Future Generation Computer Systems 19 (2003) 173–186

FGCS
Future Generation Computer Systems

www.elsevier.com/locate/future

Migration control for mobile agents based on passport and visa

Sheng-Uei Guan*, Tianhan Wang, Sim-Heng Ong

Department of Electrical and Computer Engineering, National University of Singapore,
10 Kent Ridge Crescent, Singapore 119260, Singapore

Received 17 April 2002; accepted 6 September 2002

Abstract

Research on mobile agents has attracted much attention as this paradigm has demonstrated great potential for the next-generation e-commerce. Proper solutions to security-related problems become key factors in the successful deployment of mobile agents in e-commerce systems. We propose the use of passport and visa (P/V) for securing mobile agent migration across communities based on the SAFER (secure agent fabrication, evolution, and roaming) for e-commerce framework. P/V not only serve as up-to-date digital credentials for agent–host authentication, but also provide effective security mechanisms for online communities to control mobile agent migration. Protection for mobile agents, network hosts, and online communities is enhanced using P/V. We discuss the design issues in detail and evaluate the implementation of the proposed system.

Keywords: Passports and visa; Migration; Mobile agents; E-commerce; SAFER

1. Introduction

According to the World Trade Organization (WTO), e-commerce is “the production, advertising, sale and distribution of products via telecommunication networks” [1]. One noticeable advantage is that e-commerce removes constraints set by geographical locations and speeds up traditional transaction processes by electronic means. Because monetary transactions are included, security is the number one concern. The highly distributed and global nature of the Internet also forces e-commerce systems to cope with numerous machines running on different platforms in heterogeneous networks. Moreover, current systems based on the client–server architecture are also constrained by limited network bandwidth. To overcome these difficulties, secure, cost efficient, and intelligent e-commerce systems are needed to ensure “convenience and confidence” [2].

Mobile agent technology was introduced as a paradigm to build smart e-commerce systems. It has attracted substantial attention from researchers [3–5]. Mobile agents, as defined commonly, are sophisticated software entities that autonomously travel through a network environment and make complex decisions on the user’s behalf [6]. The critical idea of mobile agent systems, compared to their client–server counterparts, is that by migrating to destination machines, mobile agents greatly reduce the consumption of network bandwidth and avoid causing excessive network traffic, and at the same time process information near data sources. These mobile programs are especially suitable for highly distributed applications and may have the potential to overcome some of the problems that current e-commerce systems face.

* Corresponding author. Tel.: +65-6874-5153;
fax: +65-6779-1103.
E-mail address: eleguans@nus.edu.sg (S.-U. Guan).

0167-739X/02/$ – see front matter © 2002 Elsevier Science B.V. All rights reserved.
PII: S0167-739X(02)00128-0

However, the introduction of mobile agents also brings up many security related issues [7–9,19]. Users of mobile agents will need to be assured that their agents are safe when they are traveling around in the network, i.e., if their agents can be protected from attacks and can function as desired. From the network hosts' point of view, they would like to be sure that incoming mobile agents originate from reliable sources and will not damage their systems when executed. It can be concluded that the advantage of mobility must not be offset by the disadvantages caused by lack of sufficient security protection. Thus providing mechanisms to establish trust and reputation in distributed mobile agent systems is an extremely important issue.

There are technologies that provide services to identify clients in distributed systems, such as digital certificates. A certificate is a statement guaranteeing the identity of a person or the security of a web site, and is issued by independent certification authorities, such as "Verisign" [10]. For mobile agents, this may be the digital certificate of its code provider. A certificate is useful for one-hop transport, but may not be enough for mobile agents as they typically travel on a multi-hop basis. Furthermore, a digital certificate cannot be modified after being issued. While some research focuses on how to develop mutual authentication and authorization protocols [11], it is known that a single certificate certifying only the code provider is not enough to ensure security in mobile agent communities. Following similar lines of thoughts, Lai et al. [12] have described a method to electronically represent endorsements, licenses and insurance policies to build enhanced confidence in distributed systems. It is desirable that novel types of digital credentials that are up-to-date to serve both authentication purpose and some security objectives can be developed.

In this paper, we propose using passports and visas for mobile agent migration across communities based on the SAFER (secure agent fabrication, evolution, and roaming) for e-commerce framework [13–15]. SAFER provides an integrated framework to manage and secure mobile agents in agent-mediated e-commerce systems. Migration refers to the travel of mobile agents from one community to another, while passports and visas should be the official travel documents that mobile agents need. The Migration Service Center (MSC) proposed in this paper provides services to manage and control mobile agents when they are roaming among community hosts (CAs), while passports and visas serve as up-to-date certificates to achieve integrated security objectives for protecting mobile agents, network hosts, and SAFER communities.

The organization of this paper is as follows. We start by introducing background information for the SAFER framework in Section 2. In Sections 3 and 4, we elaborate in detail the design and implementation issues for mobile agent migration of our proposed P/V system and the MSC entity. We also discuss and evaluate our system in these sections. Section 5 concludes this paper.

2. SAFER background

Our proposed P/V and migration system are based on SAFER because SAFER has already established a rich set of security mechanisms with its community entities. Based on SAFER, many e-commerce applications such as auction services and electronic payment systems have been proposed [16,17].

SAFER consists of SAFER-compliant and non-SAFER communities with relevant entities inside each community. Fig. 1 shows the basic structure and interactions among entities in SAFER communities.

For the sake of clarity, only entities relevant to our system are shown in Fig. 1. From the figure, it can be seen that within each SAFER community, we have several entities that are key to the functioning of the whole community. For example, the agent factory is responsible for fabricating mobile agent programs. According to the requirements set by agent owners, it can generate pieces of agent function modules and construct standard agent programs that can be dispatched to remote hosts to accomplish e-commerce related tasks. After the customization has been done and the fabrication is complete, agent programs are ready for downloading by agent owners. In order that the identity of the mobile code be recognized and its integrity protected by third party verification, agent programs need to be digitally signed by the agent factory before being downloaded. Any party can then verify the digital signature of the mobile code using the public key of the agent factory.

Agent butler is an entity that acts on behalf of the agent owner. It is responsible for dispatching mobile

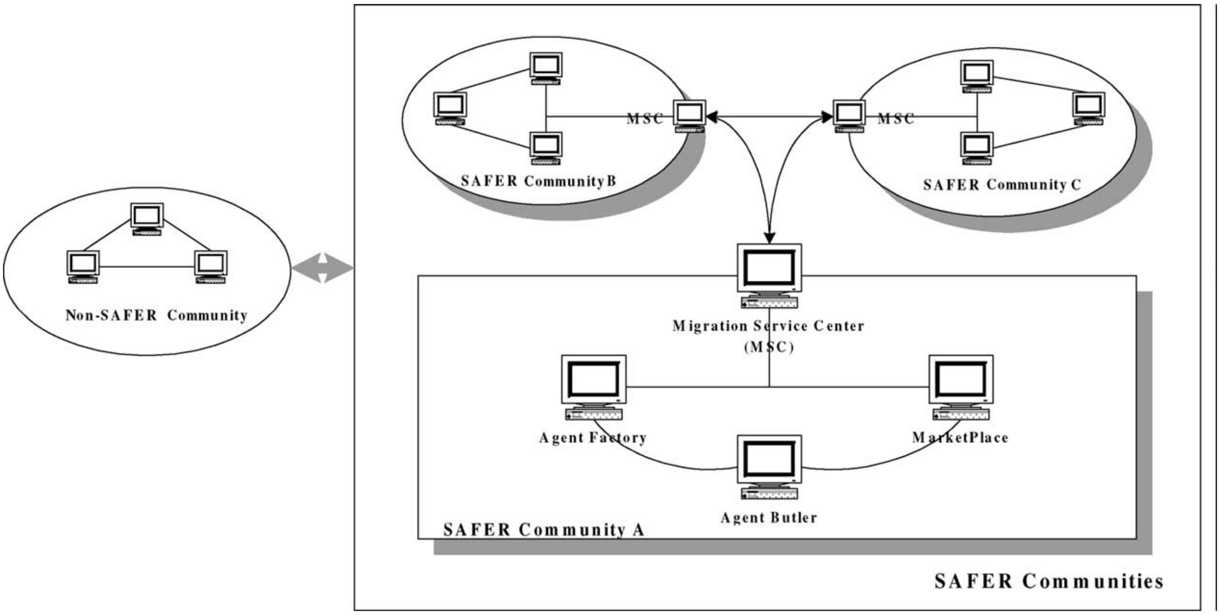


Fig. 1. SAFER and non-SAFER agent communities.

agents and responding to requests from its agents and other parties. The agent butler is also expected to be equipped with sufficient intelligence to make smart decisions and control its mobile agents in most cases. However, under certain circumstances when crucial decisions are to be made, the owner's supervision is still needed.

Besides these public entities within a SAFER community, we still have many host machines that belong to the community on which business transactions or e-commerce related tasks are performed, such as the "marketplace" server in the figure. These hosts include information reservoirs in which databases are maintained, vendor machines that sell flight tickets, or transaction servers that process electronic payments. They are also intermediate or ultimate destinations for mobile agents who will roam there to complete certain specific tasks.

The gatekeeper of each community is MSC, which is trusted by the public. MSC functions as a gateway to facilitate the entry and exit of mobile agents. Further details of the MSC functions are given in the next section.

When mobile agents are roaming among CAs, we must provide a means for hosts to efficiently recognize and verify the true identities of mobile agents. Correct authentication is important for follow-up procedures such as authorization and execution. From the agents' perspective, we must be able to provide a means to protect mobile agents in order that any compromise may be detected as soon as possible. From the communities' viewpoint, mobile agents should be monitored and controlled. To bring these three objectives together, we propose the use of passports and visas for mobile agent migration.

3. P/V and migration control

Here we propose passports and visas as credentials issued by MSCs, which are official documents for mobile agents to be authenticated by hosts. Through the successful verification of P/V, each party is assured that an agent comes from a reliable source and will not perform any malicious attacks. Proper security privileges for the incoming agent can then be decided.

3.1. Motivation

It has been suggested by many researchers that security issues within mobile agent technology can be divided into two areas: protecting hosts and protecting agents [18]. However, these two areas can never be clearly distinguished. For example, when a host verifies the signature and integrity of a mobile agent, it may detect malicious code and thus protect itself. However, if a malicious attack on the agent has been detected, the host may also notify the agent owner so that the mobile agent in concern will also be protected and further loss caused by the dysfunction of such a compromised agent can be prevented.

The code provider's certificates may be useful to prove the identity of a mobile agent program. For example, the digital certificate accompanying a Java program that is downloaded by the browser from the Internet is important to help the user assess the trustworthiness of such a program. People tend to trust the source of the code instead of actually verifying the code. However, in the case of mobile agents, this is not sufficient. Firstly, mobile agents will typically make multiple hops along their routes to perform e-commerce tasks. This means that the route information of mobile agents can be more complex and needs to be tracked. Secondly, more information is needed for the host to correctly determine the real identities of mobile agents and decide on the security procedures to be adopted to deal with incoming agents. That information may include the fabricator of the agent, the owner of the agent and the original source community of the mobile agent. Thirdly, it is desirable that an integrated mechanism that benefits all, the communities, mobile agents, as well as CAs can be provided. We elaborate in the following:

- A community must be able to administer and control mobile agents effectively. Although there are no actual boundaries in the cyberspace, a community must be able to control whether certain types of mobile agents should be allowed to leave or enter. The community may have sufficient reasons to prohibit certain types of mobile agents from leaving because these agents may disclose sensitive community information, or certain agents can have a higher possibility of dysfunction if dispatched outside; on the other hand, some mobile agents may be banned from entering the community because they have "criminal" records.
- A host must be able to assess mobile agents before allowing them to execute on its machine. Checking of the integrity and signature of the mobile agent code is not enough; it is desirable that the host also has the information about the code fabricator, the agent owner, the community origin and even the past route of the mobile agent to make a correct decision to allocate proper resources and adjust security measures.
- An agent must be able to protect itself by allowing trusted parties to detect any compromise of its integrity as soon as possible. The agent must also possess the correct credentials to let other parties verify its own identity.

Bearing the above-mentioned issues in mind, we introduce P/V for mobile agent migration among communities. Through the successful verification of P/V, each host is better informed that an incoming agent will not perform any malicious attacks. Proper security measures for the incoming agent can then be decided. For example, if a mobile agent comes from a notorious community or is fabricated by an agent factory that has been reported to produce many malicious agents, it will not pass the security check in the beginning. On the other hand, if a mobile agent comes from a well-trusted owner (or factory) within a trusted community, security check will still be performed to see whether the agent has been compromised or it is on a black list. An agent from a reliable source and clear from any black list is more likely to be authorized with more system resources.

3.2. Design issues

3.2.1. MSC

MSC is a trusted entity comprising two parts: immigration service and emigration service. Its structure and functions are shown in Table 1. As shown in the

Table 1
Structure and functions of MSCs

Functions	MSC	
	Immigration service	Emigration service
Exit control	N/A N/A	Issuing passports Stamping passports
Entry control	Issuing visas Stamping visas	N/A N/A
Route tracing	Tracing agent route based on the P/V's	

table, the principal responsibilities of MSC include issuing and stamping credentials, i.e.:

(1) *Exit control*: For outgoing agents from the local community, it is responsible for issuing passports and stamping passports.
(2) *Entry control*: For incoming agents from remote communities, it is responsible for issuing visas and stamping visas.

Migration control is actually the first step in controlling mobile agents and protecting its CAs. In order to do this, MSC maintains multiple positive lists and black lists. A positive list records hosts, factories or communities that are certified by a particular CA. Such a list can be requested and updated regularly from CAs. A black list records misbehavior of mobile agents that have ever resided or roamed in the community, and their associated parties such as factories, owners and communities. These black lists may include a community black list, a factory black list, a butler (owner) black list and an agent black list. The black lists may be maintained and updated by employing some rules, with different levels and metrics set to make the representation more reasonable. The rules are explained below:

(1) A community black list records untrustworthy communities. A community black-listed will make all the entities within such a community, such as agent factory, agent butler, and fabricated agent untrustworthy.
(2) A factory black list records untrustworthy agent factories. A factory black-listed will make all the agents fabricated by this factory untrustworthy.
(3) An agent butler (owner) black list records untrustworthy agent butlers and owners. An agent butler or agent owner black-listed will make all the agents owned by him untrustworthy.
(4) An agent black list records untrustworthy agents that have been reported as malicious.

An entity being black-listed may also affect the reputations of other associated entities. For example, mobile agents from the same owner that repeatedly misbehave when roaming outside will cause their owner to be black-listed, while significant number of mobile agents fabricated by the same agent factory which performs malicious actions will cause the manufacturing factory to be black-listed. Note that the black list should be updated promptly, and employing sufficient intelligence to make reasonable and correct decisions and deductions when necessary.

With such positive lists and black lists, MSC will be able to control strictly whether or not to issue a passport or a visa to a specific agent. For example, some mobile agents carrying sensitive information or performing important internal tasks will not be allowed to leave their own community in most situations, and their passport request for exit will not be approved. Since passport is the only official document that a mobile agent holds when roaming, lacking it will make the agent unrecognized and unaccepted. A similar black list may also be maintained by MSC for deciding on the issuing of visas to incoming agents.

As different communities may enforce different security policies, we leave open the use of positive/black lists in designing different types of security policies.

MSC may have more functions besides those mentioned above, such as tracing agent routes based on the passport and visas (P/V's). Note that although SAFER communities comply with the SAFER rules, each community still has the flexibility to have its own additional entry/exit control rules. Mobile agents roaming to another SAFER-compliant community may have problems recognizing the peculiar regulations of the destination community. The MSC may act as a translator between communities to advise mobile agents how to adjust to the new environment.

3.2.2. Passport

Passport is a certified proof of identity issued by a local MSC. It is the official travel document recognized by another SAFER community. Any mobile agent that intends to roam to other communities must have a valid passport issued by its local MSC.

After the agent butler has customized and downloaded a mobile agent to its own machine, it must request a passport for the agent from the local MSC before the agent can be dispatched. We assume a secure communication protocol is used between the agent butler and MSC. The agent butler will need to send the mobile agent with a passport request to the local MSC emigration which will then examine the authenticity of the agent code and also the identities of the manufacturer and the agent owner. If these verifications yield positive results, MSC needs to refer to its positive/black lists to decide whether the agent

Table 2
A primitive structure of passport content

Number	Passport entries	Entry semantics	Examples
1	PASID	Passport ID number	COMAIMM001
2	FACID	Agent factory ID number	COMAFAC001
3	OWNID	Agent owner ID number	COMAOWN001
4	AGTID	Mobile agent ID number	COMAFA1OW1
5	COMID	Community ID number	COM000001
6	AGTDG	Message digest of the agent	SD 8F DF 4G...
7	ISSDT	Passport issuing time	GMT + 8, 7 May 2001, 11-25 h
8	EXPDT	Passport expiration time	GMT + 8, 7 May 2001, 12-25 h
9	EXIST	Passport exit stamp	FALSE
10	ENTST	Passport entry stamp	FALSE

should be allowed to leave and how long this agent can roam out. After all decisions have been made, a passport is issued to the agent. A primitive structure of the passport can be shown in Table 2.

The first five entries are the identification numbers to help record the origin of a mobile agent. *PASID* is assigned by MSC to represent a unique passport number, and the other ID numbers are obtained, respectively, from the mobile agent itself. The entry *AGTDG* is a message digest produced by calculating the hash value of the agent program using collision-resistant hash functions; it binds this passport to the agent that is requesting the passport. The example shows an encoded representation of a 128-bit message digest. *ISSDT* is the issuing time/date of the passport and *EXPDT* the passport expiration time/date. The valid period of a passport can vary, depending on the type of the agent and the task it is to complete. Finally, the two stamp entries *ENTST* and *EXIST* are all initially stamped “FALSE”. These entries will acquire the value of “TRUE” from MSC when the agent leaves the local community and enters a remote community.

After the passport has been created, it is required that the passport issuing party, namely the local MSC, to digitally sign the passport. In this way, other parties may be able to verify the authenticity of the passport using the public key of MSC and in turn verify the authenticity of the mobile agent via the passport entry AGTDG. The procedure is shown in Fig. 2.

In this way, we are also able to prevent the misuse of passport, e.g. attaching a specific passport to an unauthorized agent, since the passport is bound to the agent by the passport entry AGTDG. In summary, we are able to do the following:

(1) detect the compromise of a passport,
(2) detect the compromise of a mobile agent,
(3) detect the misuse of a passport by an unauthorized agent.

3.2.3. *Visa*

After the mobile agent has obtained a valid passport, it also needs an entry visa from its immediate destination. For example, if the agent in community A intends to visit community B and community C, it must obtain at least an entry visa from community B before it can be accepted by the hosts in this community. In order to obtain a visa, it needs to send a copy of its passport over to MSC in the destination community to request a visa. Subsequent visas requests can be made via intermediate community MSC along its travel route. For example, the visa request for community C may be made through MSC in community B, and so on.

The remote MSC will need to check the authenticity and integrity of the passport and decide whether to issue a visa to this incoming agent based on the passport content. The MSC may look at its positive/black lists to find out if any party associated with the incoming agent has any problem. If everything is fine, the MSC may attach an entry visa to the passport. A primitive structure of a visa is shown in Table 3.

The structure of a visa is quite similar to that of a passport, so we will not discuss most entries in detail. Note that we have an entry named *PASDG* which records the message digest of the passport. This binds a specific visa to a specific passport, which makes

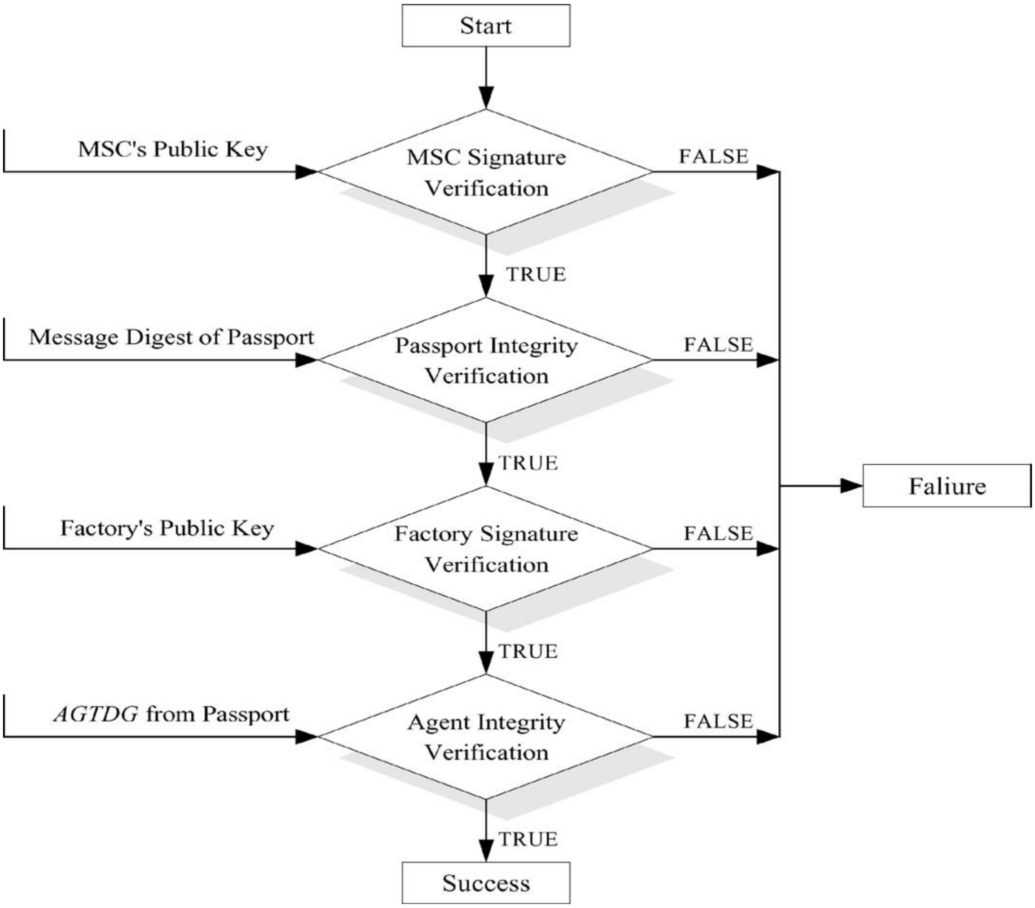

Start
MSC's Public Key
MSC Signature Verification
FALSE
TRUE
Message Digest of Passport
Passport Integrity Verification
FALSE
TRUE
Faliure
Factory's Public Key
Factory Signature Verification
FALSE
TRUE
AGTDG from Passport
Agent Integrity Verification
FALSE
TRUE
Success

Fig. 2. Binding and verification of passport in an agent.

Table 3
A primitive structure of visa content

Number	Visa entries	Entry semantics	Examples
1	VISID	Visa ID number	COMBIMM001
2	FACID	Agent factory ID number	COMAFAC001
3	OWNID	Agent owner ID number	COMAOWN001
4	PASID	Passport ID number	COMAIMM001
5	COMID	Community ID number	COM000002
6	PASDG	Message digest of the passport	34 FH DG D5...
7	ISSDT	Visa issuing time	GMT + 8, 7 May 2001, 11-40 h
8	EXPDT	Visa expiration time	GMT + 8, 7 May 2001, 12-40 h
9	EXIST	Visa exit stamp	FALSE
10	ENTST	Visa entry stamp	FALSE

impossible the misuse of a visa on another unauthorized passport and in turn on an unauthorized agent. To summarize, the binding strategy here is to bind the visa to the passport and to bind the passport to the agent, so that unauthorized use of any of these three entities (visa, passport, and agent) may be detected.

The issue of visas can be relaxed to cater to the needs of different security requirements. For example, the validity period of the visa, determined from EXPDT and ISSDT entries, may vary based on the trust placed on the incoming agent. Two communities may even have a mutual visa-waiving agreement in which no visas are needed for entry from a friendly community. These measures not only provide more flexibility, but also greatly reduce the cost caused by security checks and verifications.

After the P/V have been obtained, an agent is ready to be dispatched to other CAs. This includes three procedures: (1) passport stamping by MSC emigration, (2) visa stamping by the MSC immigration (destination) and (3) roaming to the destination hosts to perform its task. Before leaving its current community, a mobile agent needs to visit the local MSC again to have its passport entry EXIST stamped as “TRUE”. Before roaming to the destination host, the mobile agent is also required to visit the destination MSC first to have its visa’s ENTST entry stamped. This will help both MSCs to track the route of mobile agents and will also ensure that the mobile agent has authorized departure and entry into a designated community.

Upon arriving at the host platform, the agent will be subjected to a thorough examination by the host. The host will need to verify the authenticity and integrity of the passport, visa and the agent itself. The contents of the P/V will be extracted and examined to decide on the security levels and resource authorization. The host may also be required to report to its community MSC the arrival and departure of any mobile agent so that the route and behavior of the agent can be traced and analyzed.

4. Implementation

4.1. *Implementation of MSC, P/V*

We have implemented the proposed P/V and SAFER migration system in a three-community simulation environment using Java as the programming language. We developed a multiple-hop mobile agent that gathers necessary information from CAs. Java’s security packages and APIs are used to realize encryption, digital signatures with DSA-based public/private key of 1024-bit length, and a collision-resistant hash function using MD-5 algorithm that produces 128-bit message digest. Message exchanges for requests and responses will go through a secure communication protocol to prevent any attack during these transactions.

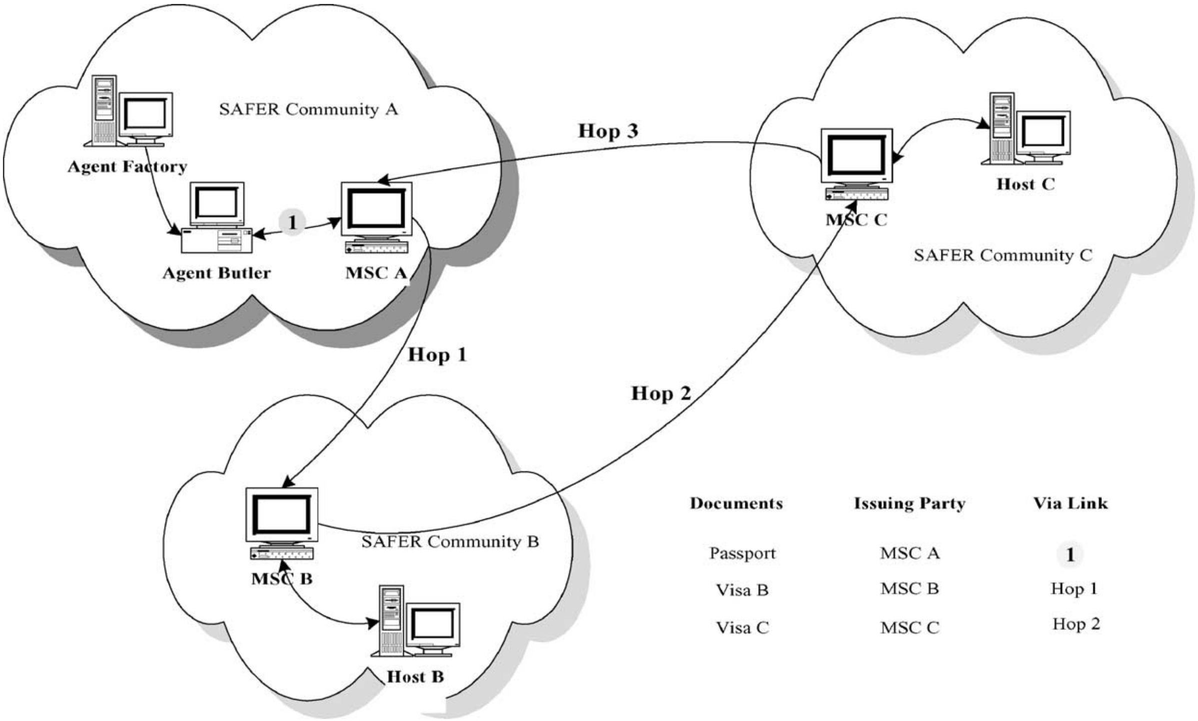
The mobile agent, which originates from community A, is equipped with tasks for information-gathering at remote hosts in community B and community C (Fig. 3).

In this implementation, the information-gathering agent is dispatched by its butler from community A and will visit Host B in community B and Host C in community C sequentially to complete its tasks. As discussed in our earlier sections, the mobile agent needs to obtain a passport from local MSC A and Visa B from MSC B in community B before departure and also needs to obtain Visa C before departure for Host C in community C.

The first task for the mobile agent is to request a valid passport from local MSC A. The local MSC may evaluate the qualifications of the requesting agent and decide whether or not to issue a passport. Fig. 4 gives the screen shot showing the GUIs of the agent butler and also the MSC in community A. The highlighted buttons indicate the present process. The dialog box on the right illustrates the situation when the agent has been black-listed by the local MSC, in this case the passport request will be refused and will not be issued.

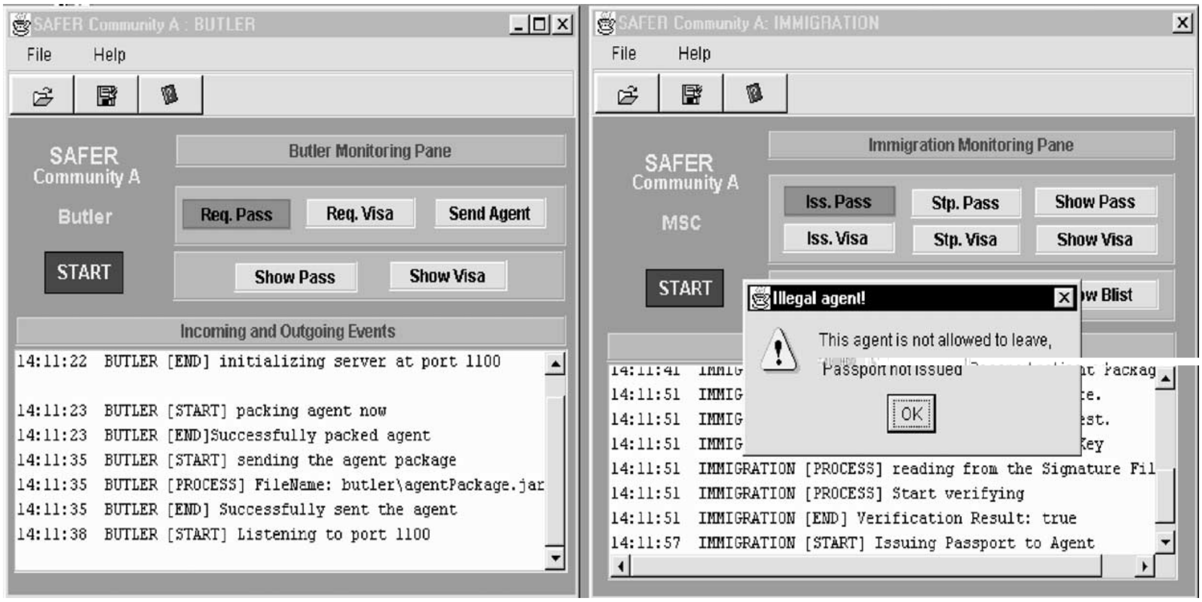
After the mobile agent has obtained a valid passport from the local MSC, it needs to request an entry visa from its immediate destination community B, following the procedure described in Section 3.2.3. At this point, the agent is ready to leave its own community and roam to its destination. The passport needs to be stamped by MSC emigration in community A for EXIST entry, and the visa also needs to be stamped by MSC immigration in community B for ENTST entry before the agent can arrive in Host B for a complete security examination.

When a mobile agent needs multiple visas, there are two ways that the agent code, P/V’s can be packaged.



Documents	Issuing Party	Via Link
Passport	MSC A	1
Visa B	MSC B	Hop 1
Visa C	MSC C	Hop 2

Fig. 3. P/V and migration system implementation overview.



```
14:11:22  BUTLER [END] initializing server at port 1100

14:11:23  BUTLER [START] packing agent now
14:11:23  BUTLER [END]Successfully packed agent
14:11:35  BUTLER [START] sending the agent package
14:11:35  BUTLER [PROCESS] FileName: butler\agentPackage.jar
14:11:35  BUTLER [END] Successfully sent the agent
14:11:38  BUTLER [START] Listening to port 1100
```

This agent is not allowed to leave,
Passport not issued

```
14:11:41  IMMIG                                    nt Packag
14:11:51  IMMIG                                    te.
14:11:51  IMMIG                                    est.
14:11:51  IMMIG                                    Key
14:11:51  IMMIGRATION [PROCESS] reading from the Signature Fil
14:11:51  IMMIGRATION [PROCESS] Start verifying
14:11:51  IMMIGRATION [END] Verification Result: true
14:11:57  IMMIGRATION [START] Issuing Passport to Agent
```

Fig. 4. Passport request refused due to that the mobile agent has been black-listed.

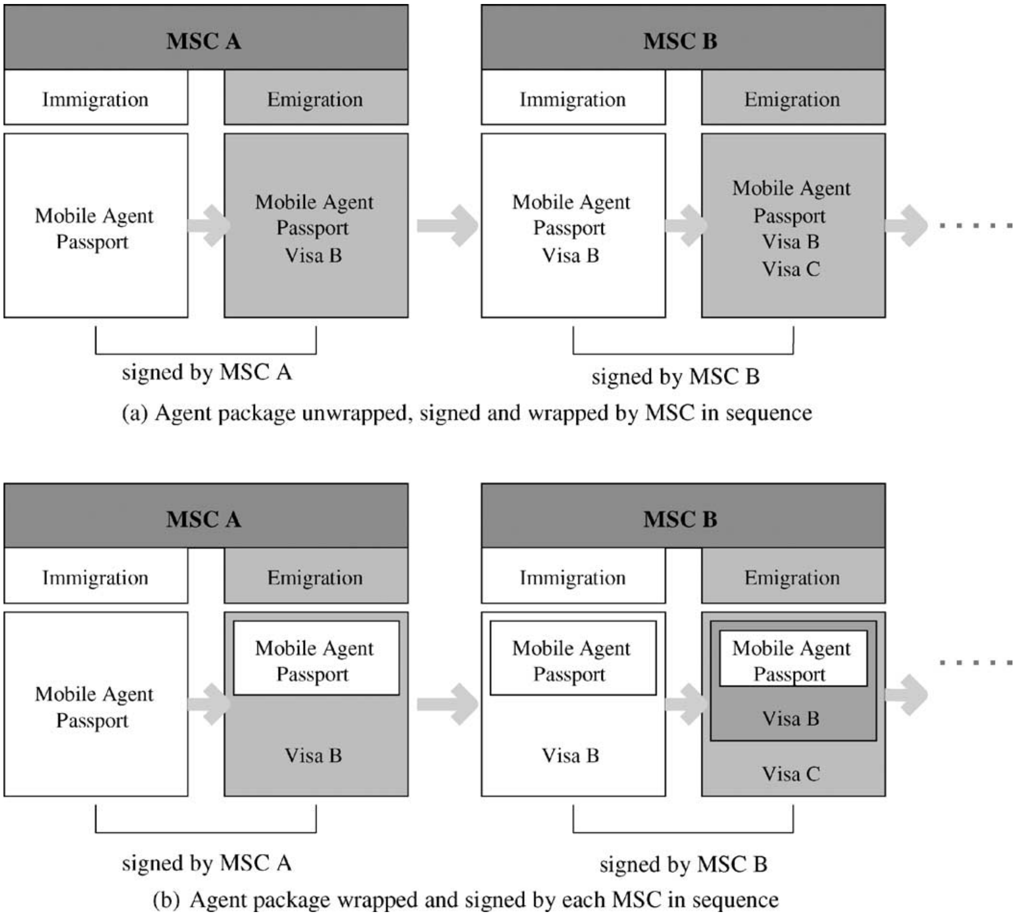


Fig. 5. Wrapping of multiple visas by MSCs.

Fig. 5 illustrates the two solutions for wrapping multiple visas B and C.

Provided that each entity within a package is digitally signed by its original producer, one way is to let the most recent MSC unpack the previous agent package and produce a new package signed with its own private key, as shown in solution (a). Obviously, this approach relies on the underlying assumption that MSC is a trusted party. This is less secure but with more efficiency for signature verification. Another way is to leave all previous agent packages intact and simply have new documents added and signed by the most recent MSC, as shown in solution (b). This is more secure because previous packages are untouched, yet with less efficiency when verifying signatures since multiple levels of packages must be unpacked for complete verification. Solution (a) is recommended when the agent travels among highly trusted communities, while solution (b) is suggested if the agent is to travel among less secured sites.

4.2. *Implementation of positive and black lists*

The lifecycle of a positive/black list may include four stages: construction, initialization, maintenance, termination and destruction. When a list is first constructed, it is empty with no listed members. Initialization refers to that a list acquiring information to establish its initial contents. Maintenance refers to the update of lists, which includes the removal or addition of members to existing lists. Termination refers to the stopping of list update that leads to a physical destruction of the list later.

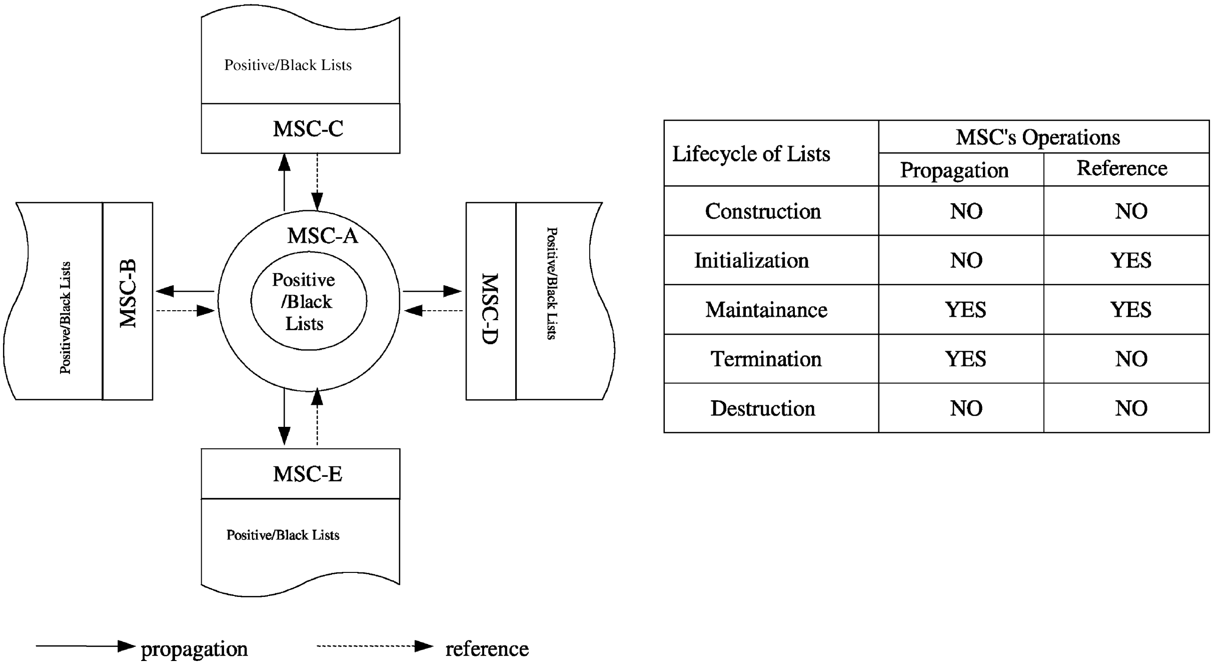
MSC's list operations include reference and propagation. Reference means that an MSC may refer to its cooperating MSCs (and CAs if a positive list is concerned) for shared information on list contents, while propagation means an MSC may distribute its own list information to other cooperating MSCs. During the different stages of list lifecycle, MSC may operate on its lists in different ways. The relationship is illustrated in Fig. 6.

During the initialization stage, a local MSC needs to refer to its cooperating MSCs (or CAs) for their list information to build its own lists. After the lists have been initialized, MSC may continue to refer to other MSCs for list information and at the same time may propagate its list information to cooperating communities. Thus during this stage, the MSC operations include both reference and propagation. The addition and removal of list members may also refer to reports from CAs. MSCs from different communities may choose to share and administer a common positive/black list database for list update and maintenance or inherit from a common database and add their community specific list members for their own use.

4.3. Discussions and system evaluation

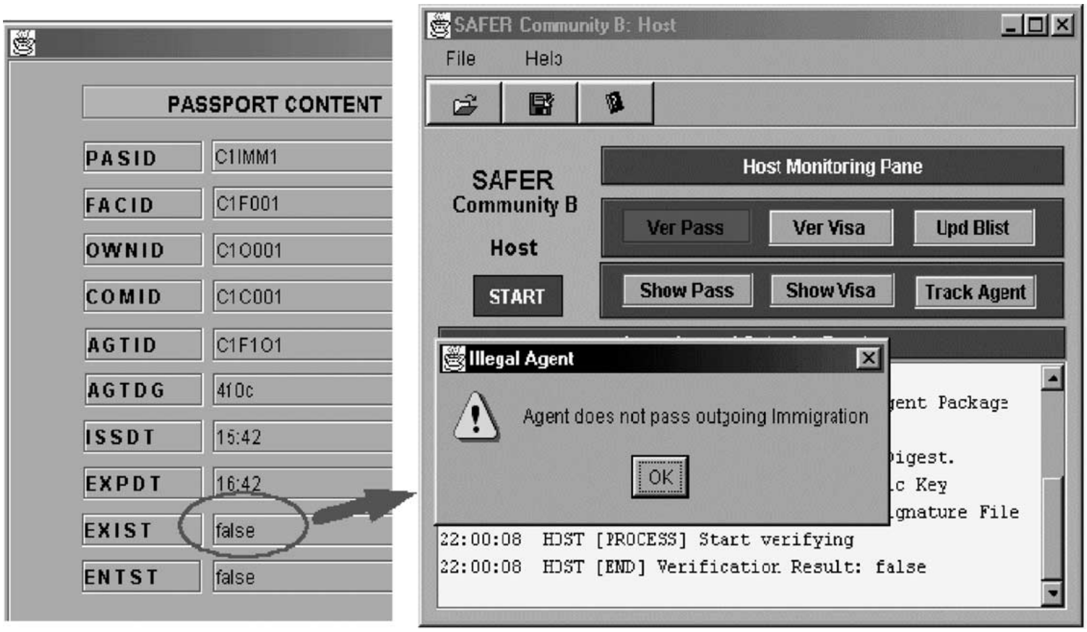
In order to test and evaluate our prototype implementation, we also developed a program that can simulate several malicious attacks to the agent, the passport, and the visa. For example, the attacker may tamper with the P/V contents, modify the mobile agent, or illegally send unstamped agents to other communities. Our implementation results have shown that all these attacks can be detected by the MSCs and CAs using our scheme. The following screen shot (Fig. 7) shows an unstamped agent trying to sneak into a community while it has been detected by the MSC in community B. The unstamped entry EXIST in the passport on the left side results in the verification failure by Host B in community B, and the agent will be treated as illegal.

P/V can also be used to trace mobile agents. Both wrapping solutions discussed in the previous section eliminate the possibility that any credential inside the agent package can be deleted by attackers, provided that MSCs are trusted parties. By analyzing the visas



Lifecycle of Lists	MSC's Operations	
	Propagation	Reference
Construction	NO	NO
Initialization	NO	YES
Maintainance	YES	YES
Termination	YES	NO
Destruction	NO	NO

Fig. 6. Lifecycle and MSC's operations on positive/black lists.



PASSPORT CONTENT

PASID	C1IMM1
FACID	C1F001
OWNID	C1O001
COMID	C1C001
AGTID	C1F1O1
AGTDG	410c
ISSDT	15:42
EXPDT	16:42
EXIST	false
ENTST	false

Agent does not pass outgoing Immigration

```
                                    gent Package

                                    igest.
                                    c Key
                                    gnature File
22:00:08  HOST [PROCESS] Start verifying
22:00:08  HOST [END] Verification Result: false
```

Fig. 7. Detecting an agent sneaking away holding an unstamped passport.

and passport carried by a mobile agent, the destination party will be able to discover where the agent has been. If the agent has been to a community that is not secure, the destination MSC may enforce a strict security check to ensure its own safety. However, if it is seen from the visa record the agent has been traveling among reputable hosts and communities, these security measures can be relaxed.

P/V are also relevant to mobile agents that download code modules (from an agent factory, for example) to upgrade its functionalities. When a code module in a community is to be downloaded by mobile agents, passports and visas can be used to for the entry and exit control of such a module. In this way, communities may not only control the migration of mobile agents, but also individual code modules. On the other hand, since the agent code part may be subjected to change during its migration, some of the entries in P/V's may be affected, for example, the AGTDG entry in passport. For such mobile agents holding P/V's to be authenticated correctly by CAs after code change, the P/V contents will need to be updated. To alleviate the cost of sending an agent back to its local community for a new passport, we suggest using TTPs (together with MSCs) as a potential solution to help with agent digest re-computation and P/V update.

From the above discussions, we may conclude that migration control for mobile agents is feasible by using the proposed P/V scheme. We are able to control and trace mobile agents when they roam into network communities and hosts. We are also able to provide a mechanism to ensure that communities, hosts, and agents will be protected. However, it seems that the detection of duplicated passport is still difficult although we are able to detect the misuse of passports and visas by unauthorized parties. We have the following suggestions to solve this problem. To prevent and detect the illegal duplication and misuse of an agent package, which contains the mobile agent, the passport, and visas, we suggest that the mobile agent maintain a regular communication with the agent butler. The agent sends regular short signals like "heart-beats" to inform its butler where it is and how well it is functioning. In this way, the agent butler may be able to detect unauthorized duplication if "heart-beats" becomes abnormal, for example, two "heart-beats" from the same agent coming from different hosts.

Our proposed P/V scheme has some advantages in comparison with the digital certificate approach. For one-hop mobile agents that do not roam to a second destination, a certificate may be enough, because the agent does not have route information that needs to be analyzed. However, for multi-hop mobile agents, the use of passports and visas provide more information. They can also be updated promptly and thus remain up-to-date compared with the static certificate. Another advantage is that they can be used for controlling the entry and exit to communities by mobile agents.

For e-commerce, there may be requirements that agents prefer to remain anonymous during any transaction (as its owner would like to be anonymous). Our P/V scheme can accommodate this requirement by allowing agents to be issued passports and visas with their (owner) names not shown. The passport and visas issued to such an anonymous agent will be linked to some unique agent ID, where the ID is maintained by the agent's original MSC and any sensitive information regarding the agent will be kept secret unless the agent has been involved in any illegal transactions.

Besides SAFER-compliant communities, there are of course non-SAFER communities that do not conform to SAFER standards and regulations. In order to promote compatibility, it is critical to provide a compatible passport structure so that it can be recognized as a standard certificate carried by mobile agents when visiting non-SAFER CAs. As a first step toward an open architecture, we have suggested in our implementation by using keyword entries to structure the P/V content. Thus, what is of importance here is not the actual format of the passport but rather the keywords.

There are some issues falling outside of technical domains but are interesting and important for research. For example, the issuing of passports and visas may also be subjected to charges as required by community MSCs. In the legal aspect, does a community have the right to destroy an agent locally if it is found to be malicious?

5. Conclusions

In this paper, we have proposed a security system for mobile agent migration with P/V. Migration refers to the travel of mobile agents among different communities, while passports and visas are the credentials issued by the trusted MSCs in SAFER to serve as the official travel documents. Besides basic functions similar to digital certificates to prove the identities for mobile agents, passports and visa provide more information about mobile agents that can be used to enhance security protection for communities, hosts, and mobile agents as well. P/V and migration system also provides a solution to effectively manage and control the entry and exit of mobile agents under community environments. The implementation result also shows that the proposed system is feasible and effective.

In our future work, we plan to formally define the structures of P/V based on the standards of digital certificates. The authentication protocols also need to be refined further. The policy to decide on proper security levels based on available information from passports and visas are also an interesting issue for continuing research.

References

[1] Study from WTO Secretariat Highlights Potential Trade Gains from Electronic Commerce, World Trade Organization (WTO) News Press Release, 1998. http://www.wto.org/english/news_e/pres98_e/pr96_e.htm.

[2] S. Hamilton, E-commerce for the 21st century, IEEE Comput. 30 (5) (1997) 44–47.

[3] V.A. Pham, A. Karmouch, Mobile software agents: an overview, IEEE Commun. Mag. 367 (7) (1998) 26–37.

[4] R.S. Gary, D. Kotz, G. Cybenko, D. Rus, D'Agents: security in a multiple-language, mobile-agent system, in: G. Vigna (Ed.), Mobile Agents and Security, Springer, Berlin, 1998, pp. 154–188.

[5] MIT Software Agents Group. http://agents.www.media.mit.edu/groups/agents/.

[6] J. Wong, G. Helmer, V. Naganathan, S. Polavarapu, V. Honavar, L. Miller, SMART mobile agent facility, J. Syst. Softw. 56 (2001) 9–22.

[7] A. Corradi, R. Montanari, C. Stefanelli, Security issues in mobile agent technology, in: Proceedings of the Seventh IEEE Workshop on Future Trends of Distributed Computing Systems, 1999, pp. 3–8.

[8] D. Chess, Security issues in mobile code systems, in: G. Vigna (Ed.), Mobile Agents and Security, Springer, Berlin, 1998, pp. 1–15.

[9] P.J. Marques, L.M. Silva, J.G. Silva, Security mechanisms for using mobile agents in electronic commerce, in: Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems, 1999, pp. 378–383.

[10] Verisign: http://www.verisign.com.

[11] S. Berkovits, J.D. Guttman, V. Swarup, Authentication for mobile agents, in: G. Vigna (Ed.), Mobile Agents and Security, Springer, Berlin, 1998, pp. 114–137.

[12] C. Lai, G. Medvinsky, B.C. Neuman, Endorsements, licensing, and insurance for distributed system services, in: Proceedings of the ACM Conference on Computer and Communication Security, 1994, pp. 170–175.

[13] S.U. Guan, Y. Yang, SAFE: secure-roaming agent for e-commerce, in: Proceedings of the 26th International Conference on Computers and Industrial Engineering, 1999, pp. 33–37.

[14] Y. Yang, S.U. Guan, Intelligent mobile agents for e-commerce: security issues and agent transport, in: S.M. Rahman, M. Raisinghani (Eds.), Electronic Commerce: Opportunities and Challenges, IDEA Group Publishing, 2000, pp. 321–336.

[15] F.M. Zhu, S.U. Guan, Y. Yang, SAFER e-commerce: secure agent fabrication, evolution and roaming for e-commerce, in: S.M. Rahman, R.J. Bignall (Eds.), Internet Commerce and Software Agents: Cases, Technologies and Opportunities, IDEA Group Publishing, 2000, pp. 190–206.

[16] F. Hua, S.U. Guan, An agent-based electronic payment scheme for e-commerce, in: S.M. Rahman, R.J. Bignall (Eds.), Internet Commerce and Software Agents: Cases, Technologies and Opportunities, IDEA Group Publishing, 2000, pp. 317–330.

[17] T.H. Wang, S.U. Guan, S.H. Ong, An agent based auction service for electronic commerce, in: Proceedings of the International ICSC Congress on Intelligent Systems and Applications, CD#1524-045, 2000.

[18] M.S. Greenberg, L.C. Byington, D.G. Harper, Mobile agents and security, IEEE Commun. Mag. 367 (7) (1998) 76–85.

[19] N.M. Karnik, A.R. Tripathi, Security in the Ajanta mobile agent system, Softw. Pract. Exp. 31 (4) (2001) 301–329.