Perspectives on Electronic Commerce with Mobile Agents

Christoph Busch, Volker Roth, and Ralph Meister

Fraunhofer Institut für Graphische Datenverarbeitung
Rundeturmstraße 6, 64283 Darmstadt
`{busch|vroth}igd.fhg.de`

Abstract. Electronic commerce is a driving force for IT. Mobile agents provit from this development, and offer substantial advantages for certain electronic commerce applications in return. Yet, a number of criteria should be applied to electronic commerce applications to assess which areas are best suited for mobile agents. A major requirement to build confidence in mobile agent technology is the availability of adequate security mechanisms. Although much remains to be done in this area, a valuable set of mechanisms exist that are suited to launch electronic commerce applications based on mobile agent technology.

Keywords: mobile agents, electronic commerce, security, malicious host.

1 Introduction

Mobile software agents (see e. g. [4]) are programs bundled with data and execution state that can suspend execution, migrate to other computers connected over a network, and resume execution there. Although numerous other definitions of mobile agents exist, we deliberately chose this definition to put an emphasis on the way most mobile agent systems are actually implemented. Mobility of programs bundled with data and state information requires special support that is generally provided by a special program providing a *runtime environment* for mobile agents.

A feature being frequently attributed to mobile agents is *autonomy*, the ability to perform certain tasks without guidance or intervention by a human user. A mobile agent that is able to achieve a given goal autonomously demonstrates two key principles peculiar to mobile agent technology:

1. **The delegation principle.** Instead of using computers as highly interactive tools requiring constant attention, autonomous mobile agents strive to achieve a given goal without permanent observation by its owner. As a matter of consequence, the user is free to take care of other tasks, saving time in the process.

2. **The Off–line processing principle.** Users may dispatch autonomous mobile agents over a temporary network connection to a target network. After dispatching, the temporary network link may be brought down until a later point in time, when the agent is ready to return and to present the results of its endeavours.

In particular, the off–line processing principle offers striking advantages for today's Internet computing. Although major companies, organisations and universities are often connected to the Internet directly and permanently, the growing number of private *netizens* are connected to *Internet service providers* (ISPs) primarily through dial–up lines. Those lines are mostly charged according to time slices, and prices are often prohibitive. Mobile agents may perform extensive searches while their home base is disconnected from the network, obliterating the need to maintain the network connection throughout the duration of the search process.

This feature is also attractive for mobile platforms that do not maintain permanent network connection such as PDAs, and laptops connected through cellular phones. However, considerable bandwidth may be saved also if a permanent network connection is available. Mobile agents allow to shift the computation process to the source of the data. Hence, extraction of information from huge amounts of data does not require transporting the source data over the network link. Since, searches and filtering may be done on the much faster local bus, the overall search time may be reduced. This is advantageous not only for the searching party, but also for the party that provides access to the data.

Further advantages of the off–line principle in conjunction with autonomous behavior is accurate control of distant machinery if the elapsed time for a signal travelling to and from the control process of remote machinery is too long for real–time interaction. This may apply for instance to satellites. Agents may migrate to satellites checking the status and applying software updates as well as correction procedures.

One of the most promising application areas for mobile agents is emerging down on earth, though. For years, *electronic commerce* is seen by experts as one of the major driving forces for information technology. Currently, forecasts predict Internet electronic commerce a strong increase in turnover. Various research institutes predict a world wide e–commerce market of 100 billion US$ [8] in year 2000, and from 400 billion US$ [12] to 500 billion US$ [10] in year 2002. At the same time, user expectations are changing. Users now demand Web sites with a focus on fast page downloading times, as well as a clear, concise and shallow structure. Flashy Web sites are not an issue any more, signalling that the

time for playing games is over – get down to business. Mobile agents can step in and provide significant improvements to cope with the challenges of Internet e–commerce such as information overload and a lack of structure in the net. However, not all areas of e–commerce may equally profit from the advantages of mobile agent systems. Section 2 will shed some light on which areas are best suited for mobile agents.

Even though the advantages of mobile agent technology are quite straightforward, a major prerequisite, before the agent paradigm will be widely used in e-commerce applications, is that customers as well as providers trust the system. The degree of trust a user puts into a system depends on two factors. Firstly, trust is based on positive experience with the technology. Considering mobile agents, limiting a user's interaction with his agent to specifying the distinct task is generally not sufficient. The feedback of the autonomous action must also be communicated to the user transparently in a way that enables him to verify that the outcome of the delegation matches his expectations. Secondly, trust is based on the fact that adequate security can be assured for applications built on mobile agents. This topic is covered in Sec. 3. Conclusions are given in Sec. 4.

2   Electronic Commerce and Mobile Agents

Traditionally strong sectors in electronic commerce such as trading in CDs and books, are also among the interesting application areas for mobile agents. However, in highly dynamic environments such as electronic markets, statements about suitability and potential of applications are difficult to make. Thus, we present not only an evaluation of e–commerce areas but also propose general criteria for evaluation. These criteria enable future assessment of emerging or changing application areas. The criteria are divided into requirements to be met by agents, by payment systems to be used in conjunction with agent technology, as well as potentials of the areas. Both, requirements and potentials, will be discussed below.

Requirements may be divided into those that agent systems need to fulfil in order to support a desired application area, and requirements that payment schemes have to meet in order to be useful in the application's context. On top of this, payment schemes must be suitable to be deployed in conjunction with mobile agent technology. In some cases it might even be desirable to delegate payment authorisation to a mobile agent which rises a number of security concerns that need to be met (see also Sec. 3).

The requirements to be fulfilled by agent systems comprise *decision capability, negotiation capability, fault tolerance* and *risk limitation* [5]. Possible decision

3

capabilities range from simple comparisons of quantitative attributes such as price or weight, up to the evaluation of complex structures such as services or attributes depending on individual preferences, for instance style and fashion. Correlated also to the provided level of intelligence are the requirements concerning negotiation capabilities. A variation of the acceptable price over time is simple. The assessment of a contract specifying complex volume discounts is demanding. Finally, except from technical capabilities the evaluation also needs to include the potential risks of a wrong decision or behavior by an mobile agent. The risks comprise losses in terms of money or privacy also indirectly, for instance production delays because of procurement problems.

Increase in timely and financial efficiency of electronic markets are supported by using electronic payment systems in an online transaction. Each application area defines a certain profile of requirements concerning the necessary payments. The evaluation criteria examine the flow of information, goods and money. Regarding the flow of information, in particular privacy and frequency of business contacts between customer, merchant, and bank are relevant. Concerning the flow of goods, the transfer of a good has to be strongly linked to a financial transaction. If we look at the flow of money, firstly a classification of the payment size is essential, and secondly the division of credit risk has to be examined. The classification of the payment size is not consistent in literature, though. We chose a division into two main categories with subcategories on a logarithmic base:

1. Micropayments having value up to 1 US$
2. Macropayments starting from 1 US$ and up.

Macropayments are subdivided further into:

	value range
Minipayments	1 – 10
Low–value payments	10 – 100
High–value payments	100 – ∞

(amounts in US$)

The requirements to payment and contracting are not particular for mobile agents. Yet, meeting these requirements is often difficult for mobile agent systems, and demands a close examination of suitable digital payment systems and their features. If the payment cannot be conducted electronically, much of the advantages in efficiency cannot be realized in electronic commerce. Thus, integrating digital payment systems, which meet the requirements, is an important factor for the success of mobile agents in most e–commerce segments.

The advantages of mobile agents do not apply in all kinds of application areas, though. Given a widely deployed mobile agent infrastructure, Mobile agents may contribe in three ways:

Optimizing decisions As [15] and [2] argue, electronic markets show increasing market transparency resulting in superior resource allocation. However, the ideal of increased market transparency cannot be realised at low cost in an interactive electronic marketplace such as online shops on the WWW. Mobile agents provide economical and fitting technical means for autonomous, fast and exhaustive information research. Thus, mobile agents can lead to almost optimised decisions for the allocation of goods.

Providing mobility, flexibility and autonomy Tasks in an electronic commerce environment are often repetitive and sometimes time critical, for instance monitoring of stock prices. Mobility of agents minimizes communication delays. Flexibility of agents by cloning itself enables almost unlimited scalability regarding the amount of input. The advantages of this autonomous flexibility holds for customers as well as merchants (see also [5]).

Increasing market efficiency for all parties To conclude mobile agents can increase efficiency by saving time, for instance online–time, and costs, for instance profit margins of intermediaries. These potential savings together with increased convenience are the added value of mobile agents in an electronic commerce scenario.

Apart from the technical potential of mobile agents, the economic potential of an application area in electronic commerce is also a key criterion in evaluating the chances of the use of mobile agents. Assessing the economic potential of an application area in electronic commerce consist of two parts:

1. The current and future market size in terms of turnover or number of customers has to be estimated.
2. The return on investment has to be evaluated as the ratio between necessary investments in fixed and variable cost, for instance the costs of the agent infrastructure, and the possible revenue according to estimates made in the previous item.

A far more detailed discussion of the applicable criteria as well as the complete analysis of application areas according to the criteria can be found in [16]. Below, we present a summary derived from the detailed analysis. Table 1 shows an excerpt of the application areas that were reviewed. The table's cells show,

	Physical goods				Digital goods					Rights	
	SG	**CG**	**SP**	B2B	N	**DG**	OM	ET	E	AR	PC
Requirements for agents											
Decision capabilities	++	+o	o-	o	+	-	o	o	o	+	o
Negotiation capabilities	+o	+	o	-	+	+-	o	o	o	-	-
Risk of wrong decisions	+	++	o	–	+	+-	o-	o	o-	o	-
Requirements for payment											
Flow of information	-	o-	+o	++	-	-	o	o	o	o	o
Flow of goods	o	-	o	o	+	+	o	+	+	+	+
Flow of monetary value	o	o-	+o	-	-	+	o	o	o	o-	-
Potential enabled by agents											
Optimisation of decisions	++	o	+	+	++	++	o	+	o	+	+
Flexibility and autonomy	+	++	++	++	o	+	++	+	+	+	+
Efficiency (time, cost)	+	+	+	+	++	++	+	o	o	+o	+o
Economic potential											
Market size	++	+o	++	++	+	+	-	+	-	-	- -
Return on investment	+o	+o	+o	o	-	+	-	-	+	o	-

Table 1. Score of application areas: SG – Standardized Goods, CG – Convenience goods, SP – Goods with major service part, B2B – Business–to–business supply, N – News, DG – Digital goods, OM – Order monitoring, ET – Education and training E – Entertainment, AR – Access rights, PC – Environmental pollution certificates.

whether a particular criterion was assessed positive (+), negative (-) or indifferent (o) for the identification of a potential application of mobile agent technology. Columns typeset in bold (SG, CG, SP and DG) qualified for further examination to be found in [16].

Among the physical goods for instance the standardized products and services received a high score. The category of trading physical goods comprises all application areas, where information retrieval and decision as well as the transaction phase are conducted electronically and only the good is delivered physically. As the historically largest electronic market segment, it includes standardized goods (books, CDs, electronics, classic MOTO-goods, etc.), convenience goods (groceries etc. bought daily from supermarkets), goods with major service part (travel arrangements, shares, tickets), as well as business to business (office supply, raw materials, etc.).
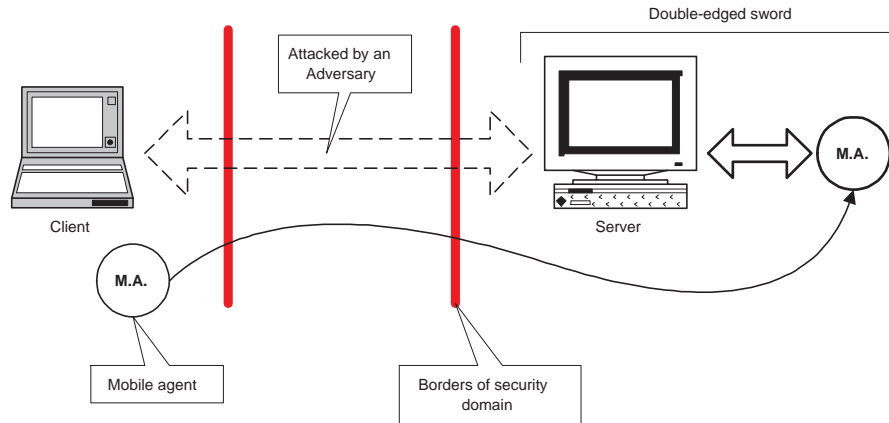
Fig. 1. Security implications of agent migration.

3 Security Considerations

With regard to computer security, mobile agent systems differ considerably from ordinary client server systems. Typical client/server systems such as the World Wide Web assume that two processes communicate, running in separate security domains controlled by the respective operators of the machines on which the processes run. In theory, neither process may threaten the other one unless the perimeter protection of one of the hosts fails. Of course, in practice, computer systems are threatened as a consequence of programming errors, misconfiguration, bad administration, attacks from legitimate users as well as dozens of further sources of attacks. However, in principle, a client/server system may be protected by controlling the borders of its security domain, enforcing access control using *reference monitors*, as well as applying well–understood cryptographic techniques for protecting the communication between hosts. Unfortunately, the same principles do not apply to mobile agent systems. The general assumptions about client/server security do not hold [6]. As a consequence, mobile agent systems include all security issues that arise in traditional systems in addition to new ones introduced by the mobile code paradigm.

Figure 1 illustrates a single migration of a mobile agent. As can be seen, the agent crosses the borders of both hosts' security domains. Agents compare to viruses – differences basically arise in the *intentions* of their senders. This leads to another issue of greates importance. While requests, received from authenticated sources can in general be safely attributed to the identified sender, upon arrival agents might already have been on a number of unknown and potentially

untrusted hosts. One of these hosts might have tampered with the agent in a way that makes the agent attack its most recent host [3].

Hence, it is not generally safe to attribute all actions of a mobile agent to its claimed sender. The security issue with greatest impact was already mentioned implicitely. Malicious hosts may attack agents in various ways, ranging from misbehaved routing of agents to stealing information, to abusing agents as (innocent) mediators of attacks on competitors or other targets.

In general the threats to mobile agent systems are classified into threats imposed by *malicious agents* and threats imposed by *malicious hosts*. Protecting hosts against malicious agents involves use of reference monitors, sandboxes and safe programming languages (see for instance [7, 24, 1]). Proof–carrying code is also discussed as an alternative [17]. Protecting agents against malicious hosts is generally deemed even more challenging. However, we agree for instance with Karjoth *et al.* in that both kinds of threats must be coped with for mobile agent systems to be acceptable [14]. Major security issues regarding the protection of agents against malicious hosts are:

1. The integrity protection of the agent, in particular the agent's mutable part. Agents might be abused as innocent carriers of illegal or offensive materials such as *warez* (pirated software). Hosts may also try to delete, replace, or invalidate committments to the agent, such as terms negotiated in electronic commerce applications. This would enable the host repudiate said terms later. Furthermore, hosts might remove or manipulate offers of competitors already visited by the agent.
2. Maintaining the secrecy of the agent's computations and data, which is a fundamental requirement for fair negotiations as well as for computations on confidential information such as the preferences (or *profile*) of the agent's owner, or secret keys.
3. Protecting the integrity of the agent's control flow which is a precondition for any agent to trust its own decisions. Otherwise, malicious hosts might make agents believe that an offer is acceptable when it is actually not.

Notable advances were made with regard to items 1 and 2. Karjoth *et al.* [13] introduced the notion of *strong forward integrity* and proposed protocols for protecting the computation results of free–roaming agents. Their work is an extension of *partial result authentication codes* introduced by Yee [25]. Roth and Jalali proposed an agent structure that supports access control and authentication of mobile agents [20]. Agent authentication and state appraisal is covered by Berkovits *et al.* [3]. Sander and Tschudin [21] introduced the notion of *mo-*

8

bile cryptography and devised first solutions for computing on encrypted functions using homomorphic encryption schemes. Regarding item 3, Vigna [22] proposed *cryptographic traces* to create verifiable execution traces of agents. Vigna also discusses a number of drawbacks with his approach such as limitation to single–threaded agents, extensive computational and memory overhead, as well as limitation to a–posterior detection. Still, no general solution is known for items 2 and 3. Roth [19] proposes to exploit open networks as a basis for protocols suitable to protect agent–based applications. The key issue is distribution of responsibilities and secret splitting of data between mutually co–operating agents. He also proposes protocols to securely record the actual itinerary taken by a mobile agent, as well as a protocol to adapt electronic cash for use with co–operating mobile agents.

The use of electronic money in conjunction with mobile agents is particularly challenging. Malicious hosts might simply offer the mobile agent a good deal; on reception of the digital money string they roll back the agent to the state in which it was upon reception. Mechanisms for securing agents against such attacks must protect the digital representation of the money as well as assure that negotiations are fair and hosts may not undo valid offers.

Apart from protecting specific areas of mobile agent security, a number of general security requirements can be identified. Firstly, agents must be clearly separated from each other within an agent server. Yet, there must be means to allow agents to authenticate themselves and to interact in a safe manner. A proper agent server architecture presumably will manage multiple security levels depending on the trust the server puts into the sender of an authenticated agent. We anticipate that black lists and role–based access control will be applied to manage rights within the agent server. Secondly, due to the political dimension of the use of strong cryptography, agents will require means to negotiate ciphers and parameters with hosting environments, to assure true interoperability and transparency.

4   Conclusions

The presented evaluation of possible application areas for mobile agents in electronic commerce provides both general criteria for assessment and suitable potential application areas. Concerning the criteria, the economic potential and the potential enabled by mobile agents proved to be decisive. The discussion of the effects of mobile agents in electronic commerce clearly showed the agents' value addition. This additional value meets exactly the need of current netizens,

who constantly complain about lacking speed or bandwidth, as well as information overload as their major problems in electronic shopping (see [11]). Mobile agents lower the bandwidth need and relief the consumer from time consuming and difficult search for relevant information. Thus mobile agents could be a leap in the development of the emerging electronic commerce.

This particularly holds for less favored regions, which are not connected through wired high–bandwidth links. Those areas may exploit global satellite coverage for interconnecting to the global electronic market, which reduces the burden of initial investments required for bringing the region's telecommunication infrastructure up to standards.

Concerning digital payment systems, the integration of the payment transaction into electronic market environments is important to realize the potential of, especially agent–based, electronic markets. In general, a variety of reliable and proven payment systems exist already for interactive transactions. For the use with mobile agents in the identified application areas, cash–like token–based systems seem appropriate. Firstly, handling of token–based money is easier for agents than securing confidential authorization mechanisms such as notational payment systems. Secondly, cash–like systems provide anonymity more easily. Anonymity is getting more and more important for users, particularly in application areas with loose and changing business contact, such as standardized goods. A classic token–based digital payment system providing security and anonymity is *ecash* from DigiCash. Ecash has proven its reliability and usability in a number pilot projects, for instance the one of *Deutsche Bank AG* in Germany.

Although much remains to be done in the area of mobile agent systems, a rich toolset exists that can be applied to electronic commerce applications based on mobile agents. However, the majority of available agent systems do not account for threats imposed by malicious hosts. At most, signing of complete agents, or protection of inter (agent–)server communication using SSL is supported. Standardisation of agent structure, interfaces between agents and agent servers as well as design patterns for secure mobile agent platforms are a grave issue for the future.

Security concepts for mobile agent platforms as well as their actual implementation are mandatory prerequisites for the use of mobile agents in e–commerce applications. In order to succeed in this major effort the driving forces of this new and challenging research field, namely the developers and users, must consider a joint global approach.

10

From a technical vantage this requires serious and continuous standardisation efforts. Effective and sound standards, as already initiated by the *Object Management Group* [18] and the *Foundation for Intelligent Physical Agents* [9] will ensure long range interoperability of different mobile agent systems but must also reflect security aspects more intensively than this was the case in the past. Beyond technical recommendations we would like to stress the need for an ongoing interdisciplinary work on the topic. On one hand legal aspects must be taken into account such as reliability, clear identification of responsibility and guarantees for transactions performed by mobile agents.

On the other hand, for instance electronic trading of sensitive investment goods by agents may bear unforseeable risks. Large numbers of autonomously operating agents, whether they are mobile or not, might rely on the same indicators thus leading to simultanous decisions. Therefor slight changes of indicators could boost a trend and cause impacts on the economy. Electronic trading systems of course must be prepared to this. Additionally, stable economic conditions are mandatory for the prospering of electronic commerce, which is not limited to national borders or regions with a single currency. The introduction of a joint European currency will reduce the risks and costs of spontaneous currency exchange, giving a positive signal to electronic commerce.

References

1. ARNOLD, K., AND GOSLING, J. *The Java Programming Language*. Addison–Wesley, 1996.

2. BAKOS, J. A strategic analysis of electronic merketplaces. *MIS Quaterly 11*, 4 (September 1991), 295–310.

3. BERKOVITS, S., GUTTMAN, J. D., AND SWARUP, V. Authentication for mobile agents. In Vigna [23], pp. 114–136.

4. BRADSHAW, J. M., Ed. *Software Agents*. MIT Press, April 1997.

5. BRENNER, W., AND SCHUBERT, W. Einsatz intelligenter softwareagenten im elektronischen handel. *Handbuch der modernen Datenverarbeitung*, 199 (March 1998), 25–37.

6. CHESS, D. M. Security issues in mobile code systems. In Vigna [23], pp. 1–14.

7. CUGOLA, G., GHEZZI, C., PICCO, G. P., AND VIGNA, G. Analyzing mobile code languages. In *Mobile Object Systems: Towards the Programmable Internet*, J. Vitek and C. Tschudin, Eds., vol. 1222 of *Lecture Notes in Computer Science*. Springer Verlag, Berlin Heidelberg, 1997, pp. 93–111.

8. EUROPAY. Europay electronic market forecast. Internet WWW–page at URL: <http://www.europay.com/E_commerce/html/Market_forecasts.html>. Version current on 1st October, 1998.

9. FIPA. Fipa home page. Internet WWW–page at URL: <http://drogo.cselt.stet.it/fipa>. Version current on 1st October, 1998.

10. GROUP, M. Electronic commerce: A practical business guide – executive summary. Internet WWW–page at URL: <http://www.metagroup.com>. Version current in 1998.

11. GVU. The 9th GVU WWW user survey. Internet WWW–page at URL: <http://www.cc.gatech.edu/gvu/user_surveys>. Version current on 10th August, 1998.

12. IDC. International data corporation. Internet WWW–page at URL: <http://www.idc.com>. Version current on 30th August, 1998.

13. KARJOTH, G., ASOKAN, N., AND GÜLCÜ, C. Protecting the computation results of free–roaming agents. In *Proceedings of the Second International Workshop on Mobile Agents (MA '98)*, K. Rothermel and F. Hohl, Eds., vol. 1477 of *Lecture Notes in Computer Science*. Springer Verlag, Berlin Heidelberg, September 1998, pp. 195–207.

14. KARJOTH, G., LANGE, D. B., AND OSHIMA, M. A security model for aglets. In Vigna [23], pp. 1–14.

15. MALONE, T. W., JATES, J., AND BENJAMIN, R. I. The logic of electronic markets. *Harvard Business Review 67*, 3 (1989), 166–172.

16. MEISTER, R. Grundlagen des electronic commerce mit mobilen agenten. Diplomarbeit an der TU–Darmstadt, October 1998.

17. NECULA, G. C., AND LEE, P. Safe, untrusted agents using proof–carrying code. In Vigna [23], pp. 61–91.

18. OMG. Omg home page. Internet WWW–page at URL: <http://www.omg.org>. Version current on 1st October, 1998.

19. ROTH, V. Secure recording of itineraries through cooperating agents. In *Proc. 4th ECOOP Workshop on Mobile Object Systems: Secure Internet Mobile Computations* (Brussels, Belgium, July 1998), INRIA, Domaine de Voluceau, Rocquencourt, B.P. 105, 78153 Le Chesnay Cedex (France), Dépot légal 010598/150, pp. 147–154.

20. ROTH, V., AND JALALI, M. Access control and key management for mobile agents. *Computers & Graphics, Special Issue on Data Security in Image Communication and Networks 22*, 4 (1998), 457–461.

21. SANDER, T., AND TSCHUDIN, C. F. Protecting mobile agents against malicious hosts. In Vigna [23], pp. 44–60.

22. VIGNA, G. Cryptographic traces for mobile agents. In *Mobile Agents and Security* [23], pp. 137–153.

23. VIGNA, G., Ed. *Mobile Agents and Security*, vol. 1419 of *Lecture Notes in Computer Science*. Springer Verlag, Berlin Heidelberg, 1998.

24. VOLPANO, D., AND SMITH, G. Language issues in mobile program security. In Vigna [23], pp. 25–43.

25. YEE, B. S. A sanctuary for mobile agents. Tech. Rep. CS97-537, University of California at San Diego, La Jolla, CA, April 1997. An earlier version of this paper appeared at the DARPA Workshop on Foundations for Secure Mobile Code.