

11:1 Anonymous Internet Access Method for Wireless Systems

Petri Jokela

Juha-Petri Kärnä

NomadicLab, Ericsson Research

FIN-02420 Jorvas

Finland

{petri.jokela, juha-petri.karna}@ericsson.com

1 Introduction

Accessing the Internet in current telecommunications systems is done using dial-up services. A circuit switched connection is established to the Internet Service Provider (ISP) and a tunnel across the connection is set up. IP traffic is sent from the accessing node to the ISP using e.g. PPP-tunnel [1]. The ISP takes the traffic out from the tunnel and forwards it to the Internet.

Mobile Internet is taking its first steps at the moment. The 2nd generation mobile telecommunications systems (such as GSM [2]) are providing Internet access with dial-up connections. Wireless LAN is not restricted in this manner but mobility support is only for a smaller area.

Circuit switched connections using GSM do not provide an attractive access method. The connection is slow and the cost is high. The new solution to provide a packet data connection also to GSM terminals is GPRS (General Packet Radio System) [3]. It can provide higher capacity than circuit switched (one channel) GSM connections and the terminal can be “always connected” to the Internet.

The 3rd generation telecommunications network, UMTS [4], is just about to come to the market. It provides faster radio link than the GSM network. The basic idea in the packet data transmission is, however, similar to the GSM GPRS. Data is tunnelled in the access GPRS network before it is sent to the Internet.

Both the 2nd generation and 3rd generation systems require user authentication when the user wants to access the network. The UMTS provides also a solution where the user does not authenticate himself to the visited network, but only to the home operator. The identity of the user is not revealed to the visited operator.

The anonymous access solution we are presenting here is based on a different concept. The access network is a very lightweight with only a minimum number of nodes present. The user data is not tunnelled in the network (only across the wireless link) but it is sent directly after the Radio Access Network to the Internet.

The visited operator is mainly interested in getting paid for the usage of the network. Current solutions in GSM and UMTS networks are based on the user authentication and charging information collection. The user is then billed later by his own operator. Also some pre-paid solutions are used in GSM networks. The user pays in advance for the service and can use the phone until the money has been consumed. Our solution uses on-line payments with e-cash. Depending on the chosen e-cash technology, the user privacy may vary. We are using e-cash concept invented by the eCash Technologies [5]. The solution is based on “blind signatures” and it gives the user a total anonymity. Even the bank cannot trace the user using the information received with the e-cash coins. Our implementation, however, does not exclude other payment methods such as a different e-cash implementation, a pre-paid method, a credit card or even the traditional user authentication and charging information collection.

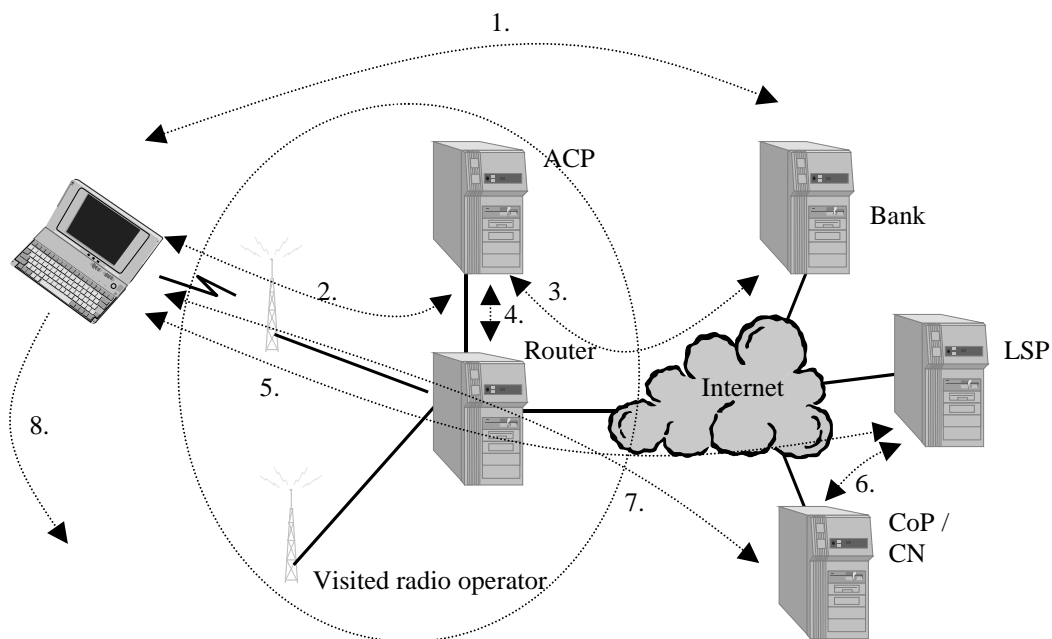
2 Network access

2.1 The network structure

Traditional mobile networks consist of separate radio access networks, connected to each other with a backbone network. The solution described here, built also as a demonstration network based on wireless LAN technology, does not provide any such backbone network, but radio access network islands are separate and only loosely connected to each other. Neither does this solution provide any solutions how the backbone network functionality is handled in this kind of network.

The Access Control Point (ACP) controls the traffic from the Mobile Node (MN) to the Internet (Figure 1). It configures the router to pass or deny traffic to and from the MN. The MN contacts the ACP to pay for the access by giving e-cash coins. The payment can also be done in a more traditional way by using some other charging method.

The bank node provides money for the MN and validates money given to it by the ACP. The Location Server and Service Provider (LSP) node provides the current location of the MN for other hosts and other services that can be bought using e-cash (they do not have to be located on the same node, but are usually totally independent on each other). The node can run for example a SIP server to which other nodes in the Internet send their call setup requests.



1. User makes withdrawal from the bank and gets e-coins (before coming to the visited network).
2. The MN contacts the visited network and sends e-coin(s) to the ACP.
3. The ACP verifies the coins from the bank.
4. The ACP configures the router to pass MN's traffic.
5. The MN makes a location update to a location server (LSP).
6. The Correspondent Node (CN) contacts the MN and resolves its current location from the location server.
7. The CN contacts the MN.
8. The MN moves to another base-station, a new IP-address is configured and the mobile-IP handles the traffic.

Figure 1. The network concept.

The Content Provider (CoP) is a totally independent node providing other services for the MN. Because the money which is used in paying for the access is not operator dependent, it can also be used to pay for the services. The MN in the test implementation is paying for the usage of different services by sending e-coins from the purse located at the MN to the CoP. The CoP in turn verifies the coins with the bank.

2.2 Access

In the following, the steps to connect to the Internet using radio access service provided by a visited radio operator are described.

First the mobile user switches his terminal on. The terminal searches for a network to log in. When it finds a network, it makes an IPv6 address autoconfiguration in order to get a prefix for its IPv6 address. When the address is configured, the mobile node is basically ready to communicate.

At this point, the ACP does not let any traffic pass from the mobile node towards the Internet. It must first receive a payment from the mobile node. When paying with e-cash, the mobile terminal sends an e-cash coin to the ACP (here the user must be sure that the ACP is not just a base station collecting money from roaming users and not giving any access to anywhere). The ACP validates the e-coin with the bank. The bank checks that the money is valid by checking the signature. It can not know to whom the coin has been given.

The bank returns a new coin (or it adds the amount of money to the account of the operator) to the operator and the operator configures the router to pass traffic to and from the mobile terminal. Some kind of QoS support can also be implemented at that point so that different priority data can have different price.

When the money is running out, the operator sends a notification to the terminal which then must send more money to get an uninterrupted access.

Because there is no authentication involved between the mobile user and the visited operator, there is a possibility that money is left unspent when connection is lost. If no information is maintained at the ACP to link the money and the mobile terminal, the money is left totally to the operator. If micropayments are used, this may be acceptable as the lost amount of money is usually very small. However, from the user point of view, this is still annoying. And of course, the smaller coins are transferred, the more transactions are needed during connection which in turn increases communication between the operator and the bank if on-line payment validation is used.

One way to overcome the problem is that the user gives his public key to the operator. When the user after a break contacts the operator, he can send some information signed with his private key. The operator can now link the money left at ACP and the connected mobile terminal. The public key should not be always the same as the operator can then make analysis about the movements of the mobile user, but it should be regenerated every now and then.

2.3 Mobility

When the user is normally accessing the Internet at the visited location, Mobile-IPv6 handling the mobility sends binding updates to the home agent located at the home network. However, in the concept described in this paper, the user does not need to have any home network which means that the home agent cannot be in the home network. The solution is to let the visited network to handle the home agent operations.

After switching on the terminal, it is configured with a new IPv6 address. This is done using IPv6 address autoconfiguration. Normally this address is just a Mobile-IPv6 care-of address which is updated to the home agent. Because we are now using the visited network also as a home network, we choose this first address to be our "temporary home address". The ACP allocates a home agent for the mobile user and configures it to contain the node with that address as the home address for the terminal. When the user is moving and changing the IPv6 address of the interface, binding updates are sent to the home agent. On the application level, the first address received from the visited network is considered as the home address.

The demonstration network was running IPv6 address autoconfiguration which easily provided new addresses for the mobile host. This is not a good solution in general case because the user can be traced using the lower 64 bits of the IPv6 address (host identifier part). In a real case, the host identifier part of the address must be chosen so that it changes when the node attaches the Internet from various places. With this system the user movements cannot be (easily) traced by other hosts by monitoring the traffic. There are many different possibilities to solve this problem, but we do not discuss that issue on this paper.

3 Anonymous Access using e-cash

3.1 General

The payment process has traditionally been based on user authentication, charging information collection and billing afterwards. Other payment methods are also used, such as prepaid access. The user pays in advance and, using some kind of authentication method (not user authentication) the paying user is connected to the amount of money paid in advance for the payment receiver.

Electronic cash is a step further in payment systems. The e-cash coins correspond more or less to the traditional money. The problem with electronic cash is that it can easily be copied which is in normal cash prevented by different techniques (e.g. putting identifying elements in paper money). One and maybe the easiest solution to prevent this double spending of the same money is to authenticate the user when he gives money. This, however, is not a very good solution as people are used to the anonymous payment: when they pay for something in a shop with traditional money, they remain anonymous to the shop and nobody can trace them afterwards.

Different solutions to provide anonymity to the user have been proposed. An e-cash method based on a tamper proof device (e.g. a device, the user cannot access) can provide anonymity. This device is given by some trusted party (e.g. bank). When payments are made, the device itself destroys the money from the purse and double spending is prevented. The user must also trust that the system is really providing anonymity and the bank is not collecting information about the user. This kind of solution is of course possible to use to pay the access in our network, but we saw that it did not fully guarantee anonymity for the user, so we decided to choose another method.

The solution we chose is based on “blind signatures” introduced by D. Chaum [6] [7] and implemented by eCash Technologies Inc. [5]. With this method the user can remain anonymous both to the payee and to the bank. Double spending is either detected using on-line checks where the payee contacts the bank each time when it receives the coin and before accepting it. In our test network, the concept for this solution has been implemented. The other possibility is to use more “real cash” type of solution, off-line payment where the payee does not have to contact the bank, but the user can be traced afterwards if the same coin has been used more than once.

3.2 Untraceable E-cash

To make the e-cash coin untraceable, Chaum [6] proposes to use “blind signatures” when the user makes a withdrawal from the bank. This method can hide the user identity from the bank at the withdrawal phase.

The withdrawal process starts when the user makes an e-coin (from a pool of “lots of coins”). He chooses a random factor with which he blinds the coin so that it looks like a random mess. He sends the coin to the bank with the information about the value of the coin. The value of the money is taken from his account and the bank signs the blinded coin with bank’s secret key which is bound to this certain amount of money. The bank can have keys bound to different amounts of money, for example 1\$, 5 \$ and 10 \$.

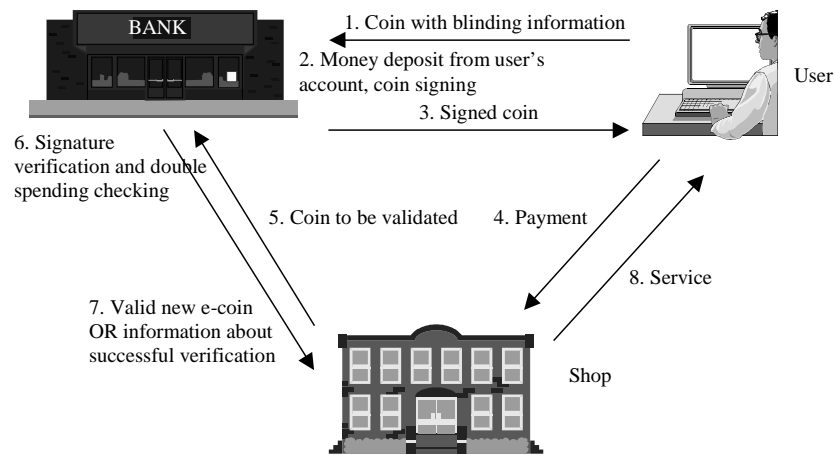


Figure 2. Anonymous electronic cash.

The bank returns the signed coin to the user who removes the blinding factor from the coin. He has now a valid coin with a valid bank signature. The user can now use the coin. This scenario now makes on-line checking mandatory for the payee. When the user sends the coin to the access provider, it must send the coin to the bank for verification. The bank verifies the signature and checks the used coins database to prevent double spending. If the coin was acceptable, the amount of money is debitted to the account of the access provider and the coin is added to the used coins database. The access provider gets information about this and can let the mobile user to access the network.

Off-line payments would be much more flexible on the system. The access provider would not need to make checks every time the user sends a coin. Solution for this is presented for example in [8]. The user adds some identifying information to the coin when he makes a withdrawal. When he makes a payment, a piece of identification information is sent with the e-coin to the payee. The payee sends this information later to the bank with the e-coin. The user cannot be identified from one piece of identity information. If the coin has been used twice, two different pieces of identity information can be found from the bank and combining these pieces, the user's identity can be revealed.

3.3 Open questions

In general, are radio operators willing to open their networks to be used without user authentication? The abuse of the network may be the thing that prevents network operators from doing that. In a limited sense, when the visited network does not care about the identity of the mobile user, but gets a positive authentication message from the home operator of the mobile node, this can be better accepted. But again, this is no longer an anonymous access.

The payment solution presented in the demonstration network does not provide a good way to make micropayments, which is almost a mandatory requirement in this kind of access method. With on-line payments, the bank can be easily overloaded so that the off-line payments would make more sense. In [8] different methods to connect partial user information to a coin (such information that one piece cannot be used to identify the user, but two pieces is enough) has been presented, but the suitability of these methods to micro e-coins must be verified. Some of the methods are just too heavy and the cost of processing can be more than the value of the coin.

Electronic coins are made by signing the coin itself with a bank's key. The key depends on the value of the coin so that the bank can afterwards verify the correct value of the received coin. If micropayments are used, withdrawal process can be long if the user is creating a lot of tiny e-coins. This is, of course, much depending on the capacity of the computers of the bank.

Another problem is the scalability. The pool for electronic coins (from which the user chooses the coin when making a withdrawal) must be large to maintain the anonymity [8]. When we are making micropayments, the number of needed coins grows very fast.

When a mobile user contacts the radio operator, he makes already negotiations in order to get the IPv6 address for the terminal. However, if the user is not even planning to pay for the access, network resources are wasted. This can lead to Denial of Service attacks when mobile node makes consequent negotiations with the network. The problem will exist always when we have an open network, where the user can configure the terminal and run different software without the control of the operator.

4 Conclusions

With anonymous access, users can be provided with more privacy than in traditional telecommunications networks. Non-anonymous access has not been a very big problem when the operator functions are strictly controlled by governments. In the future this may be one very important point if the number of radio access providers is increasing.

The main advantage for the radio operator is that this kind of networks are very simple and cheap. The IP traffic is going directly to the internet without a heavy network. To get this kind of network to work, much more work is required to overcome the previously introduced problems.

Using the Home Agent at the visited network provides one way to handle the mobility when the user does not have any home network. He does not have to make any authentications to other places in order to get mobility support. There may, of course, be problems when the temporary home agent is at the visited network, for example when a big happening ends and a lot of people switch their terminals on at the same location. The home agent allocated at that point will remain until the user switches the terminal off. Naturally, the operator can get paid for the usage of the home agent.

With traditional money the user has anonymity and he can also use the same money not depending on what he is buying. This is an advantage which is not yet achieved in e-cash: there is a huge jungle with different kinds of e-cash systems, some providing more anonymity and some less. The e-cash system which will be used must be as easy to use and also as controllable for the user as normal money has been. This implemented concept could provide a bit similar system as traditional money. The problem is to make one system the standard, and that is not a simple task to do.

Despite of the problems with this kind of network, the advantages make the solution attractive. With a very lightweight solution, both end-users and operators get something more: users faster and more open services, operators a cheaper and simple network still giving the possibility to provide more services for the user.

References

- [1] W. Simpson, "The Point-to-Point Protocol (PPP)", IETF RFC1661, July 1994.
- [2] General description of a GSM Public Land Mobile Network (PLMN) (GSM 01.02), European Telecommunications Standards Institute, March 1996.
- [3] General Packet Radio Service (GPRS): Requirements specification of GPRS (GSM 01.60), European Telecommunications Standards Institute, April 1998.
- [4] Universal Mobile Telecommunications System (UMTS); Objectives and overview (UMTS 01.01), European Telecommunications Standards Institute, February 1996.
- [5] eCash Technologies Inc. <<http://www.ecashtechologies.com/>>
- [6] D. Chaum, "Blind signatures for untraceable payments", Advances in Cryptology – CRYPTO '82, pages 199-203, New York, 1983. Plenum Press.
- [7] D. Chaum, "Undeniable signature systems", US Patent no: 4.947.430, August 7, 1990.
- [8] L. Law, S. Sabett, J. Solinas, "How to make a mint: the cryptography of anonymous electronic cash", National Security Agency Office of Information Security Research and Technology, Cryptology Division, 18 June 1996.