Organized Anonymous Agents*

Martijn Warnier Frances Brazier

VU University, Amsterdam

Abstract

Anonymity can be of great importance in distributed agent applications such as e-commerce & auctions. This paper proposes and analyzes a new approach for organized anonymity of agents based on the use of pseudonyms. A novel naming scheme is presented that can be used by agent platforms to provide automatic anonymity for *all* agents on its platform, or, alternatively, to provide anonymity *on demand*. The paper also introduces a new technique, based on the use of handles, that can be fully integrated in an agent platform. Performance measures for an anonymity service implemented for the AgentScape platform provides some insight in the overhead involved.

This paper proposes a new approach to anonymous agent-to-agent communication that guarantees anonymity, (1) if required, for all agents running on a platform without any additional effort by agent application developers, or (2) on demand. The one main assumption is that agents trust the middleware on which they run –the agent platform. The link between an agent and its owner does not have to be anonymous: the middleware is trusted and can thus be trusted to keep this information confidential.

Anonymity in the real world is not an absolute notion, communication can be anonymous to one person or organisation, and not to another. Similarly, agents can communicate anonymously to other agents, or groups of agents, but not, for example, to the agent platform on which they run. Several degrees of anonymity can be distinguished ranging from absolute anonymity to total non-repudiation this paper focuses on *organized pseudonym-based semi-anonymity*. Semi-anonymity is organized: when and where anonymity is provided is well-defined. The naming scheme this paper introduces ensures that each agent's true identity and its pseudonyms are unique and cannot be linked to each other by any outside party. Classical anonymity in Computer Systems focuses on anonymity of the underlying communication layer, focusing on sender, receiver and link anonymity (unlinkability) respectively. The first two, sender and receiver anonymity, require that the location of the sender and receiver, respectively, are hidden from the other communicating party. Link anonymity, also known as unlinkability, ensures that the link between the communicating parties remains anonymous to all third parties: it is impossible for any outside party to observe if two parties are communicating with each other. (Note that the communicating parties themselves are often aware of each others (true) identity.) In practice these forms of anonymity can be combined.

This general notion of anonymity in Computer Science can be applied to agent technology. The focus in this paper is on anonymity of communication between individual agents. As stated earlier the relation between agent owner and agent is assumed to be confidential, and guaranteed by the agent platform. Full communication anonymity, i.e., receiver, sender and link anonymity taken together, can only be established when an agent cannot be linked to a legal entity via its communication with other agents. A platform based solution that enables the middleware to (automatically) provide link anonymity and location anonymity for each individual agent is the main focus of this paper. Pseudonyms are introduced for this purpose.

The use of a pseudonym, however, on its own does not suffice. If outsiders can observe agent communication, these observations can be used to obtain/deduct (unwanted) information about an agent. If an agent uses the same pseudonym to communicate with several other agents, together they can infer that they have been talking to the same party which breaks anonymity. An agent platform identifies an agent by its *globally unique identifier*(GUID). This GUID corresponds uniquely to the identity of the agent. The following example illustrates how the use of a single pseudonym for all communication does not suffice in multi-party negotiation situations:

*The full version [1] of this paper appeared in Proceedings of the Third International Symposium on Information Assurance and Security (IAS'07).

Example 1
There are three agents A, B and C, each with their own pseudonym P_A, P_B and P_C respectively. Agent A is interested in a service that both agent B or C can provide. Agent A first uses its pseudonym P_A to ask agent B about the price of its service, then agent A uses the same pseudonym P_A to ask agent C about the price of its services. Although agent B and agent C do not know A's real identity, together they can still determine that the same agent *has been asking price information of the services they provide. Thus agent A has not been communicating anonymously.*

Example 1 above clearly demonstrates the need for agents to use more than one pseudonym to obtain (link) anonymity – one pseudonym for each individual communication event (or communication session). For similar reasons, agents should also use a different pseudonym each time they communicate with the same party at some later point in time. The example also illustrates that privacy protection against buyer profiling cannot be obtained by solely using *one* pseudonym. As the same pseudonym can be linked to multiple events over a longer period of time, a buyer profile can be constructed, and privacy cannot be guaranteed. Even if the 'real' identity of the agent owner is not known!

In our approach each agent has one globally unique identifier and multiple unique pseudonyms (called *handles*). The agent platform is responsible for ensuring that all GUID's and pseudonyms are unique, that GUID's are hidden from other agents, that pseudonyms cannot be linked to each other and that pseudonyms cannot be linked to the agent they represent. This naming scheme is implemented using handles. Each agent is assumed to have a global unique identifier (GUID) known only to the agent platform. Such a GUID can, for example, be implemented by a Universally Unique Identifier (UUID, ISO 11578:1996). Furthermore, each agent can acquire as many (globally unique) handles as it requires. These handles serve as pseudonyms and are used for communication purposes.

As handles have no intrinsic meaning and do not leak any information about an agent or its owner, agents can safely use handles as pseudonyms. Link anonymity is acquired if agents use a new handle for each individual communication event. The agent platform is responsible for creation of agent GUID's and handles and the binding between the two. The binding between handles and GUID's can be acquired using a cryptographic hash function (sha): handle$_n$ = sha(GUID + n) with $n \in \mathbb{N}^+$

This approach has two specific advantages: (i) if the GUID is not known then handles cannot be linked to each other or one specific GUID and (ii) if the GUID is known then the platform cannot deny that a specific handle belongs to a specific GUID.

An agent platform given an agent's handle, must be able to retrieve its GUID. A private lookup service provides this functionality. This service must be private to the middleware. Note, that an agent platform can always check the integrity of its own lookup service should it doubt the information it acquires. An agent platforms can always reconstruct an agent's handles given its GUID as described above and compare it to the handle it has been provided. As handles (or human readable names that are uniquely mapped to these handles) are used for all communication between agents, no information about the location of a particular agent is revealed to any other agent. Hence this technique also provides location anonymity and thus also sender and receiver anonymity. Whenever two agents communicate they do not have to share information on the location (host) on which they reside.

The proposed technique for acquiring anonymity, based on handles, can be completely integrated into agent platform middleware as a separate middleware service, (as described for AgentScape in [1]. The maximum performance penalty for this service is a factor of two overhead for agent communication.

References

[1] M. Warnier and F. M. T. Brazier. Organized anonymous agents. In *the Proceedings of The Third International Symposium on Information Assurance and Security (IAS'07)*. IEEE, 2007.