A Secured Layered Architecture For Mobile Agent

Swati Aggarwal
IMSEC Ghaziabad

Heman Pathak
KGM, Dehradun

Avdhesh Gupta
IMSEC Ghaziabad

ABSTRACT

Mobile Agent (MA) technology is one of the most brilliantgrounds of scattered computing. Mobile agents are independent programs that wander the internet from machine to machine under their own control on behalf of their users to carry outexact predefined tasks. A mobile agent can postponed its execution at any point; relocate itself to another machine then start again execution at the new machine without any loss of state. This type of Mobile Agent can hold different types of data and that data should be sheltered from dissimilar types of attacks. Thus security is one of the most talented areas for the researchers functioning in the field of scattered computing. Stillplenty of research has been done in this area and a variety of solutions and approaches has been projected but still there is lots of scope to improve them or to set up new method to solve the security problem related to MA. This paper suggests a layered architecture to offer security to the hosting platform as well as to the MA. Architecture uses a variety ofconcept such as authentication, authorization, confidentiality, encapsulation, intrusion detection and trust & reputation. Here malicious hosts are identified according to their reputation and MA is allowed to be executed only on the trusted platform. Similarly, for the security of the hosts, only certified MA is authorized to be executed on host and its behaviour are observed by the platform. In this way proposed architecture not only protects its own environments but also guide other components of network to identify malicious hosts and MAs.

Keywords

Security,Trust and reputation,Mobile agent, Mobile Agent System.

1. INTRODUCTION

Mobile agents are mobile autonomous processes operate on behalf of users in a distributed computing environment. The autonomous agent concept has been proposed for a variety of applications on large, heterogeneous, distributed systems (e.g., the Internet) [1]. Due to the problems with security of Mobile agents have limited their popularity. Mobile agents are composed of code, data, and state. Agents migrate from one host to another taking the code, data and state with them. The state information allows the agent to continue its execution from the point where it left in the previous host. For example, a mobile agent could be migrated from the home platform with the task of buying an airplane ticket for its owner. The agent would visit all the known hosts of airline companies, one after another, to search for the most reasonably priced ticket, and then purchase one for its owner. Each time the agent moves to the next host, it summarizes the current state, execution pointer on the current state, etc., so that it can start searching for reasonable tickets on the next host. The state of the agent will contain a set of possible tickets to be considered for purchase. When the agent has finished its search, it may return to the host where it found the cheapest or best ticket and purchase it. [2]

There are different issues and challenges for deployment of mobile agent in real applications. These challenges become even more critical for MAS. Security is one of the challenges among them. In emerging technology of Internet, security issues are becoming more challenging.Use of the World-Wide-Web and Internet has become widespread in recent years and agent technology has proliferated at an equally rapid rate.

The paper is organized as follows. Section 2 gives a System Architecture for ensuring the security of mobile agents against illegitimate platforms and of Host by Mobile agents. Section 3 explains all the hardware and software components of the architecture. Section 4 explains the working process of the Model Architecture. Section 5 Shows the Analysis part and Finally, Section 6 gives some concluding remarks.

2. SYSTEM ARCHITECTURE

From my past experiences I recognized that MA security issue is a very crucial issue. Lots of research has been done on the security of MA but it's not enough. Still there is a need of a suitable solution for the security of in a Multi Agent environment. So we are providing a solution of security. The following shows the security architecture.

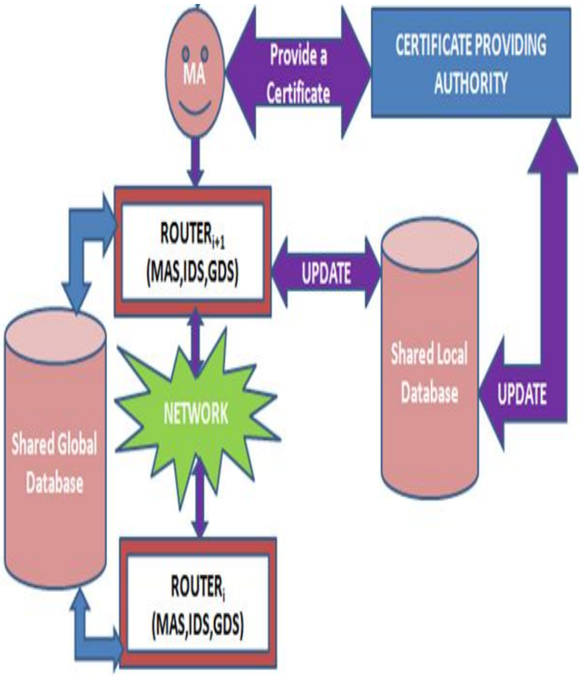


Fig 1 Security Architecture

The details architecture is shown in the figure below:-

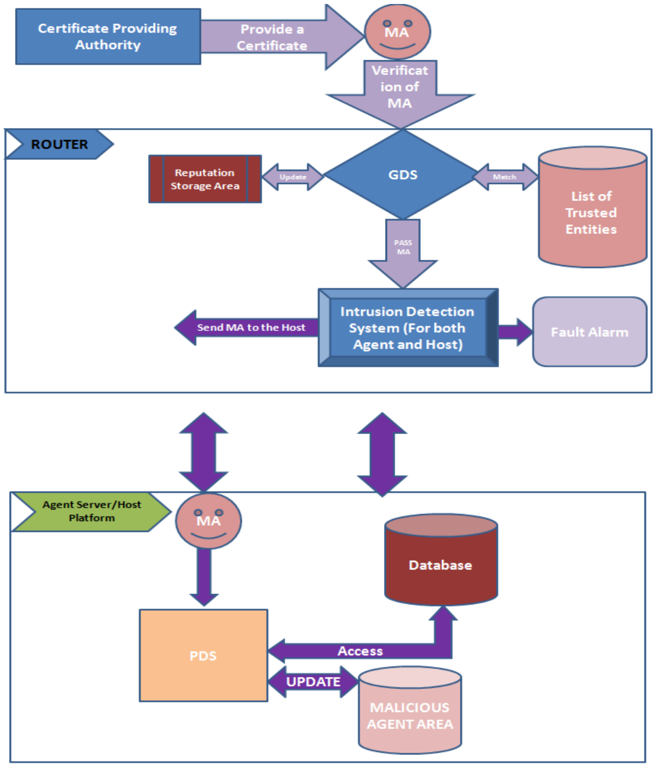


Fig 2: Detailed Architecture

3. COMPONENTS OF THE SYSTEM

The different components of the proposed architecture are as follows:-

3.1 Router

Each MA enters in to a local network or migrates from the network via router. Router is a centralized component within each network. It is responsible to detect a malicious host within the network. It also checks the status of incoming MAs as malicious or not and block the malicious MA within the network. In every 5 sec the list of trusted entities is updated on the router. This list is playing a role in the checking of the validity of the Trust Certificate of the MA. Software components other than MAS installed at router are GDS, IDS and FA [14].

Table 1: MA Table

MA_id	Host_id	Time	Rep_Counter	Expiry	Permission Type
111	101	5	0	10	Read
222	201	10	1	10	Write
333	301	15	2	10	Read/ Write

3.1.1Fault Alarm

It's a kind of indication to all the hosts inside a network that aparticular MA has been corrupted or and the platform visited by it also has been faulty.

3.1.2 GDS

GDS is a proxy server, installed at the router to handle all security related issues with the MAs. Log an arrival and departure entry into log table for each MA received and migrated from the network respectively. These log entry is used for recovery from a fault state. Responsibilities of GDS are: - [14]

- Collect the report for incoming MA from its source router as trusted or suspicious.
- Pass the MA to the target Host within the network.
- Alert the host, if MA is suspicious.
- Receive the MA from hosts within the network, ready to migrate from other part of network.
- Receive the behavioral report for each MA executed within the network from corresponding host.
- Create a status report for each MA executed within the network on the basis of behavioral report [10] as well as by analyzing check-pointed data saved at local shared storage space.
- If a MA is detected as malicious, block it within the network and inform its creator about it by sending message.

3.2 IDS

An IDS installed at the router is responsible to detect the malicious host and maintains a list of malicious hosts within the network. In order to detect the behavior of host, IDS randomly creates intruder MA and execute it on various hosts and record their behavior [15], [16], [17]. Based on the reports a host is tagged as Malicious by IDS. [14]

3.2.1 MAS/Agent Platform

The agent platform is one which is responsible for the creation of the mobile agent. The mobile agent that is produced is subject to the various processes in the model. The secure mobile agent is sent to the various parts of the system for further processing again and again before or after processing.

3.2.2 Certificate Providing Authority

To establish initial reputation level and prove its authenticity, every mobile agent is assumed to get registered with Certificate Providing Authority (CPA). For the transmission in the network MA have to first register itself to the CPA. According to [11], a Digitally Signed reputation Certificate is issued to an agent at the time of registration. It is only after registration that a mobile agent is able to access and provide services. According to the mobility of the network a trust certificate is issued to the MA by the router.

3.2.3 Local StorageDatabase (LDS)

LSDis a shared database by CPA and Router inside a network. This database contains the Agent Table, Log Table.

Table 2: Log Table

MA_id	Host_id	Dest. Router ID	Arrival/Departure
111	101	1	10
222	201	2	20
333	301	3	30

Table 3: Agent Table

MA_ID	Host_ID	Time
111	101	5
222	201	10
333	301	15

3.3 Global StorageDatabase (GSD)

GSD is a shared database by all the Routers in a global network. This database contains RouterTable, Log Table and AgentTable.

Table 4: Router Table

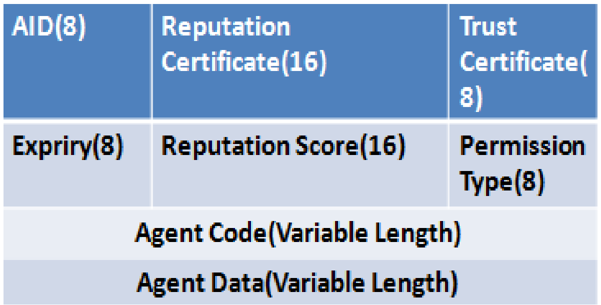
Router_ID	Network_ID	Network_Address
1	1000	192:168:12:44
2	2000	192:168:12:40

3.4 Agent Server/Host Platform

This is the real execution platform for the running o the MA's. All the components installed on AS are MAS and PDS. [4]

4.WORKING PROCESS

Initially the mobile agent is generated by the agent platform and the data it needs to carry is also allocated by the agent platform. From [12] the MA format is as follows:-



AID(8)	Reputation Certificate(16)	Trust Certificate(8)
Expriry(8)	Reputation Score(16)	Permission Type(8)
Agent Code(Variable Length)		
Agent Data(Variable Length)		

Fig 3: Agent Format

4.1 Agent Identifier

The agent identifier is the one which uniquely distinguishes the mobile agent. It is an 8 bit field which is being occupied by a unique number with respected to the system. [12]

4.2 Reputation Certificate

The Reputation Certificate is appended to the mobile agent by CPA. The authentication process uses this certificate. This part ensures the authentication services. The size of this field is of 16 bits.

4.3 Expiry Timer

The expiry time is set by the Route Marker which sets a time stamp which contains the maximum time limit for which the mobile agent must be alive. It is an 8 bit field.

4.4 Reputation Score

The **Reputation Score** is the creation of the Agent Platform. It shows the actual reputation value of the MA which indicates the how much times MA is successfully transmit the data. This is a 16 bit field. Initially its value is zero. But after registration its value will be increment by one.

4.5 Agent Code

Agent code is the actual code that the mobile agent is made of. It is the source code which is programmed to move from one host to another. The size of this field is variable and depends on the design of the system.

4.6 Agent Data

The data field is also a variable one which would contain the data the agent needs to carry in order to perform a task.

4.7 Permission Type

This field is attached by Agent Platform. It shows the type of access on the resources of the Host Platform. According to [13] three different types of permissions are read, write and read and write.

4.8 Trust Certificate

The Trust Certificate is appended to the mobile agent by Router. But it will be issued only when if the destination host will not lie in the same network. The size of this field is of 16 bits.

The mobile agent is subjected to encapsulation and Register_CPA when it gets off a system and is decapsulated when it enters the system. The encapsulation and decapsulation by different components are defined below. [12]

4.9 Communication between Agent Platform to CPA

We are dealing with a Multi Agent environment so An Agent Platform can launch multiple agents at the same time. For the communication between different hosts firstly a MA will register itself to the CPA.

Here the Agent platform encrypt the MA with its attributes by the public key of CPA i.e. K_{cpu}. Encryption Process is as follows:-

E_{Kcpu}**(AID, Expiry, Rep_Counter, PermissionType, Code, Data, DES_IP_Address)**

After then CPA will decrypt it with its private key i.e. K_{cpr}.Decryption Process is as follows: -

D_{Kcpu}**(AID, Expiry, Rep_Counter, PermissionType, Code, Data, DES_IP_Address)**

After Decryption CPA will verify the **Rep_Counter** and **SOURCE_IP_Address** .

4.10 Communication between CPA and Router

Now CPA will pass the MA to the Router inside the network. For their Authentication CPA provide a Reputation certificate to the

MA and also assign its ID to the MA and all these will be encrypted with original MA attributes by the public key of router K_{rpu}. When router will got the MA it will first scan the MA after ecryption by its private key i.e K_{rpr}. The encryption and decryption equations are as follows:-

E_{Kcpu}(AID, Expiry, Rep_Counter, PermissionType, Code, Data, DES_IP_Address,Rep_Certificate,CPA_ID)

D_{Kcpu}(AID, Expiry, Rep_Counter, PermissionType, Code, Data, DES_IP_Address,Rep_Certificate,CPA_ID)

After verification of the destination address it will assign the MA a trust certificate which shows the authenticity of the MA that means it is a part of the trusted network. For all these communication GDS and LDS are updated time to time. Our paper uses the concept of [14] and it tries to make it more secure.

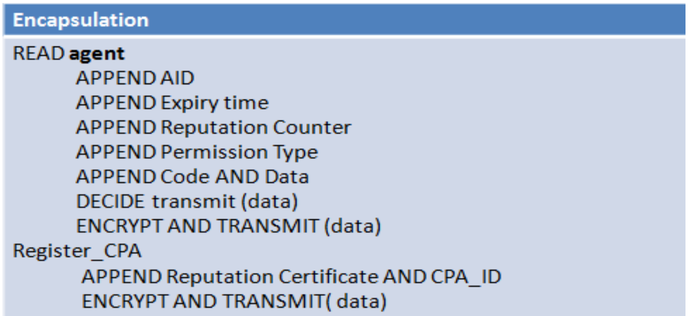
4.11 Communication between Router and Agent Server/Host

After verification the Rep_Certificate and Des_Address, Router sends this MA to the Host. According to the Destination Address GDS issues a trust certificate to the MA and pass this agent to the next router. The reputation table of an MA is shown below:

Table 7: - MA Reputation

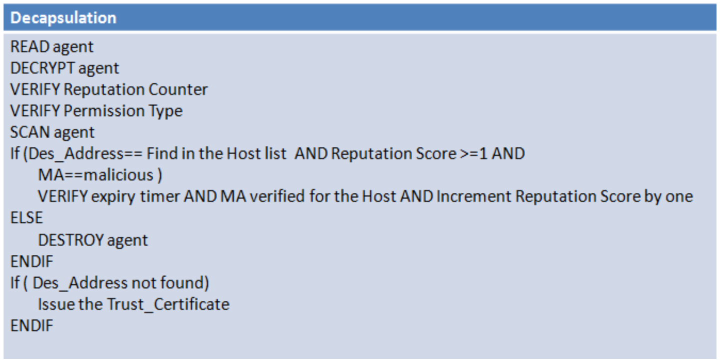
AID	MA Type	Reputation Counter	Remark	Activity
111	New Agent	0	No Access	Request for Registration to CPA
222	Registered MA	1	No Access	Request for Data Transfer to Network Router
333	Valid MA	>=2	Can Access	Transmit Data to Host

The whole Encapsulation and Decapsulation process is shown below:-



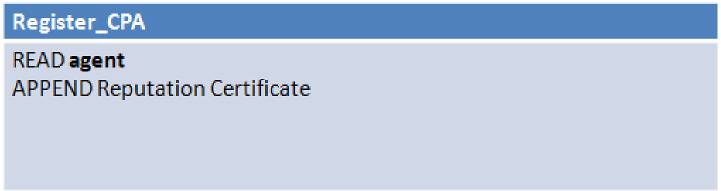
```
Encapsulation
READ agent
        APPEND AID
        APPEND Expiry time
        APPEND Reputation Counter
        APPEND Permission Type
        APPEND Code AND Data
        DECIDE transmit (data)
        ENCRYPT AND TRANSMIT (data)
Register_CPA
        APPEND Reputation Certificate AND CPA_ID
        ENCRYPT AND TRANSMIT( data)
```

Fig 4: Encapsulation



```
Decapsulation
READ agent
DECRYPT agent
VERIFY Reputation Counter
VERIFY Permission Type
SCAN agent
If (Des_Address== Find in the Host list  AND Reputation Score >=1 AND
    MA==malicious )
    VERIFY expiry timer AND MA verified for the Host AND Increment Reputation Score by one
ELSE
    DESTROY agent
ENDIF
If ( Des_Address not found)
    Issue the Trust_Certificate
ENDIF
```

Fig 5: Decapsulation



```
Register_CPA
READ agent
APPEND Reputation Certificate
```

Fig 6: -Register_CPA

5. ANALYSIS

Here we have proposed a new distributed mechanism for the security of the MA and the host. The two main components of our approach are CPA and Router. Both are playing a big role in the security of MA and Host. This new approach mainly focuses on trust and reputation modeling in multi-agent systems for a single or different network. The trust is a constraint that is commonly well-known between components and imposes impact on their one to one assistance.

Trust represents the level of consistency that agents have concerning the type and quality of information or service that is provided by other agents [5]. Although the measured trust might not reflect the actual credibility of agents, agents still need to evaluate this constraint to make judgments [6, 7]. Moreover, agents utilize trust-oriented learning approaches [8] that take into account past interactive experiences. The reputation parameter is a reason that an agent holds as a means to attract other agents in order to communicate and coordinate with them. Reputation represents the level of fame that an agent has and this value is attained with admiration to the mobile agent's honest actions regarding other agents in the surroundings [9].

For maintaining trust Router issues a trust certificate with its id to the MA. But before issuing a trust certificate it will check its reputation certificate issued by the CPA and the CPA_ID encrypted by the CPA. After decryption if the destination IP address is of the same network then it will increment the reputation counter of the MA and pass it to the destination host and also update the Local shared Database. Reputation shows the real reputation of an agent in the network similarly for trust MA shows that it is trust worthy for a network [10]

Step by step communication is done here with security checking mechanism.

5.1 Security of MA

In the proposed architecture, host is secured from the attack of malicious MA by implementing various strategies. [14]

- A MA is when arrived at router; GDS gets its report from its source router and passed it to local host.
- PDS installed at host creates a thread to watch MA behavior.
- MAS are then provided the execution environment to the MA to access the open database and other open resources.
- If MA tries to access the protected data or resources, Security Manager checks its identity and allows accessing only after authentication.
- If MA is trying to access the protected data/resources without proper authorization, its behavior is observed and reported by PDS.
- Since MA could not pass the verification by SM, DS will not allow the accessing of protected data and maintains the security.
- Resources are also available to visiting MA for limited period of time, if it is consuming resources such as CPU time, memory and others for more than expected time then PDS report its behavior and can terminate its execution.
- Checkpoint data is then used to bring the host in a consistent state as all execution by MA is roll-backed.

5.2 Security of Mobile Agent

A MA carries with it code and data. Since code is read only therefore it is not difficult to insure its security. Simple digital locking and unlocking with public and protected key concept can be used to make code secure. So, I am not discussing the security of code part of MA here.[14]

In order to protect the data, encryption technique is used. All the data carried with MA is encrypted. Encrypting algorithm is part of the MA code. The code of MA always encrypt the data before completing its execution at a host and latter when it start its execution at other host it first decrypt the data then resume execution. Since code is protected and could not alter, data is also get protected. If code has been found altered, MA execution should not allowed by the MAS.

Some of the MAs are launched with the objective to gather information while some are to perform certain tasks over the network. On this basis MAs may be tagged as Read Only, Write only or R/W MAs.

5.2.1 Read Only

These MAs can read data from any host but cannot write anything to the database. Such MAs cannot corrupt the database at the server and may simplify the security checks while executing at a Host.

5.2.2 Write Only

These MAs has been launched with the purpose to perform certain tasks over the network but does not collect any data and need not to be modified. So, data part of it is read only and can be protected easily as code.

5.2.3 Read/Write MAs

They are the general MAs which may write as well as their data may also be modified.

Reading MA requires to access only open data does not require any authorization while all other MA must carry certificate of authorization with them and their user (launcher) must have signed the agreement with the host.

Since MA is a small piece of code move freely under its own control over the network, so it is not possible for MA to suspect or detect a host as faulty. Some other components on behalf of the MA should do the task of detecting the faulty host. Every router maintains a list of faulty host, if an incoming MA tries to visit a faulty host, it is not allowed to visit it, and if an alternative host is available in MA itinerary, it is passed to it.

At the host, before executing the actual code MA first executes the sample code to check if host is responding properly or not. If it founds host faulty, it stops its execution and report this. Otherwise continues the execution of MA. For the security of MA, IDS is installed on the Router. The work of IDS has been described in [14]. Here FA is also working to alert the entire hosts inside the network that the host is not fault free.

6. CONCLUSION

To resolve the problem of mobile agent's security, especial on attacks on mobile agent data and Host, paper analyzed current protection mechanism and put forward security architecture to enforce its security with the concept of cryptography. In this paper we have proposed a security architecture which reasonably secure the MA and Host both from malicious attack. Different components of the system work cooperatively to provide the solution to the security problem. Here we are not implementing or modeled the proposed architecture yet. Its practicality is still to be tested. But the analysis shows that Trust and reputation enhanced cryptography can protect data of roaming mobile agent effectively and realize some security needs such as data confidentiality, integrity, and anonymity and also protect the Host. Different approaches has used in this paper. All of these are well known techniques and these techniques have been implemented successfully.So it is relativelypractical to admit that, this architecture once implemented will resolve the concern issues successfully. Its effectiveness or relative performance investigation is possible only after the implementation which we will solve in our next paper.

7. REFERENCES

[1] Neelesh Kumar Panthi, Ilyas Khan, Vijay k. Chaudhari “Securing Mobile Agent Using Dummy and Monitoring Mobile Agents” Department of Information Technology, T.I.T. Bhopal, India.

[2] Bharti Chouksey, Ravi Mohan, Rajneesh Argawal & Dushyant Sharma,"Security Of Mobile Agents On Network For Distributed Database" published in IJREAS Volume 2, Issue 2 (February 2012) having ISSN: 2249- 3905.

[3] Li An Qiangfeng Jiang Xiaoping Luo Zhaohui Ren Spring, 2002 “Protecting Mobile Agents against Malicious Hosts".

[4] G.Geetha , C.Jayakumar,"Trust Enhanced Data Security in Free Roaming Mobile agents Using Symmetric Key

cryptography published in International Journal of Network Security & Its pplications (IJNSA), Vol.3, No.5, Sep 2011

[5] E.M. Maximilien, and M.P. Singh. Conceptual model of web service reputation. SIG-MOD Record 31(4):36-41, 2002.

[6] B. Khosravifar, M. Gomrokchi, J. Bentahar, P. Thiran. Maintenance-based trust for multi-agent systems. In Proceeding of 8'th International Joint Conference on Autonomous Agents and Multi-Agent Systems, pp. 1017-1024, AAMAS 2009.

[7] S. P. Marsh. Formalising trust as a computational concept. PhD thesis, University of Stirling, 1994

[8] T. Tran and R. Cohen. Improving user satisfaction in agent-based electronic marketplaces by reputationmodeling and adjustable product quality. In Proceedings of the 3'rd Interna-tional Joint Conference on Autonomous Agents and Multi-Agent Systems, pp. 828-835, AAMAS 2004.

[9] B. Yu and M.P. Singh. An evidential model of distributed reputation management. Pro-ceeding of the International Joint Conference on Autonomous Agents and Multi-Agent Systems, pp. 294-301, 2002.

[10] Babak Khosravifar,"Trust and Reputation in Multi-Agent Systems A Thesis", Department of Electrical and Computer Engineering,Concordia University April 2012

[11] Singh,A., Juneja,D., and Sharma,A.K.: Elliptical Curve Cryptography Based Security Engine for Multiagent Systems Operating in Semantic Cyberspace. In International Journal of Research and Review in Computer Science (IJRRCS), Vol. 2, No. 2, April 2011.

[12] P. Marikkannu, J.J. Adri Jovin, T. Purusothaman, "An Enhanced Mobile Agent Security Protocol", European Journal of Scientific Research, ISSN 1450-216X Vol.51 No.3 (2011), pp.321-331, EuroJournals Publishing, Inc. 2011, http://www.eurojournals.com/ejsr.htm

[13] Aarti Singh, Parul Ahuja," Robust Algorithm for Securing an Agent Hosting Platform", International Journal of Advancements in Technology http://ijict.org/,ISSN 0976-4860

[14] Dr. Heman Pathak,"Hybrid Security Architecture (HSA) for secure execution of Mobile Agents" 2004.

[15] Wu, Y.S., Foo, B., Mei, Y., Bagchi, S.: Collaborative intrusion detection system (cids): A framework for accurate and efficient ids. In: Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC'03). (2003)

[16] Faukia, N., Hassas, S., Fenet, S., Albequerque, P.: Combining immune system and social insect metaphors: A paradigm for intrusion detection and response system. In: Proceedings of the 5th International Workshop for Mobile Agents for Telecommunication Applications. (2003)

[17] Li, C., Song, Q., Zhang, C.: Ma-ids architecture for distributed intrusion detection using mobile agents. In: Proceedings of the 2nd International Conference on Information Technology for Application (ICITA 2004).