International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 11 154 – 159

Cryptography Based Hybrid Security Architecture for Mobile Multi Agents

Swati Singhal
Research Scholar, Dept of Computer Science
Gurukul Kangri University Haridwar
aggarwalswati37@gmail.com

Heman Pathak
Associate Professor, Dept, of Computer Science
Gurukul Kangri University Haridwar
hemanp@rediffmail.com

***Abstract*—** Distributed Computing is the current area of research. Many researchers are working in area of Distributed Computing and trying to find a solution for the security and other issues. In Distributed Computing the mobile agents are the very important thing. When different mobile agents work in the same environment simultaneously it becomes a very important issue. Mobile agents have automatic, pro-active, and dynamic problem solving behaviors. However, scope of this paper is limited to analyze the existing security approaches for Mobile Multi Agent System. Security issues of mobile agent address the problem of securing and protecting agents from the attack of malicious hosts and other agents as well as securing the host from attack of malicious agents. This paper introduces a new approach of security for agent from other agents. Paper discusses Cryptography Based Hybrid Security Architecture with trust and reputation named CBHSA. It breaks the security of MA in two parts. The first level of security is work on the MA and second level of security is maintained on network. The model CBHSA, its different components and security of MA during movements around the network are discussed in this paper. This paper emphasis on the security of MA's during migration within the network or outside the network.

Keywords: *Mobile Agent (MA), Mobile Agent System (MAS), Multi Agent System (MUS), Security, Intrusion Detection System (IDS)*

*****

I. INTRODUCTION

MA is a process that can transport its state from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. MA is robust & autonomous. It supports disconnect computing which is not only reduces bandwidth consumption but also moderates the effects of high latency. MUS is a system composed of multiple interacting intelligent agents. It contains multiple MAs launched by same user or by different users or combination of MAs and software agents.

Basically, the security requirements of any computer system are confidentiality, integrity, authentication, authorization, non-repudiation and availability [1][2][3]. A malicious host environment can compromise the security requirements of a MA in a number of ways. This includes denial of service, eavesdropping, interception, alteration, replays and masquerading [1, 4, 5, 2, 6]. While techniques such as access control, password protection and sand boxes have been developed to protect MA platforms against hostile agents [7], none of the approaches adequately addresses every aspect of security [8]. Security for MA environment is a complex problem and requires a multifold solution. This paper proposes a new security framework which combines various existing approaches such as reputation based trust management, Intrusion Detection System (IDS) based approach, behavior analysis and cryptography based encryption etc. Cryptography based encryption with different keys plays major role for secure migration of MAs in the network.

II. SECURITY IN MULTI AGENT SYSTEM

Since the codes of MA are executed on remote platforms, security concerns arise to protect the MAs if the remote platforms are malicious. On the other hand, there are threats to host if the MA is malicious. In MUS agents can attack other agents as well. Malicious MA may attack the hosts (platforms), which enables it to execute. Various types of attacks in MA environment can be broadly classified as: [21]

Table: Types of Threats

Agent to Host	Agent to Agent	Host to Agent
Masquerading	Masquerading	Masquerading
Denial of Service	Denial of Service	Denial of Service
Eaves Dropping	Unauthorized access	Unauthorized access
Alteration	Repudiation	Damaged to host resources

III. LITERATURE SURVEY OF DIFFERENT SECURITY ARCHITECTURE

Every MA needs an environment to execute itself which is known as MAS. Various MAS have been developed or are under development in various university research groups or industrial companies. Some of the MAS developed so far are – SOMA, Ajanta, Concordia, AGENT TCL, Wave Secure System (WSS), MANSION FRAMEWORK, Aglet and many more.

In [9] Researcher focuses on security & interoperability and describes a Secure and Open Mobile Agent (SOMA) programming environment. SOMA is based on a through security model and provides a wide range of mechanisms and tools to build and enforce flexible security policies. This framework permits to interoperate with different application components designed with different programming styles.

In [10], Ajanta's (a Java-based system for MA programming) security architecture has been describe. It provides mechanisms to protect server resources from malicious agents, MA data from tampering by malicious servers, and to protect the system infrastructure itself. An MA can carry three kinds of protected data: read-only objects, objects visible only to specific servers, and a secure append-only list of objects.

In [11], researcher proposed an authentication mechanism to guarantee that the MA only executes in a trust environment to prevent attacks. They proposed some security goals and proposed architecture to achieve these goals. A unique aspect of the architecture is the "State appraisal" mechanism that projects users and hosts from attacks through state modifications and that provide users with flexible control over the authority of their agents.

In [12], researcher proposes a two non-detachable signature schemes using RSA and computed with encrypted functions. The undetectable signature scheme allows the MA to sign a message without revealing the secret key. A MA acts as a

delegate of its creator application and executes on behalf of its owner. Each MA carries a set of credentials which compose the MA's identity and public key certificate. The creator may delegate to the MA only a limited set of privileges while working on its behalf. Such access restriction is encoded in the credentials. When a server receives a MA, it uses these credentials to validate the authenticity of the MA, and based on the MA's identity and delegated rights, it can grant access privileges for its local resources.

J. Y. Park et al. [13] announced a new key generation scheme called one time key based system. This system uses, computations to generate a key at each node using information received from previous hosts. Only, the originator is able to decode the information since he had the initial value. The main strength and weakness of this system is that there is an interrelationship among consecutive MA keys. Therefore, in case that some intermediate MA data or key are get tempered or deleted then the whole system will fail.

In [14] Researchers have proposed Mobile Agent Distributed Goal Satisfaction (MADGS) system. They implemented two separated models, first model explores the user of JINI to provide security to MA environment and the second one builds a separated security component inside MADGS. They enforce the security polices from these two models on the main functions of MADGS including the MA migration and communication. They empirically compare these two models based on their performances, integrity and scalability.

In [15], researchers describe a peer-to-peer distributed-computing platform based on MAs. The platform, called yaca, has been built on top of Aglets, MA platform written in Java. Next to the client agents, who seek computational resources in a cluster, yaca consists of four agents, who manage the computers within a cluster. (1) The Directory Agent keeps track of the computers belonging to the cluster. These computers are called nodes. (2) The Weather Agent monitors the status of a node and (3) The Account Agent keeps track of the resources used by client agents. (4) The Controller Agent manages a single node. It controls the access to the node and responsible to shift client agent to other nodes in the cluster in case of overloaded.

IV. CRYPTOGRAPHY BASED HYBRID SECURITY ARCHITECTURE (CBHSA)

This paper proposes a new security framework which combines various existing approaches. Proposed framework has been named as Cryptography Based Hybrid Security Architecture CBHSA which is inspired by Hybrid Security Architecture (HAS) proposed in [16]. This section of paper explains the assumptions, requirement and working of CBHSA.

A. Assumptions and Rrequirements

CBHSA has certain assumptions/system requirements, which has been summarized here.

- Internet is network of networks (Local) where two networks are connected with each other via router. Routers are assumed to be fault free.
- MAS or platform is installed on router but it is only responsible to receive, check and forward the MAs not to execute them.
- In each Local Area Network (LAN), there are various Agent Servers (AS) or Hosts communicate via communication services designed to work in LAN. MAS is installed on each Agent Server/Host.
- In each network there is a shared Local Storage Space (LSS), which is assumed to be fault free and accessible by all hosts and router of the LAN.
- It is also assumed that there is a Global Storage Space (GSS) maintained by one of the router and accessible by all routers. It is assumed to be fault free and used to maintain Global Reputation Table (GRT) of malicious MAs.

B. System Components

System model used by the framework proposed in the paper is consisting of three main hardware components Router, Hosts, LSS and GRT. Various software components installed on each hardware components of the system are explained in the following section.

1) Router

Routing is the process of forwarding MA from one network to another but in the proposed framework, router plays key role to provide security to both hosts and MAs from various attacks. Components installed on the router are listed here.

a) Intrusion Detector System (IDS)

An IDS installed at the router randomly creates intruder detectors (ID) and execute it on various hosts and record their behavior. Behavior report is then analyzed and RV is updated for host.

b) Logging Manager (LM)

This s/w routine is responsible for Log an arrival and departure entry in log table for each MA received and migrated from the network respectively. These log entries are used for tracing the MA path and for recovery from a fault state.

c) Trust Manager (TM)

This s/w routine installed on router is responsible for computing reputation value (RV) for all incoming and outgoing MA via router. It also maintains the reputation value of the hosts, part of the network [23][24].

d) Migration Manager (MM)

This s/w component is responsible for the secure migration of MA from one host to another host within the network or outside the network. It is basically used for the encryption and decryption process. If MA migration is local then authentic and confidential cryptographic encryption is used for MA transmission and if migration is Global then MAC function is used for encryption technique using the public and private key of router.

e) Mailbox Manager (MBM)

Once MA is found trustworthy, Every time MA arrives at MBM it checks the target address of MA, if the next host is within the network it save its mailbox at LSS and the remaining part of MA is forwarded to the MM for further encryption process. If the next host does not exist within the network then it attach mailbox with MA and again send it to the MM for encryption process.

f) Recovery Manager

This s/w routine installed at router is responsible to initiate recovery procedure in case a MA or host is found malicious. Recovery procedure is quite complex and lots of policy and

legal issues are involved with it, so I am not discussing them in this paper but left for future work.

2) Host

Host is a computer in the network which offers services to the MA. It provides executing platform to the MA. A MA is passed to be executed on a Host only if both MA and host are found trustworthy. To ensure the trustworthiness of both, some of the security components are installed at the host. Following section discuss these components.

a) Personal Domain Server (PDS)

PDS is a proxy server, installed at each Host. It maintains a thread to watch the behavior of the host. When a MA is arrived at a host for execution, it starts threads to record the behavior of MA and executing platform. Executing After the execution of MA, it prepares and store reports for at the local shared storage space.

b) Checkpoint Manager (CM)

This is responsible to save the MA and its execution state to LSS periodically and after every successful transaction. This checkpoint data can be used to recover the host in case it has been attacked by the malicious host. These data can also be used to recover the MA in case malicious host attacked it.

3) Local Shared Storage Space (LSSS)

Each network is assumed to maintain a fault free storage space. This space is accessible by all hosts and components installed at router. It is used to store Log Table, behavior report of MA and Hosts, reputation table for MA and hosts.

4) Global Reputation Table (GRT)

This table maintains the list of MAs and their RVs that have been found suspicious or malicious by some watching entities. This table is concerned only when information gathered locally or from source router of MA is insufficient to make decision about the RV of the MA.

C. CBHSA Description and Working

CBHSA uses the existing technology to serve our purpose [16]. A MA wishes to visit a host within a network, first arrive at the router of the network and then only pass to the designated host. Host in a network offer services and provide an executing environment to the MA to be executed. CBHSA consists of agent migration, code integrity verification, data collection, encryption –decryption and signing. CBHSA framework provides the full security approach for both agents and Hosts. Figure-1 shows the basic architecture and different components of CBHSA. According to the type of security, it is divided into three main parts:

1) Security of Host from Agent

To secure the hosts from attack of malicious MAs, MA reputation is maintained in the Local Reputation Table (LRT). The RV for a newly created MA is same as the RV of its base host. For an incoming MA, TM collects the RV of the MA from the last visited router. LRT for MA is also consulted to get the RV of incoming MA if it has previously visited the network. If these data are not sufficient then GRT is consulted to check whether MA has been tagged as suspicious or malicious by any of the entities. TM then analyzes these data and compute new RV for the MA and if found trusted, passed to the target. If MA is found malicious, GRT is updated and MA is transferred to Recovery Manager. During the execution of MA its behavior is observed by PDS. TM is responsible for analyzing this report and to update the RV of the MA in the LRT. [22]

2) Security of Agent from Host

In order to secure MAs from the attack of malicious host, MAs are allowed to be executed only on trusted Hosts. Each host is initially assigned an average RV five (5). Behavior of host is watched by its PDS and executing MAs. IDS installed at router periodically launch Intruder Detectors (ID) to record the behavior of hosts. These Behavior reports are used to update the RV of host. Host RV is computed locally and stored in HRT. TM allows trusted MA to be executed on trusted hosts. [22]

3) Security of Agent from another Agent

In MUS, MAs communicate each other via dropping messages in mailbox of target MAs. MA always carries its Mailbox with it. While MA is executed on a host, its Mailbox resides at the local router. When a MA wants to send a message to the mailbox of target MA, it will first locate the location of other MA. [23,24,25] whenever the location is found by MA, it will encrypt the message with the target MA's public key and the whole message is encrypted with the router's public key and drop this message to the mailbox of target MA on the target router. This two way encryption provides the security to the message. After getting the message, router will first decrypt the message using its private key and then the whole encrypted message has been dropped in the mailbox. Whenever MA wants to see the message it will use push approach. In the decryption process, MA first decrypt the mailbox using its private key and then decrypt the message with its private key and then check the authenticity of Message using the agreement associated with the message shown in fig 3. [25][26]

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries [18]. For the security purpose encryption and decryption are used. Encryption is the process of encoding messages or information in such a way that only authorized parties can read it [19] and decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. [20] These encryption and decryption are possible with the help of some keys. Keys can be private and public. 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. A MA contains eight parts Source Host Id $\mathbf{BH_{id}}$, Itinerary of MA $\mathbf{IT_0}$, Data $\mathbf{d_0}$, Code $\mathbf{C_0}$,execution state $\mathbf{ES_0}$, Mailbox $\mathbf{M_0}$ and MA Id for communication $\mathbf{MAC_{id}}$, and Base Host id of the communicated MA $\mathbf{BAC_{id}}$ shown in fig 2.

$$\mathbf{MA\ (BH_{id},\ IT_0,\ MA_{id},\ d_0,\ C_0,\ ES_0,\ MAC_{id},\ BAC_{id},\ M_s,\ M_0)}$$

Then BH makes signature on Code, Data and Execution State using MA private Key.

$$\mathbf{S_0 = E\ (PR_{MAi},(d_0,C_0,\ ES_0))}$$

There can be three types of communication among hosts.

a) Host to Router

In Host to Router MA transmission, the complete MA is encrypted with the public key of Router after then a complete message is sent to the Router with the source and destination ids of hosts.

1. The complete MA is

$$(BH_{id}, IT_0, MA_{id}, d_0, C_0, ES_0, MAC_{id}, BAC_{id}, M_0)$$

2. After Signing the code part MA is

$$C= (H_0||(H_1,H_2\ldots.H_n)||MA_{id}||d_0||Sig(C_0)||ES_0||MAC_{id}||BAC_{id}||M_0||PR_{MAi})$$

3. Encrypt the complete MA using public Key of Router R_i

$$M_0 = Enc (PU_{R0}, C)$$

4. Sent source Id, Destination Id and M_0 to Router now it will find the next host to send packet.

$$H_0 \text{---}\rightarrow R: (S, D, M_0)$$

b) Router to Host

In this type of communication every time the packet is encrypted with Host public key. So that confidentiality is achieved.

1. First PDS decrypt the message with the private key of host.

$$C = Dec (PR_{H1}, M_0)$$

2. After decryption, MA performs its assign task and again encrypted with the router's public key by the PDS. Now PDS finds the Next Host to Migrate M_0. Next Host can be part of local and global network.

$$M_1= (H_1||(H_2, H_3\ldots.H_n)||MA_{id}||S_0||MAC_{id}||BAC_{id}||M_0||PR_{MAi})$$

$$M= Enc (PU_{R0}, M_1)$$

3. Sent source Id, Destination Id and M_0 to MBM on router now it will find the next host to send packet.

$$H_1 \text{---}\rightarrow R: (S, D, M_1)$$

c) Router to Router

In the Global network, two Hosts can communicate with each other using a MAC Function. Confidentiality and Authentication are two necessary things for a secure communication. This case provides confidentiality and authentication both.

1. Suppose a Host doesn't exist inside the network. So MBM on Router first attach the mailbox of MA with it and will send the Message to the router using MAC functions. Here two separate keys (K_1 and K_2) are needed, each of which is shared by the both routers.

2. The MAC is calculated with the message as input and is then concatenated to the message. The entire block is then encrypted. It is preferable to tie the authentication directly to the plaintext as shown in Fig 5

3. On Router R_1 message is decrypted using shared key K_2 and then again MAC function is applied on the message using shared key K_1.

4. Finally both the messages are compared.

D. Work Flow of CBHSA

The work flow of CBHSA is shown in figure 6 and 7.

V. CONCLUSION AND FUTURE WORK

This paper introduces the cryptography based Hybrid security architecture for mobile multi agent system. This system deals with the security of hosts and Agents. For the security of hosts IDS has been used. IDS identify the malicious behavior of host. In CBHSA, only trusted MAs are transferred to the host so host gets protected from the attack of malicious MA. During the execution, behavior of MA is recorded and CM saves the MA and its execution state in the LSS periodically. In case MA attacks the host during execution, this attack can be detected and RM can use the checkpoint data to bring the host in consistent state. Since MA is allowed only to be executed on trusted host, it gets protected from the attack of the malicious host. Even during the execution if it has been attacked, RM can rollback all MA execution and recover it from checkpoint data.

MA is a moving entity and may be captured and altered while on the way in local and global network so in order to protect MA from attack of malicious entity during transmission, MA is always transmitted in the encrypted form various types of encryption are used for different communication channel. During the migration from host to router and router to host in local area network public key cryptography has been used and from router to router in global network MAC function based cryptography has been proposed. When two MA wants to communicate with each other then source MA sends message to be dropped in mailbox of target MA. For the security purpose mailbox of the MA as well as message during transmission are send and stored in encrypted form as discussed in the paper.

Hence this paper provided full security framework for the MA during migration among the network. All the components of the architecture have been explained in this paper. Various components of the system work collectively to provide solution to the said problem. The approach discussed in this paper models a variety of trust relations, and allows a mobile agent system to be used effectively even when some of the parties stand in a competitive relation to others. Since the proposed architecture has been implemented or modeled by Color Petri net Tool (CPN) but its practicality is still to be tested. Most of the approaches used in this paper are well known and has already been implemented successfully. Its efficiency or comparative performance analysis will do in our future work.

REFERENCES

[1] Dadhich, P., Dutta, K., Govil, M. C. (2010) 'Security Issues in Mobile Agents', International Journal of Computer Applications, 11(4), pp. 1-7.
[2] Ahmed, T.M. (2013) 'Protect Mobile Agent Against Malicious Host Using Partial-Mobility Mechanism', International Journal in Foundations of Computer Science & Technology (IJFCST), 3(6), pp. 41-52.
[3] Singh, D., Thakur, A., Gupta, D. (2015) 'A Review of Mobile Agent Security', International Journal of Advanced Research in Computer Science and Software Engineering, 5(2), pp. 188-190.
[4] Pai, P., Shinde, S.K., Khachane, A.R. (2012) 'Security in Mobile Agent Communication', International Journal of Advanced Engineering Research and Studies, 1(4), pp. 74-80.
[5] Mahmoodi, M., Varnamkhasti, M. M. (2013) 'A Secure Communication in Mobile Agent System', International Journal of Engineering Trends and Technology (IJETT), 6(2), pp. 186-188.
[6] Ahmed, T.M. (2009) 'Using Secure-Image Mechanism to Protect Mobile Agent against malicious Hosts ', International Scholarly and Scientific Research & Innovation, 3(11), pp. 364-369.
[7] Lee, H., Alves-Foss, J., and Harrison, S. (2004)'The Use of Encrypted Functions For Mobile Agent Security'. Hawaii International Conference On System Sciences. Hawaii: DARPA. 1-10

[8] Shrivastava, R., Mehta, P. (2012) 'Securing Mobile Agent And Reducing Overhead Using Dummy And Monitoring Mobile Agents', International Journal of Management, IT and Engineering, 2(4), pp. 296-303.
[9] Bella vista, P., Corradi, A., Stefan Elli, C., "Protection and Interoperability for Mobile Agents: a Secure and Open Programming Environment," IEICE Transactions on Communications, Special Issue on "Autonomous Decentralized Systems", Vol. E83-B, No. 5, May 2000, pp. 961-972.
[10] Tripathi, A., Karnik, N., "A Security Architecture for Mobile Agents in Ajanta", Proceedings of the International Conference on Distributed Computing Systems, April 2000.
[11] Farmer, W., Swarup, W., "Security for Mobile Agents: Authentication and State Appraisal," LNCS-Research in Computer Society, Vol. 1146, Springer Verlag, 1996, pp. 118-130.
[12] Sander, T., Tschudin, C.F., "Protecting Mobile Agents Against Malicious Hosts," LNCS-Mobile Agent Security, Vol. 1419, Springer Verlag, 1998, pp. 44-60.
[13] Jong-Youl Park, Dong-Ik Lee, Hyung-Hyo Lee, "Data Protection in Mobile Agents: One-Time Key-Based Approach," is ads, Fifth International Symposium on Autonomous Decentralized Systems, 2001, pp 411.
[14] Feng Zhang, Markus Kaiser, Hien Nguyen and Shu Wang," Security and Agent based Computing environment" Department of Computer Science Engineering, University of Connecticut.
[15] S. Pleisch," State-of-the-art of Mobile Agent Computing: Security, Fault Tolerance, and Transaction Support", Research Report, IBM Research, Z. R. Lab. Switzerland, 1999.
[16] Heman Pathak," Hybrid security architecture (HAS) for secure execution of mobile agents" Published in the proceeding of the ICCCS(International Conference on Communication, Computing & Security) in 2011,Pages 499-502.
[17] Pathak H., Garg K., Nipur, 2010. Comparative Performance of Hierarchical Fault Tolerance Protocol for Mobile Agent Systems. International Journal of Information Technology and Knowledge Management with ISSN No 0973-4414, January, 2010.
[18] From the web through link https://en.wikipedia.org/wiki/Cryptography.
[19] From the web through link https://en.wikipedia.org/wiki/Encryption.
[20] From the web through link http://www.computerhope.com/jargon/d/decrypti.htm.
[21] Adri Jovin J.J. and Marikkannan M.,"A Review on Attacks and Security Approaches in Mobile Agent Technology, Research paper published in Australian Journal of Basic and Applied Sciences ISSN:1991-8178 EISSN: 2309-8414, Journal home page: www.ajbasweb.com.
[22] Dr. heman Pathak," Colored Petri Net (CPN) based Model for Hybrid Security Architecture based on Reputation for Secure Execution of Mobile", research paper published in International Journal of Appli cation or Innovation in Engineering & Management (IJAIEM),Web Site: www.ijaiem.org Email: editor@ijaiem.org,Volume 5, Issue 1, January 2016 ISSN 2319 – 4847
[23] Jean Evens, Jiao Yu, and Hurson Ali R., 2007. Addressing Mobile Agent Security through Agent Collaboration. Journal of Information Processing Systems, Vol.3, No.2, December 2007 43 10.3745/JIPS.2008.3.2.043.
[24] K. Hoffman, D. Zage, C. Nita-Rotaru, A survey of attack and defense techniques for reputation systems, ACM Computing Surveys 42 (1)(2009) 1–31.
[25] jiannong cao, liang zhang, xinyu feng+ and sajal k. Das++,"path pruning in mailbox-based mobile agent communications",research paper published in journal of information science and engineering 20, 405-424 (2004).
[26] Xinyu Feng, Jiannong Cao, Jian Lü, and Henry Chan,"Efficient Mailbox-Based Algorithm for Message Delivery in Mobile Agent Systems", G.P. Picco (Ed.): MA 2001, LNCS 2240, pp. 135-151, 2001.© Springer-Verlag Berlin Heidelberg 2001.
[27] Swati Aggarwal, Dr. Heman Pathak,"Modelling of Hierarchical Location Management Schemes to Locate Mobile Multi Agents using Coloured Petri Net ",research paper published in IEEE explore through International Conference on Advances in Computer Engineering & Applications (ICACEA-2015), IMS Engineering College, Ghaziabad, UP, India.
[28] Swati Aggarwal, Dr. Heman Pathak,"Improved Hierarchical Location Management Schemes to Locate Mobile Agents in Multi Agents Environment", research paper published in IPASJ International Journal of Computer Science (IIJCS) Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm, Volume 2, Issue 10, October 2014 ISSN 2321-5992.
[29] Heman Pathak, Swati Aggarwal," Performance Analysis of Hierarchical Location Management Scheme to Locate mobile Agents", International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016, ISSN (Online) 2278-1021ISSN

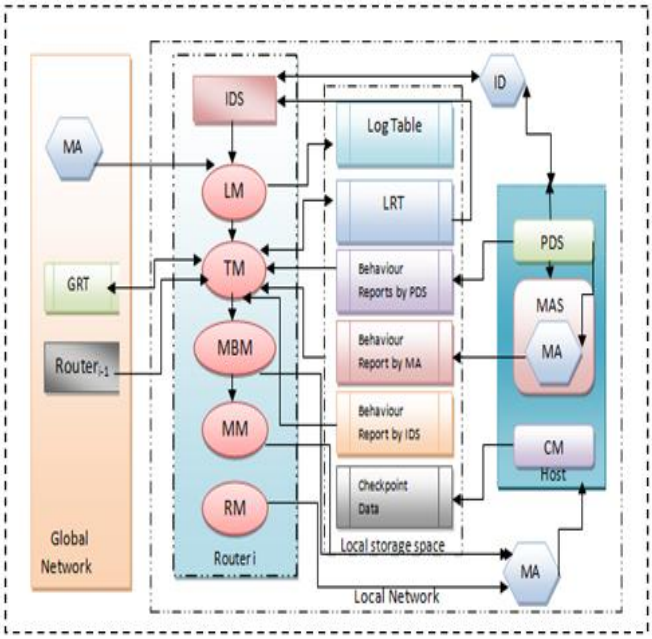

Figure 1. Fig 1: Interaction of between components of CBHSA to compute RV

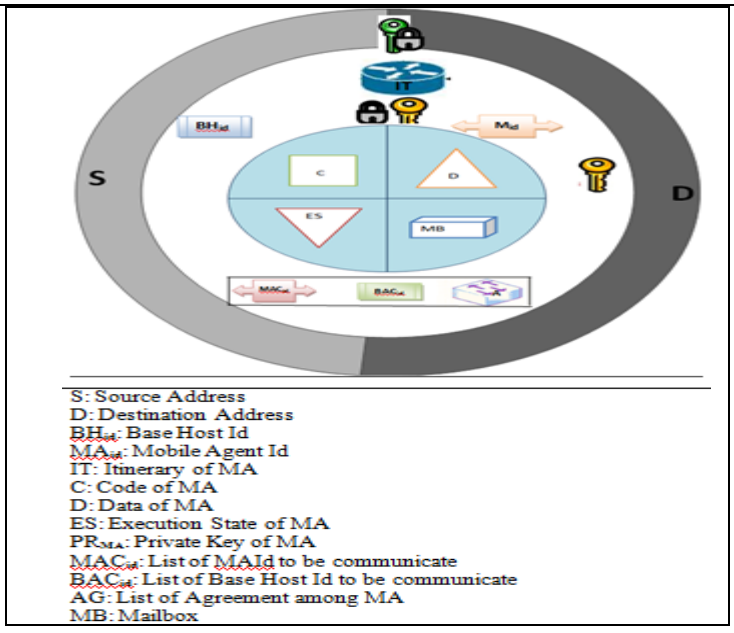

Figure 2. Fig 2: Components of MA

ISSN: 2321-8169
154 – 159

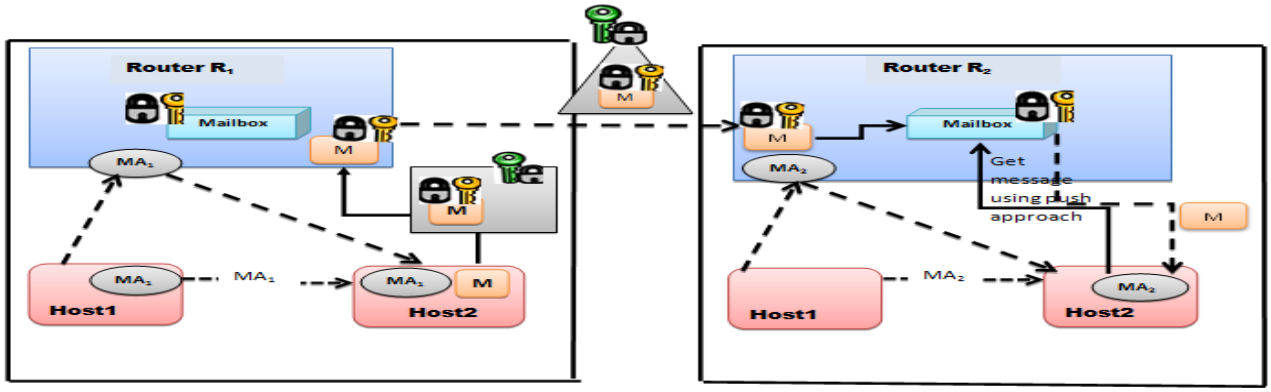

Figure 3. Fig 3: Message Communication among MA's in Global Network

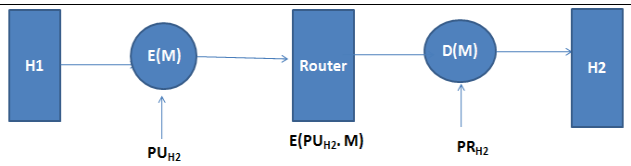

Figure 4. Fig 4: Host to Router and Router to Host Communication

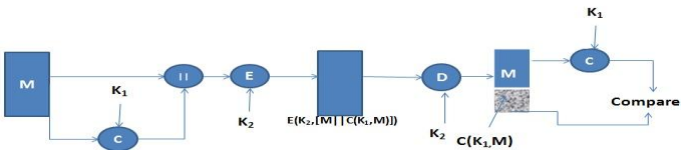

Figure 5. Fig 5: Message Encryption Using MAC Function

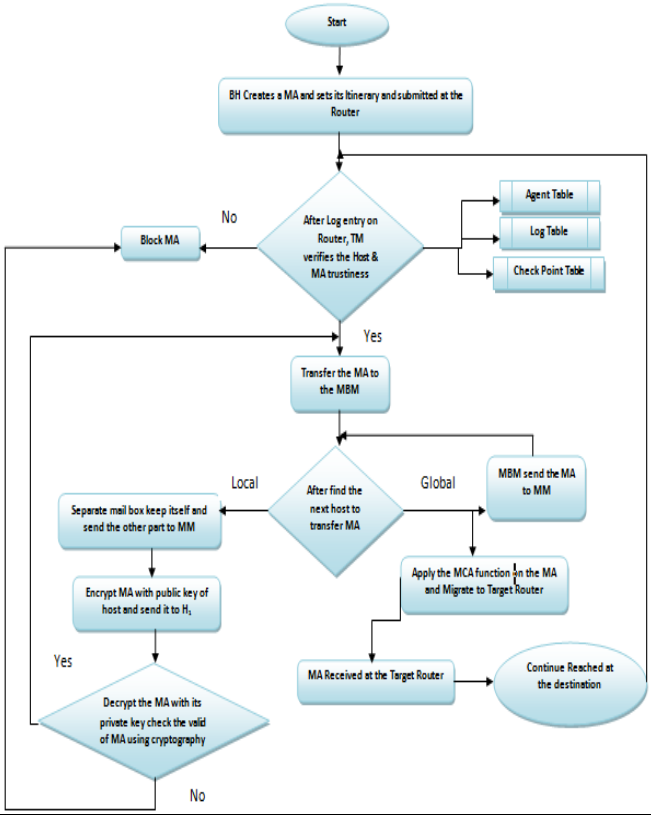

Figure 6. Fig 6: CBHSA Work Flow

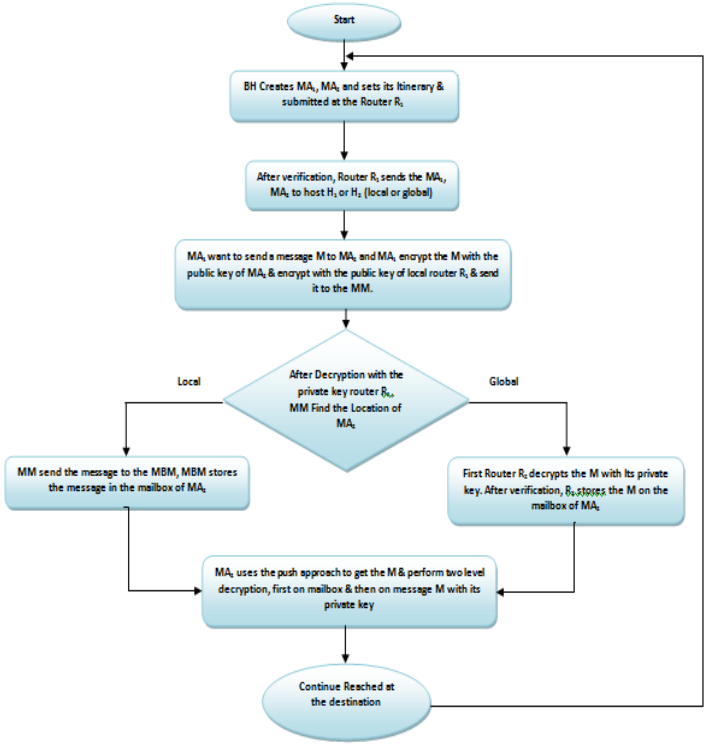

Figure 7. Fig 7: Message Passing In CBHSA Framework