

Wireless Internet Access Using Anonymous Access Methods

Petri Jokela
Ericsson, NomadicLab
02420 Jorvas
Finland

Abstract- Accessing the Internet from a mobile computer can currently be done by opening a circuit switched call to the ISP (Internet Service Provider). New packet based services are now being introduced, such as the GPRS (General Packet Radio Service) for the GSM system.

The solution described here will give a simpler access to the Internet, at the same time providing complete user anonymity. However, the solution here doesn't exclude the use of traditional accounting methods, or more sophisticated electronic cash solutions which do not provide anonymity at the same level, as the solution described here.

A MH (Mobile host) attaching to a visited radio network receives an IPv6 address prefix from the access router in the visited network. The MH configures the whole IPv6 address for its interface. After initialization, it starts paying for the radio and Internet access to the visited radio operator. Paying method is e-cash, providing full anonymity for the mobile user. After receiving access to the network, the mobile user registers its current location information on a Location Server (dynamic DNS or some other), so that other hosts can resolve the mobile user's current IPv6 address and contact the roaming mobile user.

The same e-cash, which is used to pay for the network access, will be used to buy services provided in the network. Services can be either local or global. Local service could be, for example, buying a soda, global such as receiving a video stream from a video server.

I. INTRODUCTION

Internet access through current cellular networks is provided by using dial-up services. First, a mobile user has to dial his Internet Service Provider and, using e.g. the Point-to-Point protocol (PPP) [1], transmit IP-packets first to the ISP, who in turn forwards the packets to the Internet. Circuit switched connections in a cellular network are relatively expensive, which makes this type of connection very expensive for the user. Efficiency is not very good, as most of the traffic is bursty and intermediate times when data is not transmitted may be long. From the operator's point of view, one channel is reserved for one user, and it is not necessarily used (meaning that operator could make more money by sharing this channel with other users).

New solutions are emerging now. For example, in the GSM system [2], the idea of using same physical channel for many users is taken into use in the General Packet Radio System (GPRS) [3]. GPRS is already been marketed. It provides packet mode access for mobile users by allowing terminals to send data using unused timeslots in the radio access network. So, the less other user connections are reserving the radio network, the more connection bandwidth

the GPRS user gets. There is, however, quite a complicated functionality behind the GPRS system. The data traffic is routed in the visited GPRS system through GSNs (GPRS Support Nodes). During this traversal, packets are tunneled using GTP (GPRS Tunneling Protocol). This obviously increases the packet overhead.

The third generation mobile system, UMTS (Universal Mobile Telecommunications System) [4], is going to appear on the market soon. In the current phase of standardization, the basic idea of making a data connection to the Internet is quite similar to the one used in the GPRS network.

In future telecommunication networks, a similar visited network tunneling does not have to be used. The access could be received directly from the mobile host to the Internet. Basically, the data traffic could be taken "out of the telecommunications network" immediately after the base station, or at the first router on the route path. This causes some changes to the mobility management function. In the second and third generation cellular systems, mobility is handled by the cellular network itself. If, however, the data is not going through the whole visited network, mobility management is not used. In this case, Internet mobility management methods (Mobile-IP [5]) are used.

For operators, accounting is the main interest. In current systems the visited radio network authenticates the user with help of the mobile user's home operator. Using this information, the visited operator sends billing information to the mobile user's home operator, which in turn will charge the user for the usage of the visited network. This charging is only counting the usage of the telecommunications network.

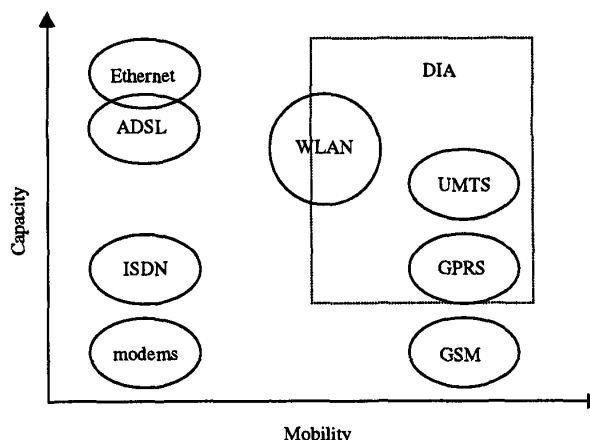


Fig. 1. Positioning of the proposed concept in current wireless and wireline environment.

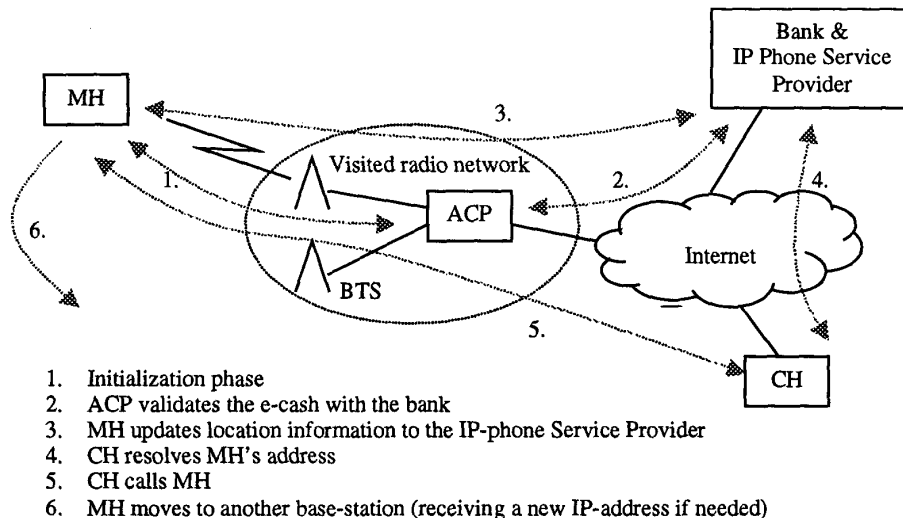


Fig. 2. Demonstration network for the proposed system

The usage of the Internet is billed by the ISP with which the mobile user has made an agreement, and to which she makes the call from the visited network location.

Accounting can be based on different criteria (time based, data amount based, Quality of Service based, ...), and our proposed system does not make any restrictions on what accounting system is chosen.

The built demonstration system uses a Wireless LAN network to simulate the radio access network. The system has been carefully checked so that it meets the requirements which the UTRAN (UMTS Terrestrial Radio Access Network) sets on both ends of the radio connection. This ensures the best possible compatibility if the proposed system is to be implemented in the future mobile telecommunications systems. The positioning of the proposed system, called DIA (Direct Internet Access), is shown in Fig. 1.

The UMTS network provides good possibilities to enhance data services even more than there has been done during standardization. However, our work goes beyond the UMTS system. The radio network is simulated with a wireless LAN (IEEE 802.11, 2.4 GHz) network, and the core network is based on an IPv6 network [6] with mobility support (Mobile-IPv6 [7]). In the future, the wireless LAN can be replaced with UTRAN (UMTS Terrestrial Radio Access Network).

The following sections show how it is possible to anonymously access the Internet and, at the same time assure that the visited radio operator gets paid for usage of his radio network and for the Internet access. The proposed system makes as few requirements on the e-cash system as possible. So, other methods, such as traditional accounting models could also be used with small changes in the system. Neither does this solution exclude the traditional ISP from existing in the system. He might only have a slightly different role.

II. DEMONSTRATION SYSTEM

The demonstration system forms a small-scale Internet. All computers are connected to one host, ACP (Access Control Point), acting as a router.

The operating system on all hosts is FreeBSD 3.2 with Kame [8] IPv6 stack installed. The Kame package also contains IPsec [9] (with IKE implementation), which is used to provide needed security in our network.

Location server, to which the mobile host can update its current IP-address at the visited network (shown in Fig. 2) is simulated with dynamic DNS [10] (provided also with the Kame package). The location server is running on the IP-Phone Service Provide -node (see Fig. 2). The location server could be, for example, a SIP (Session Initiation Protocol) [11] server, providing mobile user location information to hosts willing to call our mobile user.

Mobility in the visited radio network is handled using mobile-IPv6. The implementation has also been developed in the same project within which the DIA concept was created.

The application simulator is implemented using Java. It provides a graphical user interface (PDA-like), where the user can configure security related information and select and download services provided in the network (either services which are "local", i.e. provided near the current location of the mobile user, or services provided at other locations in the Internet, like at "home" location of the mobile user). The implementation uses Java RMI to communicate between the client at the MU (Mobile Unit) and the application server at the CH (Correspondent Host) node. Downloading a service means really that the PDA-device downloads a piece of software which implements the service. Due to limitations in Java (i.e. missing IPv6 support), traffic generated by Java applications is tunneled using IPv4 in IPv6 tunnels between hosts where needed. This ensures that all traffic in the network is IPv6 traffic.

For accounting purposes, a simple software is implemented to simulate the concept of eCash's anonymous electronic money [12]. Anonymity in this system is based on blind signatures [13], where the user together with the bank can make the "coin" look like a valid "coin" (from the bank's point of view), but bank cannot afterwards say to whom it gave the coin. The Java implementation includes following components:

- Electronic purse at the MU to maintain money for the mobile user.
- ACP Access Controller to maintain state information about the MU connection (how much money it has paid for the access, how much is left and so on). With this information the ACP can control the MU's access through it towards other hosts in the Internet. The ACP Access Controller also checks the validity of the received money with the Bank node.
- Bank to generate money and to validate used money to prevent double spending.
- CH to sell services to the MU. It also implements the money checking procedure.

III. DEMONSTRATION

A, user carrying a PDA (running on the MU), switches it on. The PDA device notices that it is under the coverage of a WLAN network and starts an address autoconfiguration procedure with the ACP (Router Solicitation / Advertisement pair). It receives the IPv6 address prefix and makes its IPv6 address using the physical address of the network card as the lower part of the IPv6 address. To ensure the anonymity of the user, something other than the network interface physical address could be used (to avoid snoopers on the Internet to make information collection and to follow a network interface traversal in the Internet, using the routing part of the address as the location information source).

During the address configuration, the visited radio operator notices that it has a new mobile node wanting to access the Internet using its radio access service. The ACP sends a notify message to the MU, telling information about the access and requesting money for the usage of the radio network (phase 1 in Fig. 2). The PDA responds by sending e-cash coin(s) to the ACP. ACP checks the validity of the e-cash coin from the Bank (phase 2 in Fig. 2), and if success, it configures the router to pass packets to and from the MU.

This solution is not limited to the eCash electronic money, but other methods can also be used. The used solution is not scalable as all "coins" have to be checked on-line at the bank. If not done so, double spending of coins cannot be prevented. This leads to other solutions, such as a tamper proof device at the MU to make sure that the user cannot spend the same money more than once.

The ACP now keeps track of the MU usage of the network. After the money is almost "used" (either time is running out, or the amount of data transferred almost exceeds the paid limit), it again sends a notify message to the MU, telling that more money is needed to keep the connection alive.

Following a successful login to the network, the MH makes a dynamic update to the DNS (representing the IP-phone operator) with its current IPv6-address (Phase 3 in Fig. 2). The MU can now be contacted by other hosts. They can now resolve the current location of the MU from the location server (phase 4 in Fig. 2). If the location server is a SIP server, the CH can make an IP-phone call to the MU (phase 5 in Fig. 2).

Roaming under one radio operator is simulated using two Wireless-LAN base stations, connected to the same ACP. Mobility is handled using Mobile-IPv6 (Phase 6 in Fig. 2).

IV. CONCLUSIONS

The demonstration system described in this paper has closely been modelled after the current standardization in the UMTS system. The system here could be implemented in such a system.

In UMTS-based systems, terminals don't necessarily have a MAC-style hardware address. That's why some other way has to be found to generate a unique address for the terminal while operating under a visited network. Mobile user identifier, IMSI (International Mobile Subscriber Identity), or some part of it could be used as part of the IPv6 address for the MU. This, however, reveals the user identity information to the network, which in some cases is not wanted by the user. He might be traced from the network and the information about his locations could be registered. There are certain temporary identifiers generated in the visited network, which can be used instead to form the full IPv6 address. Because these identifiers vary when the user changes the point of attachment, he cannot (easily) be traced and identified from other hosts in the Internet by snooping traffic.

The electronic cash system used in this solution is useful, when complete anonymity is required. However, it does not scale well. All coins used in this system must be checked sequentially in the Bank node. Only with this checking system can the double spending of coins be avoided. There can also be other disadvantages with anonymity. Risk for Denial of Service attacks is usually higher. There should be some way to identify an attacker and to either initiate some legal action to make the attacker responsible for his actions or to prevent the attacker from making the same kind of attacks again against the system.

Unfortunately, maybe there are too big risks in providing an access method for a user, who doesn't have to reveal the identity information to any entity in the network. Half-anonymous solutions (such as the one specified in the UMTS standards, hiding the user identity from the visited operator) could possibly be a more realistic option. On the other hand, this could also be implemented with some non-anonymous e-cash solution. The identity of the user could be traced either after double spending of coins or only after some kind of attack against the system.

Furthermore, fully anonymous access using a radio network can cause legal problems in some countries. If local law requires that there has to be a possibility to decrypt a certain user's radio traffic, the key to decrypt the traffic has

to be available at the radio operator. If the user cannot be identified at all, the needed key for decryption cannot be retrieved.

Operators are keen on keeping their "own" customers. This means that they are not necessarily very happy with the anonymous access concept, as they want to be the operator that provides the customer all possible services. This solution makes the competition harder, as all services have to be bought separately. Traditional ISP's may lose customers to other service providers, but, on the other hand, they may even manage to get new customers who are accessing the network only in an anonymous manner.

There are still some open questions which require future work:

- Denial of Service attacks in an anonymous environment: detecting and preventing
- Providing seamless handover between different radio access systems: providing users with faster access while going through a Wireless LAN network and switching back, for example, to a UMTS system when going out of range of the W-LAN network.

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] C. Perkins, "IP Mobility Support", IETF RFC2002, Oct. 1996.
- [6] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 2460, Dec. 1998.
- [7] David B. Johnson, Charles Perkins, "Mobility Support in IPv6", IETF Internet Draft, June 1999.
- [8] Kame project, <<http://www.kame.net>>
- [9] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", IETF RFC 2401, Nov. 1998.
- [10] P. Vixie, S. Thomson, Y. Rekhter, J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", IETF RFC 2136, April 1997.
- [11] M. Handley, H. Schulzrinne, E. Schooler, J. Rosenberg, "SIP: Session Initiation Protocol", IETF RFC2543, Mar. 1999.
- [12] eCash Technologies Inc. <<http://www.ecashtechologies.com/>>
- [13] D. Chaum, "Blind signatures for untraceable payments", Advances in Cryptology - CRYPTO '82, pages 199-203, New York, 1983. Plenum. Press.