Anonymous Network Access using the Digital Marketplace

Alisdair McDiarmid, James Irvine
Institute for Communications and Signal Processing, University of Strathclyde
Email: a.mcdiarmid@strath.ac.uk, j.m.irvine@strath.ac.uk

***Abstract*— With increasing usage of mobile telephony, and the trend towards additional mobile Internet usage, privacy and anonymity become more and more important. Previously-published anonymous communication schemes aim to obscure their users' network addresses, because real-world identity can be easily be derived from this information. We propose modifications to a novel call-management architecture, the Digital Marketplace, which will break this link, therefore enabling truly anonymous network access.**

I. Introduction

Anonymous communication has been of interest to researchers for many years. The most basic goal of this research is to allow message sending without revealing the identity of the sender. Several schemes exist in the literature which meet this aim under certain circumstances, many of which also conceal other information about the communication[1][2][3][4].

One assumption common to all of these proposals is that a person's identity is defined as their network address. Currently, this is accurate: for example, in many countries Internet Service Providers are legally obliged to divulge to the authorities any information which ties a network address to one of their customers. Since network addresses are assigned by the network service provider, this applies to all fixed and mobile Internet communications. From a privacy standpoint, it would be far preferable to remove this link between network address and anonymity at source, thus greatly reducing the impact of failure of a higher-layer anonymity protocol.

The Digital Marketplace (DMP) is a next-generation call management architecture which enables free-market competition for connectivity on a per-call basis[5]. Recent work presents an analysis of the many security issues inherent with the architecture[6], and a series of modifications which ensure secure operation[7]. In this paper, we propose further modifications which would allow DMP users to place bids and receive service without revealing any identifying information, therefore enabling truly anonymous network access.

II. Anonymous Network Access

Many anonymous communication protocols are based on mix networks[8]. The core principle of such protocols is simple: sending an encrypted message on an unpredictable path makes it difficult for an observer to determine the sender. Additions to this technique include: padding the message to stop attackers gaining information from the content length[3]; sending false traffic to ensure that eavesdroppers cannot prove that a message was sent at all[9]; higher-level protocol inspection to prevent timing attacks based on multiple requests[4].

The threat models of these protocols have several features in common. The most clear commonality is that the identity of the user is tied to the network address, and therefore the address is the information that the protocol tries to obfuscate. This is most crucial in the failure case: when the network address is discovered by an attacker, it is often trivial to link this to a real-world identity.

Additionally, even when using anonymous communication schemes, the network operator is in a position to record communications metadata: for example, time of transmission; or in mobile systems, the user's location. These data can be analysed to track the user's communication habits and whereabouts, revealing still more information which many people feel should be private. Recently, mobile network operators have faced public criticism over handling of their customers' personal information: examples include secretive location-tracking services in the UK[10], and cell phone call records in the USA[11].

Therefore, we believe that it is desirable to break the link between network address and identity, which is only feasible with wireless network access. This would provide a solid foundation on which to build a series of privacy measures, including using the anonymity networks discussed above. With no ability to determine a user's identity given their network address, the consequences of failure of the anonymity scheme are much less significant. Furthermore, allowing users to fully hide their identities from their network service provider allows a fundamentally new perspective on anonymity: instead of normally being identifiable, users can be anonymous by default, and will remain so unless they reveal identifying information. This circumvents the problem of the increasingly-untrustworthy network operator, using technical rather than legal methods.

III. Digital Marketplace

As mobile systems evolve beyond the third generation, new challenges arise in network service provision. Users will request access to a diverse range of services, which will cause increasing demands on the network. Higher capacities will force a move to environment-optimised air interfaces and smaller cell sizes. Current call management architectures are insufficiently flexible to cope with these changes.

One solution to this problem is to employ a market-based middleware. The Digital Marketplace proposal introduces the

1-4244-0063-5/06/$20.00

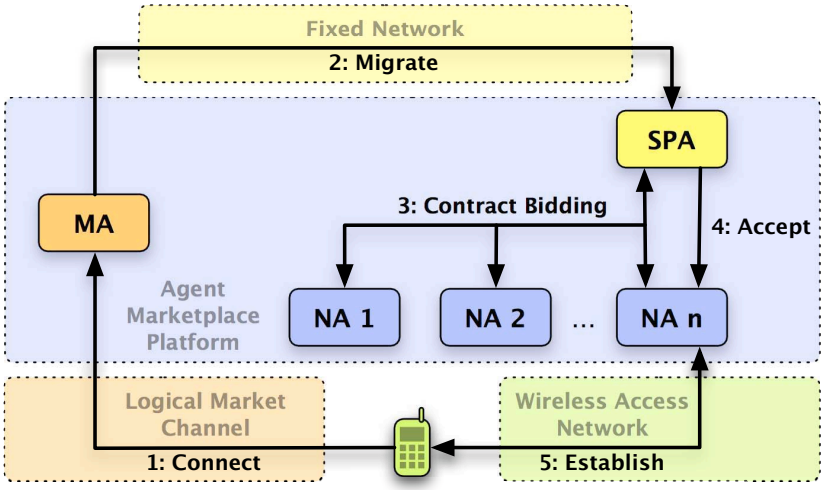

Fig. 1. Organisation of agents in the Digital Marketplace, represented as a simplified protocol diagram

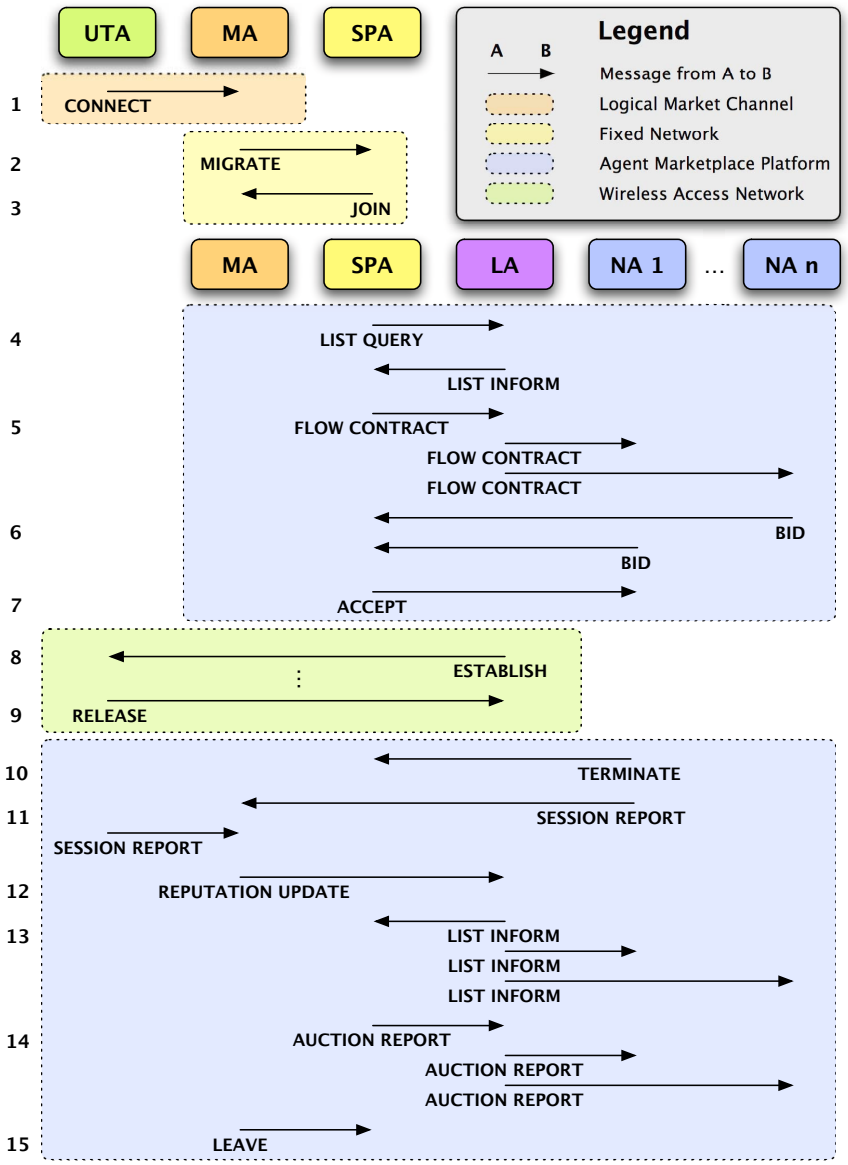

Fig. 2. Secure Digital Marketplace protocol operation; see also section III-B

concept of a market channel, across which auctions for service contracts are conducted[12]. This allows many independent network operators to supply network connectivity, via service providers, to mobile users. With correct protocol design and implementation, a freely-operating market can be achieved[5]. It is argued that this will optimally and fairly allocate network resources.

A. Overview

Consider a mobile user who wishes to initiate a communications session. The user's terminal scans radio channels, seeking a marketplace channel broadcast signal. Once the market is located, the terminal transmits a session contract stating quality and price requirements, either to make a new call or initiate a registration and paging contract. This allows Digital Marketplace users to both make outgoing and receive incoming calls. The market operator agent (MA) forwards this request to the user's service provider (SPA), which then enters the agent marketplace platform to negotiate on behalf of the user. Registered network operator agents (NAs) propose bids on the contract tenders, and the service provider selects those which best match the requirements. Each network operator has a market reputation, based on how well it has previously met its contract requirements; this is considered in the selection process, and is updated after every session. See figure 1 for an overview of the marketplace organisation.

B. Current Protocol Operation

Previous work has outlined the Digital Marketplace protocol operation[7]. The sequence of interactions in the protocol session is given below, and in figure 2.

1: User Terminal Agent (UTA) makes a connection request to the Market Agent (MA). The request includes the network address of the user's service provider, and a session contract. **2:** MA forwards the contract to the service provider, including the network location of the marketplace, and the address of the Logging Agent (LA). **3:** The service provider migrates a negotiation agent (SPA) with the contract to the marketplace.

4: SPA verifies that the LA is running on a secure platform, then requests the list of Network Agents (NAs) and their reputations. The LA responds with the list. **5:** SPA analyses the session contract, creates a flow contract, and forwards the flow contract to the LA. The LA forwards the flow contract to all subscribing NAs.

6: NAs calculate their commitments, and make appropriate bids. **7:** SPA selects the most suitable bid(s), based on price, quality, and network operator reputation, and informs the winning NAs of acceptance. **8:** NAs confirm to the UTA that the flows are established.

9: At the end of the session, the UTA releases each flow. **10:** NAs inform the SPA of end of session. **11:** NAs and the UTA report commitment fulfilment to the MA. **12:** The MA updates the reputations of the two reporting parties, and sends the new reputations to the LA. **13:** The LA forwards the new list of NAs and reputations to subscribing parties. **14:** The SPA decrypts and sends all bids to the LA. The LA forwards the bids to subscribing parties, to allow them to verify the fairness of the auction. **15:** SPA exits the marketplace.

IV. Achieving Anonymous Network Access

We want to achieve two properties of private communications: unidentifiability and unlinkability[13]. Unidentifiability can be achieved if no other party in the DMP is able to derive a user's identity from a network address. Unlinkability can be achieved if no actor in the DMP can observe any relationship between two subsequent calls made by one user. If these goals are achieved, the Digital Marketplace can be used to enable anonymous network access.

A. Unidentifiability

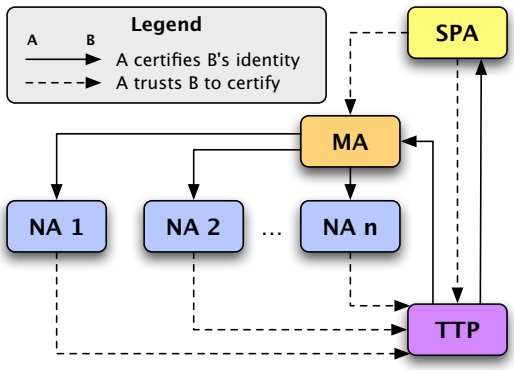

Fig. 3. Certification and trust in the Digital Marketplace

As can be seen from figure 1, the Digital Marketplace does not fundamentally change the traditional relationship between the mobile terminal user and the service provider. The service provider is still the user's representative in the market, knows the identity of the user, and maintains a long-term relationship. Clearly, we cannot provide unidentifiability while this relationship exists.

However, the DMP demands that an agent is present in the marketplace to negotiate for network service. Therefore, we propose modifying the DMP specification to permit user-submitted agents to take the role of the SPA. These User Negotiation Agents (UNAs) would have to comply with the DMP protocols, and be compatible with the DMP Agent Environment, but may otherwise operate however the user desires. One possibility is a standard Open Source UNA, which would allow the user to verify that the agent does not violate its privacy. Making this change also creates other possibilities for the Digital Marketplace, unrelated to privacy concerns: for example, users could modify the negotiation behaviour of their agent to exactly suit their requirements.

We propose modifying the initial Connect message to include an optional parameter: the code of the UNA. Therefore, as indicated in figure 4, the UNA is migrated into the marketplace via the Market Agent. For anonymous users, this removes the need for steps 2 and 3 in the previously-described protocol (see section III-B).

Figure 3 shows that the SPA has its identity certified by a Trusted Third Party in the DMP, but also that it is not in a position of trust. As described in previous research[7], certification is necessary to give network operators a course

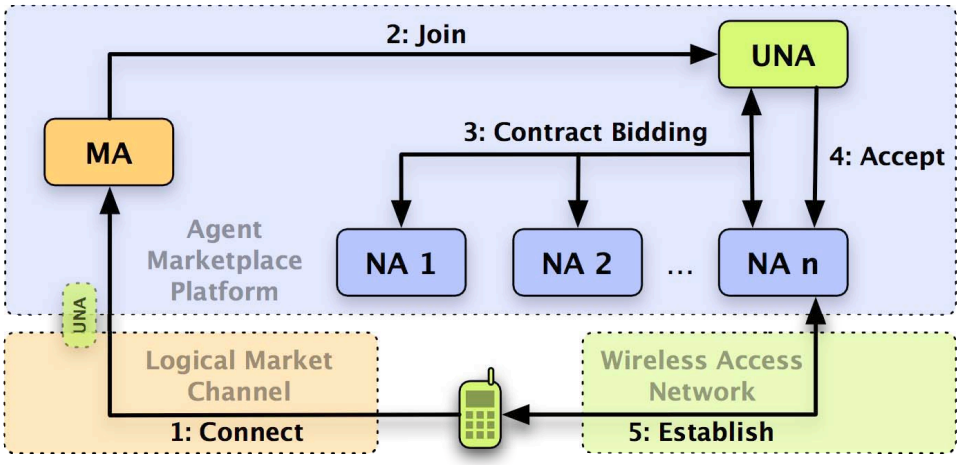

Fig. 4. Integration of UNA into the Digital Marketplace: the UNA is migrated in the Connect message

of action if a service provider fails to pay for network connectivity provided to its users. This facilitates the standard telephony model of "payment in arrears": service is used, and paid for in aggregate at the end of the billing period. However, this is the only reason for certification.

The UNA cannot be certified, as this would enable linking of multiple calls, defeating anonymity. Therefore, to allow a UNA to function in place of an SPA, we require pre-payment. This is an unavoidable consequence of anonymous service usage: with user anonymity, there is nowhere to send a bill, and no practical incentive to pay after the service has been provided. As the Digital Marketplace is an online marketplace, we propose the use of electronic cash[14] as a payment mechanism.

Users will often not be able to specify in advance how much they want to use the network. Therefore, we cannot pay fully in advance, as even after negotiations we do not know what the final charge will be. To solve this problem, we require a scheme which supports micropayments[15], to allow the user to pay in advance for network usage by throughput or time in small units. For example, the market negotiation could lead to a contract of 50 cents per megabyte of data transfer; then, the user would pay 50 cents up-front for the first megabyte, and make another payment if that limit was reached. There are several examples of anonymous micropayment systems in the literature[16][17], some of which are currently available commercially[18].

At first glance, another issue seems to arise from allowing unsigned SPAs to negotiate in the DMP. The SPA's certification is also used to ensure that detected unfair bid selection is punishable, to counter collusion. With an unsigned UNA, this cannot be punished. However, we do not expect this to be a major problem, for two reasons. Firstly, individual users have no motive to select anything but the most competitive bid; therefore, when the unsigned UNA chooses between bids, the selection will be fair. Secondly, we expect that the free market will adapt to ensure that the less trustworthy anonymous transactions incur a premium, due to increased risk on the part of the network operators. Therefore, it would not be a sensible business strategy for a service provider to present an unsigned agent to the marketplace, in order to collude with network operators without punishment. The associated increase in call cost should ensure that this approach would lead to higher costs to the user, and therefore the service provider would become uncompetitive.

B. *Unlinkability*

The modifications proposed in the previous section allow users to gain network access without directly revealing their identities. However, to achieve anonymity, we must also ensure that there are no detectable links between two separate Digital Marketplace interactions. Without such a property, long-term profiling is possible, which can eventually lead to identification.

To achieve unlinkability, we must remove any possible links between sessions. For this paper, we exclude any application-level information disclosure; it is assumed that the user will use higher-layer anonymity schemes as appropriate to counter this problem. In this paper, we only examine in depth the Digital Marketplace protocols. We therefore also assume that the only adversaries are the network operators; both the Market Agent and Logging Agent are verifiably trustable[7], and no other agents have any interaction with the UNA.

A diagrammatic representation of the Digital Marketplace protocol is given in figure 2. From figures 1 and 4 it is clear that the second and third steps of the protocol are elided when using a UNA; the agent code is already present in the agent platform, as part of the Connect message.

Almost all messages sent by the UNA clearly provide no opportunity for profiling, with the exception of bid selection and flow contract proposal. Since the bid selection behaviour is opaque, and the algorithm used may be complex, we assume that it is unfeasible to identify a unique UNA from bid choice alone. Similarly, parameters in the flow contract are likely to be similar for all agents, with random variation depending on network conditions; this again prevents profiling.

However, the mobile agent itself may be different, especially if the user customises its behaviour. The secure agent execu-

tion environment ensures that the agent code is unreadable by the network agents; therefore, the only place that the agent code could be read by the Network Operators is in the connect message. We therefore propose that the connect message should padded to a fixed length, and encrypted so that only the MA may read it. This implies that the UNA must be of a fixed size; restrictions on the agent's operation are necessary to ensure efficient operation of the agent environment, so it is not onerous to constrain its size. The value for the agent's maximum size is an implementation-specific issue.

Finally, one other possibility for linking several sessions exists. We assume that all local wireless networks used by the Digital Marketplace require hardware addresses for clients; for example, the MAC address in 802.11. This is observable by anyone accessing the network, and is normally never changed. It therefore provides a very simple method for tracking users over multiple sessions.

Previous work by Tortonesi and Davoli discussed this problem, and proposed several solutions[19]. They suggest using cryptographic techniques to create dynamic hardware addresses. One proposal requires a loosely-synchronised clock to generate a guaranteed-unique local hardware address. At time of connection to the network, the algorithm encrypts the combination of a local network prefix, the true hardware address, and the current time. The output remains IEEE 802 compliant, and would therefore work with any EUI-48-supporting network interface. Other access protocols would require similar dynamic hardware address techniques to provide unlinkability.

V. Summary and Conclusions

The Digital Marketplace (DMP) is a call management architecture which creates a freely-operating market in network access. We propose to modify the DMP to allow some users to access the network with complete anonymity. These changes have no impact on other users who are content to be identified.

Our proposed changes are described above in section IV, and can be summarised as follows:

1) Allow unsigned User Negotiation Agents (UNA) to migrate from the user's handset
2) Modify the Connect message to include the UNA
3) Require that the UNA portion of the Connect message is padded to a fixed length and encrypted to the MA
4) Pay for service in advance, using anonymous digital cash micropayments
5) Ensure that the user's local wireless network hardware address is dynamically generated each session

Several properties arise from these changes. First, the user no longer requires a long-term relationship with a service provide in order to gain network access. Secondly, there is no requirement for the user to reveal their identity to anyone in order to gain network access. Finally, two separate network access sessions cannot be linked together to build up a profile of any user. Therefore, this modified Digital Marketplace enables a new form of anonymous communication: anonymous network access.

References

[1] Oliver Berthold, Hannes Federrath, and Marit Kohntopp, "Project "Anonymity and Unobservability in the Internet"," in *Workshop on Freedom and Privacy by Design*, Computers, Freedom and Privacy Conference 2000, April 2000.

[2] Paul F. Syverson, David M. Goldschlag, and Michael G. Reed, "Anonymous Connections and Onion Routing," in *Proceedings of the 18th Annual Symposium on Security and Privacy*, pp. 44–54, 4–7 1997.

[3] Roger Dingledine, Nick Mathewson, and Paul Syverson, "Tor: The Second-Generation Onion Router," in *Proceedings of the 13th USENIX Security Symposium*, pp. 303–320, August 2004.

[4] Michael K. Reiter and Aviel D. Rubin, "Crowds: Anonymity for Web Transactions," *ACM Transactions on Information and System Security*, vol. 1, no. 1, pp. 66–92, 1998.

[5] James Irvine, "Adam Smith Goes Mobile: Managing Services Beyond 3G with the Digital Marketplace," *Invited Paper to European Wireless 2002*, February 2002.

[6] Alisdair McDiarmid and James Irvine, "Security Requirements for the Digital Marketplace," *Proceedings of 61st IEEE Vehicular Technology Conference*, May 2005.

[7] Alisdair McDiarmid and James Irvine, "Securing the Digital Marketplace," *Proceedings of 62nd IEEE Vehicular Technology Conference*, September 2005.

[8] David Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–88, 1981.

[9] David Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," *Journal of Cryptology*, vol. 1, no. 1, pp. 65–75, 1988.

[10] B. Goldacre, "How I stalked my girlfriend," *The Guardian*, February 2006.

[11] J. Krim, "Online Data Gets Personal: Cell Phone Records for Sale," *Washington Post*, July 2005.

[12] Gwenaël Le Bodic, Demessie Girma, James Irvine, and John Dunlop, "Dynamic 3G Network Selection for Increasing the Competition in the Mobile Communications Market," in *Proceedings of 52nd Vehicular Technology Conference*, pp. 1064–1071, September 2000.

[13] Andreas Pfitzmann and Marit Kohntopp, "Anonymity, Unobvservability and Pseudonymity — A Proposal for Terminology," in *Designing Privacy Enhancing Technologies: Proceedings of the International Workshop on the Design Issues in Anonymity and Observability*, pp. 1–9, July 2000.

[14] David Chaum, Amos Fiat, and Moni Naor, "Untraceable Electronic Cash," in *CRYPTO '88: Proceedings on Advances in Cryptology*, pp. 319–327, 1990.

[15] Ron Rivest and Adi Shamir, "PayWord and MicroMint – Two Simple Micropayment Schemes," *CryptoBytes*, vol. 2, no. 1, 1996.

[16] Robert Tracz and Konrad Wrona, "Fair electronic cash withdrawal and change return for wireless networks," in *WMC '01: Proceedings of the 1st International Workshop on Mobile Commerce*, pp. 14–19, 2001.

[17] Yang Zongkai, Lang Weimin, and Tan Yunmeng, "A new fair micropayment system based on hash chain," in *EEE '04: Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service*, pp. 139–145, 2004.

[18] Daniel Nagy, "On digital cash-like payment systems," in *Proceedings of the International Conference on e-Business and Telecommunications 2006*, August 2006.

[19] Mauro Tortonesi and Renzo Davoli, "User untraceability in the next-generation Internet: a proposal," in *Proceedings of Communication and Computer Networks*, November 2002.