Self-Protected Mobile Agent Approach for Distributed Intrusion Detection System against DDoS Attacks

P. Marikkannu, J. J. Adri Jovin, and T. Purusothaman

***Abstract*—With the growing Information Systems and Network technologies, security threats over the systems have also become common. Providing a security mechanism to detect such threats has become an inevitable part of Information Systems. Distributed Denial of Service (DDoS) attack is one of the most common attacks which are done in a co-ordinated manner. Hence, we need a Distributed Intrusion Detection System to detect those attacks. We use mobile agents for the purpose of Intrusion Detection. However, these mobile agents are prone to attacks which may lead to the failure of the IDS as a whole. In this paper, we propose a system for distributed intrusion detection system against DDoS attacks. In our system, we propose two security architectures namely Isolated Trusted Environment SMADIDS and Integrated Trusted Environment SMADIDS based on the mechanism of reference clone to protect the mobile agent from being modified. We also incorporate the functionality of Protocol Analysis Method in combination with the traditional rule based IDS to enhance the Intrusion Detection and to reduce false alarm rate. From the results obtained, it was observed that the system proves to be better in its performance compared to other traditional Intrusion Detection Systems and is found to provide at most security to the Mobile Agents.**

***Index Terms*—Distributed intrusion detection system, self-protected mobile agents, DDoS, reference clone, protocol analysis, network security.**

I. Introduction

Information Security is the process by which an organization protects and secures systems, media and facilitates that process and maintains information vital to its operations (Federal Financial Institutions Examinations Council, 2002). An Intrusion Detection System (IDS) is a defense system which detects hostile or unusual activities and announces that an intrusion is detected [1]. It is usually used to detect the various activities which compromise with the security services such as integrity, confidentiality and availability. One major threat to the availability of network resource is the Denial of Service attack. The Denial of Service prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target, for example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages, so as to degrade performance [2].

Manuscript received April 4, 2012, revised June 6, 2012.

P. Marikkannu is with the Department of Information Technology, Anna University of Technology, Coimbatore, India (e-mail: pmarikkannu@gmail.com).

J. J. Adri Jovin is with the Department of Computer Science and Engineering, SriGuru Institute of Technology, Coimbatore India (e-mail: adrijovin@yahoo.co.in).

T. Purusothaman is with the Department of Computer Science and Information Technology, Government College of Technology, Coimbatore India (e-mail: purushgct@yahoo.com).

II. Background

A. Mobile Agent

Mobile agent is a kind of software that can migrate freely on the internet from one server to another in a diverse network system. It can interact and communicate with other different mobile agents or distributed systems. The mobile agent is an independent model or program. Each mobile agent can single-handedly execute tasks assigned by its user by interacting and communicating with other agents. The mobile agent is extremely adaptable. Also, it provides high credibility services to its users [3]. Mobile agent can be transferred to a different address space to perform, and its implementation after the transfer is a continuous process, that is, begin to continue to implement from next one after the transfer, in the process it can maintain its own state. Mobile agent makes the calculation shift to data to change the traditional calculation, reduce network communication overhead, save bandwidth, load balancing, speed up implementation of its mandate, thereby enhancing the processing efficiency of distributed systems [4].

In different systems, its concrete realization is slightly different, but the mobile agent generation process, roaming path, implementation process are basically similar. The communication mechanism refers to develop the communication means between the agents and other entities. The security mechanism is to describe the approach of the mobile agent to access other mobile agents and network resources. The migration mechanism is responsible for organizing the mobile agent code and its implementation intermediate state, allowing it to move between different locations [4].

The mobile agent, in addition to the basic characteristics of the intelligent agents, also has the following features:

- Autonomy
- Intelligence
- Platform-independent feature
- Distribution facility
- Low-network data traffic
- Strong fault tolerance
- Multi-agent cooperation

The advantages of using mobile agents in IDS are

- Reduced network load and load balance
- Asynchronous & Autonomous Execution

- Dynamic Adaption
- Heterogeneous Execution
- Fault tolerance

B. Mobile Agent Security

Since the beginning of mobile agent research, many security issues have been identified. Research efforts in the field of mobile agent security have been intense over the last decade [5]. Several protection mechanisms have been proposed in order to provide a solution to this problem. However, the problem of malicious hosts attacking an agent is by far much difficult to solve. Platforms can do anything when executing an agent, from denial of service to prevent its access to a given resource, to a modification of its code and data in order to change its final behavior [5]. Moreover, mobile agents are prone to attacks like Masquerading, Unauthorized access, replay attacks etc. In such a scenario, mobile agents themselves may become malicious and may destroy the entire system. There are possibilities that a mobile agent may provide false data to the user, when it becomes malicious. Since mobile agents have the property of mobility, it moves from one host to another, which in turn increases the vulnerability of the host being attacked. The mobile agent security not only depends on the external network, but also the agent platform from where the mobile agent obtains its resources to perform various tasks. The agent platform, when becomes malicious either denies its resources to the mobile agent or kills the mobile agent or injects the mobile agent with its malicious code making the mobile agent malicious. This would spread to other systems in the network, causing damage to the entire network. Hence, it is highly essential that a mobile agent must be provided with security for the proper functioning of the entire system.

C. Distributed Intrusion Detection System (DIDS)

An intrusion detection system (IDS) is a software and/or hardware that continuously monitor activity, looking for something suspicious. When it detects suspicious activity, it takes some action. The action could be alerting an administrator or simply recording the activity in another log file. Some newer IDSs have the ability to automatically respond to certain attacks. In general, policies tend to be either prohibitive or permissive [6]. The DIDS comprises of a collection of standalone IDSs which functions in a co-operated manner. They follow a mechanism for sharing data, intrusion patterns and other control information. The information exchange between IDS in a distributed environment can be carried out by means of a mobile agent. The DIDS may have a centralized rules library or individual rules library. A centralized rules library adds more networks overhead. While using individual rules library, it is very essential to check whether the rules library possess the latest updates of intrusion patterns in order to make the DIDS efficient.

D. Distributed Denial of Service Attack (DDoS)

A Distributed Denial of Service involves an attack comprising of a large number of hosts to launch DoS attacks of SYN flooding, UDP flooding and ICMP flooding against any target system.

III. Related Works

In the Distributed Intrusion Detection System proposed in [7], various types of Intrusion Detection Systems are discussed, but it does not provide any systematic setup to provide security to the mobile agent.

In the Distributed multi-level anomalies detection system proposed in [8], a well-defined system is proposed for anomaly detection using mobile agents. However, it does not care much about the security of the mobile agent. Though the system provides a well-sophisticated architecture for anomaly detection, it fails in case of the mobile agent security, which in turn may affect the stability of the entire system.

The Intrusion Detection System described in [9] explains a system which uses a set of hosts as coordinators. The central coordinator is composed of various hosts, of which failure of any one of the host may affect the system, as a whole. Also, the hosts in the central coordinator, though have diversified functionalities, rely on one another. As a result, this system could not be considered as a reliable one.

The Distributed Intrusion Detection System proposed in [10] just gives an introductory architecture of the DIDS and does not address any sort of security issues. The system contains various modules like data flow capture, Intrusion Detection Agent, a Mobile agent environment in each host, A data analysis part and a Sensor(Sniffer) in each host. The working principle is so simple and could be broken by any malicious attacker. Thus, this system is found to be vulnerable to a wide range of mobile agent security threats.

[11] gives an open system with good flexibility and expansibility. It provides architecture to overcome the problem of single-point failure. The architecture is composed of various sub modules like the Supervisor, Trace collecting agents, Mobile Inspection agent, Response Agent, Policy modify agent, Database and a Policy database. The Supervisor is composed of two parts namely the Management Agent, which is responsible for managing and controlling the agents in the system, and the Billboard. The Trace-collecting agent moves around the network and collect all sort of information. The mobile-inspection Agent implements the decision making function in the system. The Response Agent is concerned with the functionalities like canceling of user's connection, limiting the number of users etc. The Policy-modifying agent updates the security policy based on the profiles of intrusion action. The Database stores the audit data, network package and relevant information. The Policy databases perform some processing functions of specific events. This system provides architecture of IDS in a co-operative environment. But, it does not address the issues related to mobile agent security.

[1] Compares the various schemes that are available for the development of inside attack proof intrusion detection system of which the Benachenhou and Pierre's scheme [12] is found to be much effective with respect to detection and provision of trusted server. It compares the Schneider's scheme and Roth's scheme with Benachenhou and Pierre's scheme of which it conclude that the Benachenhou and Pierre's scheme is comparatively better than the previous two schemes. It also provides an improved architecture of CONFIDANT agent and agent gateway structure. This scheme is resistant to the security attacks like Masquerading,

unauthorized access, denial of service and repudiation. This also provides security to the mobile agent to a certain extent.

The New Distributed Intrusion Detection System introduced in [13], proposes a system which uses both pattern as well as protocol analysis. This system contains three modules namely the Control Management Module, Intrusion detection module and Intrusion Response module. The control management module is responsible for collecting and processing the event sent by the intrusion detection module for administrator reference. It contains the User Interface, basic functional sub-module and a scheduling sub-module. The Intrusion detection module here may be divided into Host-based intrusion detection module, which uses host audit data and system logs as the information sources and the Network based intrusion detection module which detects intrusion through analysis of data packets. This also introduces a new method of Intrusion Detection based on Protocol Analysis Method which involves network data acquisition, protocol decoding and packet analysis. This method is found to be more reliable than the traditional Intrusion Detection Systems. This system also incorporates the pattern based IDS along with the protocol analysis method.

The Distributed Intrusion Detection System introduced in [14] gives a solution for single-point failure. It has six types of agents which are Manager Agent, Analysis agent, Monitor agent, Executive agent, Retrieval agent and Result agent of which the first four are static and the latter two are mobile. The responsibility of the Monitor Agent is collecting and preprocessing information of both system audit records and network traffic. The Analysis Agent integrates and analyses the information received from Monitor Agent. The executive agent is responsible for executing tasks depending on the notification of the Analysis Agent. The manager agent manages retrieval processes and also maintains a Neighborhood list of the host which the Manager Agent resides on. The Retrieval Agent moves to other hosts and lets their Analysis Agents check whether there are similar records from the same suspicious remote host. The Result agent contains the result sent by the remote host. The system provides a wide range of protection to the system against DDoS attacks but fails to provide security to the host.

IV. Proposed Solution

In order to overcome the problems in mobile agent security, we propose the Self-protected Mobile Agent Distributed Intrusion Detection System (SMADIDS).

The components of SMADIDS are explained below.

A. Monitor Agent

The Monitor Agent performs the functionality of monitoring the various activities that happens in the host system. It monitors the Host's Audit records as well as the network packets that are entering the host. It contains a packet capture module, which captures the network packets and sends them for analysis. Winpcap is used for the purpose of packet capturing. Each and every packet that enters the host is captured by the packet capture module. The Monitor Agent also performs the function of protocol decoding and audit record decoding, making it suitable for the Analysis Agent to perform analysis.

B. Analysis Agent

The Analysis Agent is responsible for the analysis of the protocol. The Analysis Agent contains integrated rules library and a protocol analysis module associated with it. The rules library contains the various attack patterns and the protocol analysis module checks the captured packets by means of pattern-matching the packet structure. The rules library used in association with the Analysis Agent is that rules library that is being used by SNORT. The patterns which are identified to be intrusions are stored in the rules library and are immediately send to the neighboring hosts. This work is done with the help of the Executive Agent. The Analysis Agent notifies the Manager Agent as well, the Executive Agent about intrusion as soon as it encounters one.

C. Executive Agent

The Executive Agent is used only for the purpose of executing the notifications given by the Analysis Agent and the Manager Agent. It performs various tasks like restoration of corrupted files, establishment and termination of network connection, communicating with other hosts and similar tasks.

D. Manager Agent

The responsibility of the Manager Agent is to manage the various activities that take place in the host. The Manager Agent creates the Mobile Agent and a Clone Agent, for each Mobile Agent that is being created. The Clone Agent is send to the Trusted Environment, which is discussed below. The mobile agent is send to the other hosts through the network. It also receives mobile agents from other hosts and responds to it. It is not only essential for the communication between various hosts, but also for the proper functioning of the Analysis Agent and the Executive Agent. A communication channel exists between the Manager Agent and Analysis Agent as well the Executive Agent and the Manager Agent. Non-restricted flow of data is assured between the Manager Agent and Analysis Agent. The Manager Agent also informs the neighboring hosts of the intrusion that is being detected in a host.

E. Mobile Agent

The Mobile Agent is generated by the Manager Agent. The Mobile Agent is a specialized one, which consists of a Header, Code, State, Itinerary, Retrieval Query and the Result Data. The data format of the Mobile Agent is shown in Fig. 1.

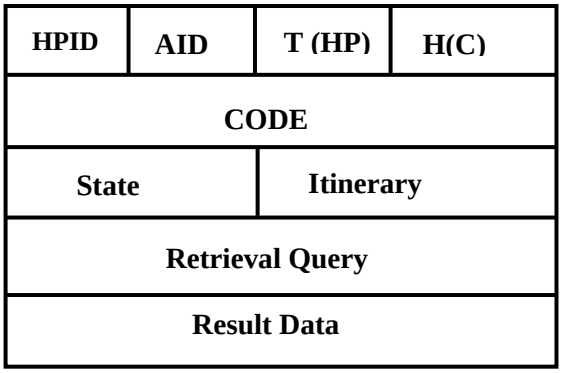

Fig. 1. Mobile agent data format.

HPID is the Home Platform Identity which is generated by the Host Agent Platform, AID represents the Identity of the Mobile Agent and is unique for a Mobile Agent in the entire system, which is generated by the Manager Agent, T (HP) represents the timestamp at which the Mobile Agent left the Home Platform and H(C) is the hash value of the Agent code obtained by means of a Hash function. The Code part of the Mobile Agent contains information about the negotiation, decisions and the next platform choice. The state contains information about the data structures and execution state containing the control information. The retrieval query is used to retrieve data from the other host and resultant data is carried by the Result Data field. The itinerary denotes the set of platforms, the agent need to visit.

The Host systems follow an ordered system of naming which makes it convenient to create Mobile Agents with a Unique ID within the system. Using the Unique ID, the origin of a Mobile Agent can be identified. The Mobile Agent also carries other information like alerts, controls and Intrusion specific data. It is the Mobile Agent that carries the pattern of intrusion that has been detected in one host, to another, so that all the hosts will be aware of any new type of intrusion and remains updated. The intrusion pattern will be stored in the rules library present in each host.

F. Clone Agent

In the SMADIDS system, for each mobile agent generated, a Clone Agent is being created which contains the data almost similar to that of the mobile agent. The Clone Agent can execute only in the Trusted Environment. The data format of the Clone Agent is shown in Fig. 2. The HPID, AID, T (HP), H(C), are the same for both the Mobile Agent and Clone Agent. The State $_{ref}$, Itinerary $_{ref}$, Retrieval Query $_{ref}$ and Result Data ref are created in reference with the Mobile Agent and are subjected to a Virtual Execution in the Trusted Environment.

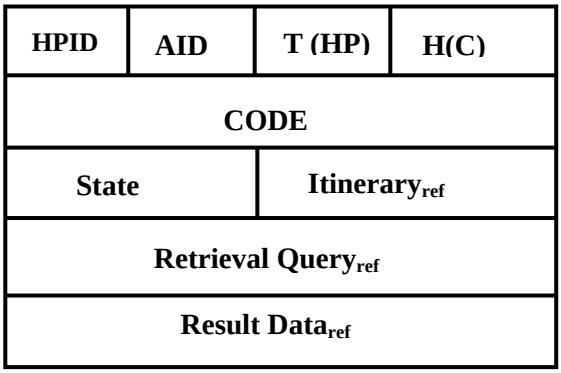

Fig. 2. Clone agent data format.

The Retieval Query$_{ref}$ and the Result Data$_{ref}$ has no role to be played inside the Trusted Environment. However, both the fields are kept alive inorder to retrieve back the Mobile Agent, in case if the Mobile Agent gets destroyed, from the Reference clone. Thus, the reference clone can be used for data retrieval in case if a Mobile Agent fails or get destroyed in its itinerary.

G. Trusted Environment

The Trusted Environment is an isolated Virtual Execution Platform (VEP) which is assumed to be immune to all sorts of attacks. The Trusted Environment may be a part of the Host or a Secure Server. Trusted Environment as a part of the Host reduces the Network Traffic overload. When a Mobile Agent is created, a Clone Agent of its similar type is created and sends to the Trusted Environment. The Trusted Environment, based on the itinerary$_{ref}$ creates a Virtual Execution Environment, similar to the External Network and performs execution of the Clone Agent. The Trusted environment has the capability to simulate the itinerary alone and cannot perform any other data transfers. Execution here represents the simulation of the itinerary. The Trusted Environment provides a free communication channel for all the hosts present in the network, but does not allow any type of execution inside the Virtual Environment. Once the itinerary is completed, the Clone Agent is destroyed by the Trusted Environment. If a proper response is not received by the Trusted Environment at regular time intervals, from the hosts in the network, the Trusted Environment keeps the Clone Agent to regenerate the Mobile agent. This is usually done based on the assumption that the Mobile Agent might have been destroyed somewhere in the network.

For each itinerary of the Mobile Agent, the remote host checks the status of the Clone Agent in the Trusted Environment to check whether the Mobile Agent is safe to access and to be accessed or not. In case, any misbehavior is found, a copy of the Mobile Agent is created based on the Clone Agent by the Home Platform and is send to the remote host. Based on these, the information is being exchanged and the DDoS attacks are identified based on the results.

We propose two variant architectures of SMADIDS which are as follows

- Isolated Trusted Environment SMADIDS
- Integrated Trusted Environment SMADIDS

Fig. 3 shows the architecture of Isolated Trusted Environment SMADIDS.

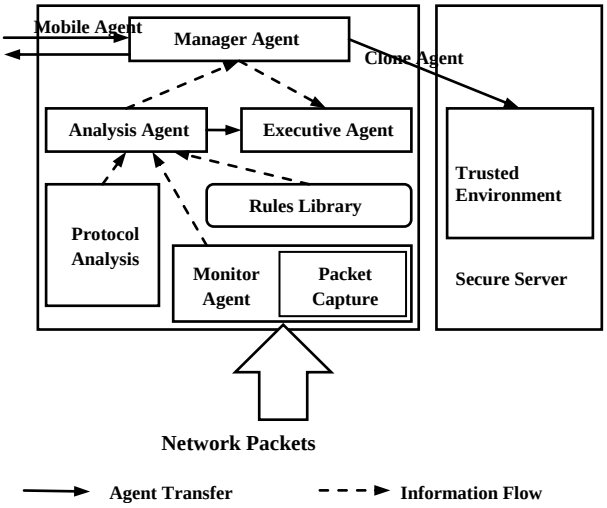

Fig. 3. Isolated trusted environment self-protected mobile agent distributed intrusion detection system architecture.

In the Isolated Trusted Environment SMADIDS, the Trusted Environment is located in a separate Secure Server which is protected from external threats. For each Clone Agent received, the Secure Server has the ability to create a Trusted Environment. From experimental results, the Isolated Trusted Environment SMADIDS was found to

exhibit a latency due to network load when the number of hosts connected to the Secure Server is more. Inorder to overcome this latency, the Integrated Trusted Environment SMADIDS could be used. The architecture of Integrated Trusted Environment SMADIDS is shown in Fig. 4.

In the Integrated Trusted Environment SMADIDS, the Trusted Environment is located inside the host itself. This would reduce the latency due to network load. Hence, this architecture would support a number of hosts and doesnot need a central Secure Server to control the Clone agents. Each host would manage its own Clone Agents. There would be no concern about the transfer of data from the Manager Agent to the Trusted Environment, since exists an unrestricted communication channel between them. Thus it reduces congestion in the network.

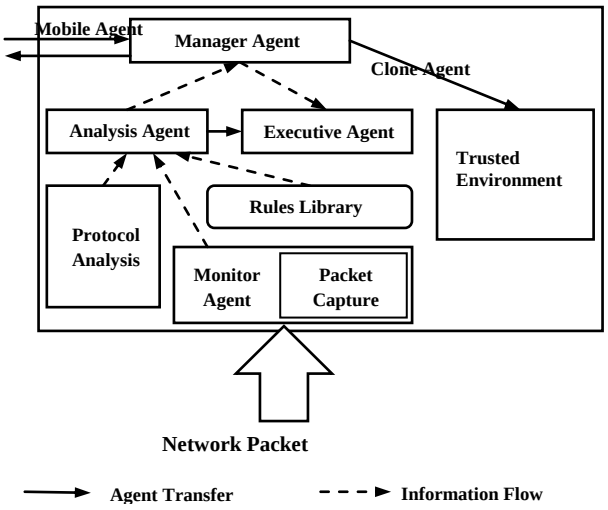

Fig. 4. Integrated trusted environment self-protected mobile agent distributed intrusion detection system architecture.

V. Security Analysis

The SMADIDS produces Mobile Agents which is controlled from all inter-domain access. Hence, it proves to be efficient against the following attacks.

A. Masquerade

The malicious Mobile Agent, if makes a trial to masquerade as an agent from a trusted domain, the remote host would check it and would cooperate with home platform to detect the masquerader. Since, the system possess a mechanism of providing Unique ID, masquerading attacks cannot be done so easily. Also, the Mobile Agent is checked at each itinerary with the Reference Clone which would avoid any sort of mismatch in the identity. Since, Clone Agent cannot be created for the Mobile Agent with a fake identity; it is obvious that the masquerading Mobile Agent could be identified so easily. Once identified, the fake Mobile Agent would be destroyed immediately by the Agent platform in the corresponding host. Thus this mechanism provides complete security against masquerading attacks.

B. Unauthorized Access

If a malicious mobile agent tries to gain unauthorized access over an agent platform, the agent platform checks the HPID and AID and verifies it with the platform with the corresponding HPID. Based on this, the malicious mobile agent can be detected and the information is shared among the hosts and thus access towards the resources will be blocked for that Mobile Agent that is identified to be malicious. Thus, unauthorized access can also be controlled by means of SMADIDS.

C. Denial of Services

A malicious Mobile Agent can launch Denial of Service which may develop into a DDoS. By using the reference clone, the permissions for a Mobile Agent can be checked. Based on the inferences made, the replication of the Mobile Agent can be controlled or totally avoided. Moreover, intimation about the existence of such Mobile Agents is done to all the hosts and the Mobile Agent is destroyed. Thus the DDoS attack can be detected and controlled.

D. Replay Attacks

The itinerary of the mobile agent is compared with the reference clone, each time it gets into a platform. Also creation of new Mobile Agent and transfer of data is controlled by the Manager Agent and hence, replay attacks could be controlled.

The system is also found to be efficient in terms of fault tolerance. Even if a Mobile Agent fails to complete a task or gets destroyed, it could be easily recovered by using the Clone Agent in the Trusted Environment. This mechanism enhances the stability and reliability of the system. Thus this system has been found to be fault tolerant and is resistant to security threats.

VI. Conclusion and Future Work

This paper proposes a solution for the problem of mobile agent security based on a reference clone. The methodologies introduced in this paper have enhanced the Distributed Intrusion Detection technique against DDoS attacks. Also, this method is found to be efficient in tackling the various attacks like Masquerading, Unauthorized Access and Replay attacks and strengthens mobile agent security. Since this paper provides two varied solutions for mobile agent security, namely Isolated Trusted Environment SMADIDS and Integrated Trusted Environment SMADIDS, the user could choose the architecture which the user desires based on the needs.

In future, a mobile agent security protocol may be used to replace this architecture, which would promote the safe transmission of the Mobile Agent without any external interference.

References

[1] W. Shi, I. Jang, and H. S.Yoo, "An inside attacker proof Intrusion Detection System," in *Proceedings of Fourth International Conference on Computer Sciences and Convergence Information Technology (ICCIT'09)*, South Korea, 2009, pp. 1020-1024.

[2] W. Stallings, *Cryptography and Network Security*, Prentice Hall, 2005, ch. 1.

[3] Y.-F. Chung, T.-S. Chen, and M.-W. Lai, "Efficient Migration access control for mobile agents," *Computer Standards and Interfaces*, pp 1061-1068, 2009.

[4] G. Kun and J. Sumei, " Research on the Application of Mobile Agent in Intrusion Detection Technology," in *Proceedings of 2nd International*

Conference on Computer and Technology, China, 2010, pp. V6-549 – V6-553.

[5] C. Garrigues, S. Robles, J. Borrell, and G. N. Arribas, "Promoting the development of Secure Mobile Agent Applications," *The Journal of Systems and Software*, vol. 83, pp. 959-971, 2010.

[6] M. G. Solomon and M. Chapple, *Information Security Illuminated*, Jones and Bartlett Publishers, Inc., 2005, ch. 1.

[7] C. Akyazi and A. S. E. Uyar, "Distributed Intrusion Detection using Mobile Agents against DDoS Attacks," in *Proceedings of 23rd International Symposium on Computer and Information Sciences (ISCIS '08)*, Istanbul, 2008, pp. 1-6.

[8] F. B. Ftima, W. Tounsi, K. Karoui, and H. B. Ghezla, "A Distributed Multi-level anomalies detection system using the mobile agent approach," in *Proceedings of Global Information Infrastructure Symposium (GIIS '09)*, Tunisia, 2009, pp. 1-4.

[9] A. Javan, K. M. Samsudin, A. R. Ramli, and W. A. W. Adnan, " Co-ordinator Association Approach to Mobile Agent Based Intrusion Detection System," in *Proceedings of First International Conference on Distributed Framework and Application (DFmA 2008)*, Malaysia, 2008, pp. 111-114.

[10] X.-L. Mo, C.-D. Wang, and H-B. Wang, "A Distributed Intrusion Detection System based on Mobile Agent," in *Proceedings of 2nd International Conference on Biomedical Engineering and Informatics (BMEI'09)*, Tianjin, 2009, pp. 1-5.

[11] L. Jianxio and L. Lijuan, "Research of Distributed Intrusion Detection System Model based on Mobile Agent," *International Forum on Information Technology and Applications (ifita)*, Changsha , 2009, V2-53- V2-57

[12] L. Benachenhou and S. Pierre, "Protection of a mobile agent with a reference clone," *Computer Communications*, pp. 268-278, 2006.

[13] X. Qing, "The structure design of a New Distributed Intrusion Detection System," in *Proceedings of 2nd International Conference on Computer Engineering and Technology (ICCET)*, Lianyungang, 2010 pp. V7-100-V7-103.

[14] D. Ye, Q. Bai, M. Zhang, and Z. Ye, "P2P Distributed Intrusion Detection by using Mobile Agents," in *Proceedings of ICIS*, Wollongong, 2008, pp. 259-265.

P. Marikkannu received his Masters (Master of Technology) in Information Technology from College of Engineering, Anna University, Chennai. He is currently pursuing his PhD in Anna University of Technology, Coimbatore. He is working as an Assistant Professor in the Department of Information Technology, Anna University of Technology, Coimbatore. He has published many research articles in various Journals. His research interests include Agent-Based Intelligent Systems, Network Security and Distributed Computing. Mr. P.Marikkannu is a member of ISTE.

J. J. Adri Jovin received his Masters (Master of Technology) in Information Technology from Anna University of Technology, Coimbatore. He is currently pursuing his PhD in Anna University of Technology, Coimbatore. He is working as an Assistant Professor in the Department of Computer Science and Engineering, SriGuru Institute of Technology, Coimbatore. He has published research articles in various Journals. His research interest includes Agent-Based Intelligent Systems, Network Security, Cloud Computing and Algorithm Analysis.

Mr. J.J. Adri Jovin is a member of various professional bodies such as ISTE, IACSIT, IAENG, ACM, ACCS and AIRCC.

T. Purusothaman, completed his BE degree in the year 1988 under Madras University and completed his ME (CSE) degree at Government College of Technology, Coimbatore in the year 2002. He did his Ph.D. under Anna University in 2006. He is currently working as Associate Professor in the Department of Computer science and Engineering at Government College of Technology, Coimbatore. His research areas include Network Security and cryptography, Distributed operating systems, Mobile computing, Advanced Genetic Algorithm and Grid Computing. He is the co-investigator of the project titled "Optimization of search time for evaluation of ciphers using Genetic Algorithm based cryptanalysis" sponsored by Ministry of Communications & Information Technology, New Delhi. He has presented various papers in International conferences and attended a Faculty Development Program at Canada.