functions, where N is the number of payments made, to obtain the starting payment and endorsement hashes. The redeeming brokers later clear payment chains in bulk with the issuing broker using a financial clearing network. A prototype has been developed in Java and demonstrated using NOMAD[8], an application based on a popular Internet Telephony package.

4 Conclusions

Current billing methods for mobile networks will become increasingly restrictive and inadequate as both the number of service providers and roaming users grow. To solve these problems a real-time multi-party micropayment scheme has been proposed. It uses a single pre-paid hash to pay all parties involved in a call in real-time. The idea of an enforcer and an endorsement chain were introduced. These allow unused pre-paid payment hashes to be spent through different entities without fear of double spending. Previous micropayment research has concentrated on providing payment to only a single party.

The scheme improves over current CDR billing by removing the need to trust users, eliminating the need for online user authentication with a home register, and avoiding use of user certificates. Incontestable charging is provided with flexible dynamic tariffs. In addition the need for inter-operator trust and complex billing agreements are removed. The scheme can be applied, not only to traditional mobile networks, but also to other scenarios where real-time multi-party payment is desirable such as Internet Telephony and wireless ad hoc networks.

References

[1] D. O'Mahony, M. Peirce, and H. Tewari, *Electronic Payment Systems*, Artech House Publishers, Boston/London, 1997.

[2] T. Pederson, Electronic Payments of Small Amounts, In *Security Protocols*, pp. 59-68, Lecture Notes in Computer Science vol. 1189, Springer-Verlag, Berlin, 1997.

[3] R. Rivest and A. Shamir, PayWord and MicroMint: Two Simple Micropayment Schemes, In *Security Protocols*, pp. 69-87, Lecture Notes in Computer Science 1189, Springer-Verlag, Berlin, 1997, http://theory.lcs.mit.edu/~rivest/

[4] R. Anderson, H. Manifavas, and C. Sutherland, NetCard - A Practical Electronic Cash System, In *Proceedings of the Fourth Cambridge Workshop on Security Protocols*, Cambridge, UK, 1996, http://www.cl.cam.ac.uk/users/rja14/

[5] R. Hauser, M. Steiner, and M. Waidner, Micro-payments based on iKP, In *Proceedings of the 14th Worldwide Congress on Computer and Communications Security Protection*, pp. 67-82, Paris, 1996, http://www.zurich.ibm.com

[6] J. Boly, A. Bosselaers, R. Cramer et al., The ESPRIT Project CAFE - High Security Digital Payment Systems, In *Computer Security - ESORICS '94 Proceedings*, pp. 217-230, Lecture Notes in Computer Science vol. 875, Springer-Verlag, Berlin, 1994.

[7] G. Horn and B. Preneel, Authentication and Payment in Future Mobile Systems, In *Computer Security – ESORICS '98 Proceedings*, pp. 277-293, Lecture Notes in Computer Science vol. 1485, Springer-Verlag, Berlin, 1998.

[8] D. O'Mahony, L. Doyle, H. Tewari, and M. Peirce, NOMAD - An Application to Provide UMTS Telephony Services on Fixed Terminals in COBUCO, Vol. 1, pp. 72-76, In *Proceedings of the 3rd ACTS Mobile Communications Summit*, Rhodes, Greece, June 1998.