A New Approach for Privacy-Preserving Communication by Combining Virtual Identities with Mobility Management

Christian Hauser

Institute of Communication Networks and Computer Engineering

University of Stuttgart, Germany

hauser@ind.uni-stuttgart.de

Future mobile systems tend to become open systems with many different providers for services as well as for content. Moreover, location-based services are often predicted to become so-called killer-applications for future mobile communication systems. Current research projects, e.g. [1], even aim at publicly providing spatial information which enhance the expressiveness of location information. Thus, the danger for privacy increases. Regarding this scenario, it is obvious that protection of users' privacy is of great importance for the acceptance of such systems and that today's trust model of mobile systems (GSM) will no longer be applicable.

It will become necessary, that users can appear under several virtual identities (VID). A VID is the "view" of a system or service on a particular user, i.e. a pseudonym as identifier possibly augmented with additional information, e.g. credentials for a payment system. By using several VIDs the user will be able to tune his level of anonymity and may separate his data trace into several contexts, that can be known to others. In order to insure this separation of contexts, it is of great importance to prohibit linking of different VIDs of one user, which could be derived from unique or even identifiable application data as well as by data of communication systems. It is, e.g., possible for attackers to link two VIDs if they use the same IP-address at the same time. Thus, it is necessary to hide the IP addresses of communication peers. In the remainder of this article a system for that will be outlined.

Regarding communication of a client to a server, several systems exist to hide the client's (i.e. the sender's) IP address, mostly focusing on WWW browsing, e.g. [2], [3]. Nevertheless, these systems do not provide anonymity of the recipient (regarding the server as recipient of the client's request). So if a service, e.g. a notification service of stock news, is contacting a VID it will see the IP address of the VID's device. Although there are systems which principally can provide anonymity of the recipient, e.g. anonymity of a Web server that receives http-requests [4], there is no system known to the author, that is designed for anonymity of the recipient and that can be used in systems sketched above, in which VIDs have to be protected. Therefore, we have designed a system for communication setup in both directions - client initiated and server initiated - that hides the IP addresses of both participants. It is possible to contact (virtual) identities by their fixed pseudonym and it is possible for the instances to change their IP addresses for flexibility purposes. The communication partner does not even see the subnet of the VID's IP address which would already shrink the anonymity group and therefore could lead - together with other information known about the VIDs - to the linking of VIDs.

A changing IP address and a fixed identifier (here: the pseudonym) for communication setup are the typical elements for a mobility management framework, like Mobile IP. Therefore, our idea was to combine the anonymity management with the mobility management, which can principally be achieved by two approaches. The first approach is to modify the mobility management and, e.g., to augment Mobile IP regarding anonymity properties. The second approach is to start with anonymity management and augment it with mobility properties. The latter one is the way we chose because of easier implementation of a prototype serving our needs of message exchange. Nevertheless, there are no obvious reasons that would prevent the implementation of our approach on the IP layer, thereby supporting more applications.

For concealing the IP addresses, there must principally be a proxy in the communication path between the peers. As an easy solution with a single proxy-system of one provider is not feasible because of too much knowledge of this proxy-system, it is necessary to have many proxies of different providers. The pseudonyms of one user are distributed on different proxies. Regarding mobility management, this would in a first approach increase the number of parties, knowing the client's current IP addresses and would be a contradiction to the principle of data avoidance and data economy. Therefore, a client's IP address may only be known by the proxies if it is in fact needed, i.e. in case of communication. This is achieved by splitting up the IP address in several shares, which are stored on several proxies. In case of a communication request, these shares must be combined by one proxy to compute the IP address. In order for proxies not to know the IP address forever when they have combined it once, the address must change in certain time intervals. In our Scenario, this is given by mobility of the client.

As many different proxy providers are necessary, attacks of proxies must be considered. An attack of a proxy could be to pretend communication to the client for a long period of time. Thus, it would know the client's IP address during this whole period. That attack is defeated by using a credit system for combining the shares. If a proxy's credits are consumed, it will no longer get the shares from the other shareholders and it is another proxy's turn to provide communication to this client. Thereby, it is possible to define a maximum trace of IP addresses known to a single proxy.

In means of application of our system, the IP addresses are completely concealed to the communication peers. Additionally the trace of IP addresses known by a mobility management unit (here: a proxy) is limited, which is an advantage considering Mobile IP, in which the trustworthy Home Agent always knows the IP address of the client. The system designed to limit a proxy's knowledge was principally shown to be deadlock-free by modelling it as a petri net and subsequent analysis. We implemented a prototype for proof of concept and showed the principal functionality of our system. Future work will be focused on availability as well as evaluation of an IP layer solution.

[1] "NEXUS - an open platform for spatially aware applications": http://www.nexus.uni-stuttgart.de.

[2] Syverson, P., Goldschlag, D., Reed, M.: "Anonymous Connections and Onion Routing", in Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, IEEE CS Press, May 1997, pp. 44-54.

[3] "JAP - Anonymity & Privacy": http://anon.inf.tu-dresden.de.

[4] Goldberg, I., Wagner, D.: "TAZ Servers and the Rewebber Network: Enabling Anonymous Publishing on the World Wide Web", First Monday, Vol. 3, No. 4, April 1998.

Universität Stuttgart

Institut für
Nachrichtenvermittlung
und Datenverarbeitung

A New Approach for Privacy-Preserving Communication by Combining Virtual Identities with Mobility Management

Background

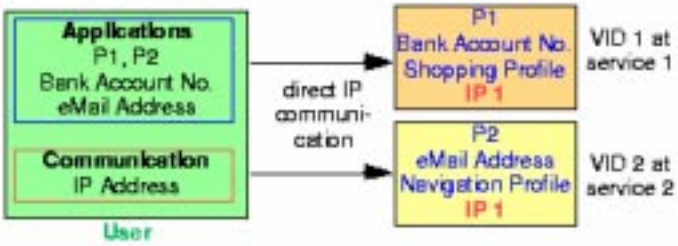
Future of mobile comm.: Increased threat to privacy

- Open systems
- Disclosure of position to location-based services
- Publicly available spatial information ➡ context for location
- Disclosure of other context-data

Virtual Identities (VID)

- **Separation of data trace into unlinkable contexts**
- **Virtual identity (VID) is a "view" on the user**
- **Tunable level of anonymity**
- **Threat: link between different VIDs ➡ augmented VID**
  - unique, identifying data of application
  - unique, identifying data of communication system

VID Scenario

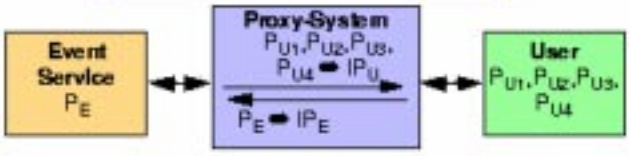


- **Concealing of IP address necessary**
- **Client initiated communication**
  - several systems proposed (JAP, Onion Routing, Crowds, ...)
  - mainly for web browsing
- **Server initiated communication**
  - examples: event notification, stock information
  - server has to address client
- **Requirements**
  - bidirectional initialization of communication
  - addressing via fixed pseudonym
  - changing IP address (flexibility)
  - ➥ Similarity to mobility management framework (e.g. Mobile IP)

➥ **Idea: Combining mobility management with anonymity management**

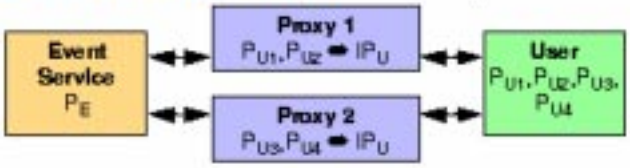
- **Approaches**
  - augmenting anonymity management with mobility support
  - augmenting mobility management with anonymity properties

Architecture



- **One single proxy system of one provider**
  - all pseudonyms (VIDs) of a user linkable
  - knowledge of all communication relations
  - complete profile of IP addresses

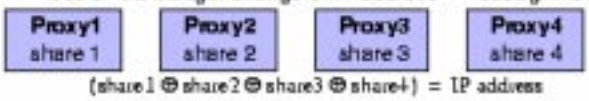
➥ **Distribution of knowledge on several providers**



- **Several proxies of different providers**
  - retrieval of proxy in charge via Name Service (e.g. DNS)
  - some pseudonyms (VIDs) of a user linkable
  - knowledge of communication relations of some pseudonyms
- **But: IP address profile known to many parties!**
  ➡ contradiction to paradigm of data minimization

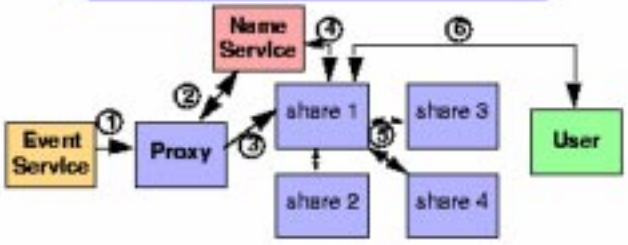
➥ **Revelation of IP address only when necessary (only in case of communication)**

- secret sharing
- loss of knowledge: change of IP address ➡ reassignment



(share1 ⊕ share2 ⊕ share3 ⊕ share4) = IP address

Complete Comm. Procedure



1. **Sender chooses arbitrarily any proxy (concealing sender's IP address)**
2. **Proxy queries for proxies of recipient pseudonym**
3. **Proxy contacts one of these proxies**
4. **Proxy queries for other shareholders**
5. **Proxy collects shares and combines IP address**
6. **Proxy delivers message**

Universität Stuttgart

Institut für
Nachrichtenvermittlung
und Datenverarbeitung

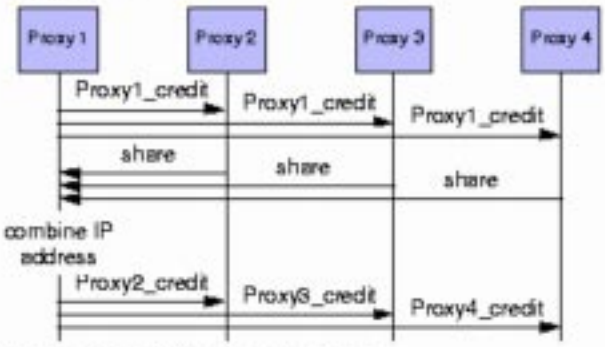
A New Approach for Privacy-Preserving Communication by Combining Virtual Identities with Mobility Management

Attack by Proxy

- **Open proxy system ➥ many providers**
- **No trust in proxies ➥ consider attacks by proxies**

  attack: continuous communication over long period of time (large profile of IP addresses)

  ➥ limited serving time of a single proxy
- **Credit system**
  - proxies have credit at other shareholders
  - IP address can be combined as long as credit available
  - after combination, credit is given to other shareholders
  - no credit left ➥ another proxy's turn
  - system modelled as petri net and analytically proven as being deadlock-free



- **Proxies do not trust each other**

  different providers

  ➥ compliance to credit system must be checked by other shareholders

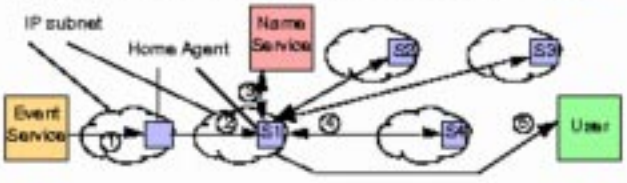
Alternative Approach

Augmenting mobility management with anonymity properties

- **Home Addresses resemble pseudonyms from application-layer approach**
- **All addresses from home network**
  - pseudonyms (=addresses) from small anonymity group
  - together with some application data link of VIDs can become possible
- **Several Home Addr. from different subnetworks**

➥ **Several Home Agents (resemble Proxies from 1st approach)**

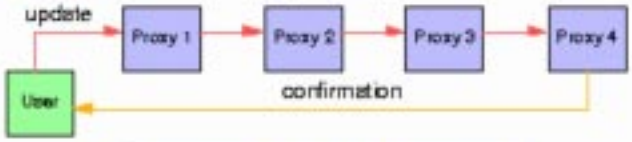
- **Huge amount of IP addresses necessary ➥ IPv6**



Update of IP Address

- **Simultaneous update of several pseudonyms on same proxy ➥ VIDs linkable**
- **Only one share of IP address has to be updated**
- **Update only one pseudonym per proxy**
  - not possible if too few proxies
  - artificial delay of some updates necessary

  ➥ update chain sent from proxy to proxy



Summary

- **Mobile communication without disclosing IP address of neither sender nor recipient**
- **Prevention of linking different VIDs by simultaneous use of same IP address**
  - at communication peers
  - at proxies (dependent on scenario)
- **No complete trace of IP addr. known by any instance**
- **Prototype for exchange of messages (e.g. notifications)**
- **Use for other variable private data possible (e.g. proxies as location service)**

Future Work

- **Availability**

  e.g. (m,n) threshold schemes

  ➥ petri net and analysis much more complicated
- **IP layer solution**
  - evaluation of architecture
  - implementation of prototype

  ➥ support of more applications
- **Credit system robustness against misbehaving proxies**
  - credit signed by issuer
  - nonce in credit against replay
  - centralized reputation register for misbehaving proxies
- **Change algorithm of proxy**
- **Performance evaluation**
- **Evaluation of linking probability**

  ➥ Mobility-triggered change of IP addresses sufficient?
- **Scenarios: How many proxies? How many VIDs? How much communication?**
- **MIX concepts**
- **Adaptation to ad-hoc scenario**

  proxies can leave and transfer knowledge to another node