Intrusion Detection in Agent-Based Virtual Knowledge Communities

Ogunleye G. O.
Department of Mathematical Sciences (Computer Science Programme), Redeemer's University (RUN)
Redemption Camp, Ogun State, Nigeria
E-mail: ope992000@yahoo.com

Ogunde A. O.
Department of Mathematical Sciences (Computer Science Programme), Redeemer's University (RUN)
Redemption Camp, Ogun State, Nigeria
E-mail: adewaleogunde@yahoo.com

Abstract

Virtual Knowledge Communities (VKC) are current popular media on the internet through which the access and sharing of knowledge and information among communities of similar interest groups are made possible. Agent's technologies are presently being deployed to facilitate the success of VKC, which is a virtual place where knowledge agents can meet, communicate and interact among themselves. Recently, quite a number of works have been done on agent-based knowledge communities but most of these works have not actually considered the possibilities of intrusion and the consequences that these malicious attacks can have on those systems. This paper therefore addresses the issue of intrusion detection problems in the sharing of knowledge in agent-based virtual knowledge communities. Intelligent agents are proposed as measures to guide against any spy or intruder into the VKC environment. The relevance of this method in current scientific research cannot be overemphasized as the work shows great potentials of yielding promising results.

Keywords: Virtual knowledge communities, Knowledge sharing, Mobile agent technology, Intrusion detection

1. Introduction

Virtual communities are becoming increasingly popular, particularly on the Internet, as a means for like-minded individuals to pursue common goals. It is a way to access and share knowledge and information among participants of such communities without physical or hardware constraints. The concept of a community of interest can be supported in a virtual community in order to bring the appropriate parties together and to share their knowledge with each other.

An agent is a program that helps a user to perform a task (or set of tasks), possibly by maintaining persistent state and communicating with its owners, other agents or its environment in general (Zoran and Zoran, 2000). Virtual knowledge community is a virtual place where agents can meet, communicate and interact among themselves (Maret and Calmet, 2009). It is possible for agents to be sharing some vital information concerning trade secrets among themselves. Recently, how to make the system to be rigid against any vulnerability of an intruder such that agents are free to exchange any information without any fear of attack has become a subject of much concern. Most organizations today can not freely share knowledge with their employees due to insecure system.

Intrusion detection is a method of supervising the events occurring in a computer system or network and examining them for traces of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (Karen and Peter, 2007). Incidents have many causes, such as malware (e.g., worms, spyware), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many incidents are malicious in nature, many others are not; for example, a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

Intrusion detection has been a subject of discussion for most organizations today and it has posed serious threats on how to make the system more secured against intruders. Many researchers have used different approaches to address the problem of intrusion detection in computer systems. Some of these approaches are: data mining approach proposed by (Lee and Stolfo, 1998) and neural network component for an Intrusion Detection (Debar, et. al., 1992). In view of this, system problems that are being caused by malicious users are threatening, and the

inability of commodity operating systems to provide more than minimal protection has led to a variety of attempts to secure computing systems through add-on or external means. Firewalls and similar mechanisms produce the principal line of defense for many installations.

This paper therefore presents a framework for knowledge sharing activities in multi-agent systems that is secured against any intrusion or malicious access. The rest of the paper is organized as follows. In section 2, intrusion detection, mobile agents, virtual knowledge communities are reviewed. In section 3, our intrusion detection method is introduced based on intelligent light and monitoring agents. Section 4 gives some initial results and discussions while conclusions are drawn in section 5.

2. Literature Review

2.1 Intrusion detection

Intrusion detection can be defined as potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable (Anderson, 1980). Sundaram (1996) noted that an intrusion threat is the potential possibility of a deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable. With this perspective, Sundaram (1996) also noted that there are different aspects to an intrusion, each of which is significant to a full analysis and response. These aspects include:

Risk: Accidental or unpredictable exposure of information, or violation of operations integrity due to the malfunction of hardware or incomplete or incorrect software design,

Vulnerability: A known or suspected flaw in the hardware or software or operation of a system that exposes the system to penetration or its information to accidental disclosure.

Attack: A specific formulation or execution of a plan to carry out a threat.

Penetration: A successful attack, that is, the ability to obtain unauthorized (undetected) access to files and programs or the control state of a computer system.

However, intrusion detection techniques can be divided into two main types: anomaly detection and misuse detection.

Anomaly Detection: Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a couple of interesting possibilities:

Anomalous activities that are not intrusive are flagged as intrusive.

Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are). This is a dangerous problem, and is far more serious than the problem of false positives.

The main issues in anomaly detection systems thus become the selection of threshold levels so that neither of the above 2 problems is unreasonably magnified, and the selection of features to monitor. Anomaly detection systems are also computationally expensive because of the overhead of keeping track of, and possibly updating several system profile metrics

Misuse Detection: The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems, they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity.

2.2 Mobile Agents

Agents are autonomous entities that have their own knowledge and can act and communicate with each other. Agent's knowledge is stored in the personal repository of the agent, which contains the relations between the concepts, the properties associated to these concepts, and the different instances of concepts and properties.

A mobile agent is a kind of software program that can migrate from one host to another in a heterogeneous network (Kuo-Huang et al., 2007). Also known as travelling agents, these programs will shuttle their being, code and state among resources. They are network nomads that act as personal representative, working autonomously

through networks. They are able to visit network nodes directly using available computing power and are not limited by platform. The technology has become an alternative approach for the design and implementation of distributed systems to the traditional Client/Server architecture.

Mobile agents can migrate from one system to another during their execution and communicate amongst one another, clone, merge and co-ordinate their computations. Mobile agents are autonomous agents in the sense that they control their relocation behavior in pursuit of the goals with which they are tasked. Main fields of application for mobile agents are information retrieval on the www, distributed database access, parallel processing, automation of electronic marketplaces and others. Mobile agent frameworks are currently rare, due to the high level of trust required to accept a foreign agent into one's data server. However with the advances in technologies for accountability and immunity, mobile agent systems are expected to become more popular in the future.

Some other recent works found in the literature on mobile agent based intrution detection systems are highlighted in the next section.

2.3 Agent-Based Intrusion Detection Systems

Abraham et al. (2007) worked on lntrusion Detection System (IDS) that was based on a hierarchical architecture with Central Analyzer and Controller (CAC) as the heart and soul of the Distributed Intrusion Detection System (DIDS). The CAC usually consists of a database and webserver which allows interactive querying by the network administrator for attack information/analysis and initiate precautionary measures. CAC also performs attack aggregation, building statistics, identify attack patterns and perform rudimentary incident analysis. Sodiya (2006) proposed Multi-Level and Secured Agent-based Intrusion Detection System (MSAIDS) which focused on improving IDS performance, detection of autonomous attack using its architecture, Reduction in false alarm, IDS agents' security.

Wang et al. (2006) proposed Mobile Agent for Network Intrusion Resistance. The designed system framework includes the following components: (i) Manager: the centre of controlling and adjusting other components and it maintains their configuration information. The manager receives intrusion alarms from host monitor Mobile Agent (MA) and executes intrusion responses using intrusion response MA. (ii) Host monitor MA: this is established on every host in the network. If intrusions occur confirmatively, the host monitor MA will appeal to the manager and report the suspicious activity directly. After receiving the appeal, the manager distributes a data gathering MA patrolling other hosts in the network to gather information. If a distributed intrusion is found, the manager will assign an intrusion response MA to respond intelligently to every monitored host. The database of configuration stores the node configuration of detecting system.

Onashoga et al. (2009) also worked on the Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems. Their paper proposed a way of classifying a typical IDS and then strategically reviews the existing mobile agent-based IDSs focusing on each of the categories of the classification, for example architecture, mode of data collection, the techniques for analysis, and the security of these intelligent codes. Their strengths and problems were stated wherever applicable. Furthermore, they suggested ways of improving on current mobile agents' intrusion detection system designs in order to achieve an efficient mobile agent-based IDS for future security of distributed network.

2.4 Virtual Knowledge Communities

Virtual communities are becoming increasingly popular, particularly on the Internet, as a means for like-minded individuals to meet other individuals they can learn to trust and to share and gain access quickly and efficiently to the information they are mostly interested in. The concept of a community of practice or a community of interest can be supported in a virtual community in order to bring the appropriate parties together and to share their knowledge (Maret and Calmet, 2009) . The advantage of this is that the members of a community centered on one specific topic or practice will only be presented with knowledge from domains they are, or at least are relatively likely to be, interested in. This knowledge needs not be something they have specifically asked/searched for.

Many virtual communities' applications already exist on the Internet. Some are using agents in various forms as part of the back office system. (Maret and Calmet, 2009) proposed an approach that extends the abstraction of an agent, such that it acts within the system, searching for or delivering knowledge within other agents and through communities. With such a model, agents can choose to join, leave, create and destroy a community, they can ask for information and send information to the community, and they can be member of several communities simultaneously. Virtual Knowledge Community (VKC) was called the virtual place where agents can meet,

communicate and interact among themselves. Basically, a VKC is centered on a topic, corresponding to a domain of interest for which the interested agents have joined this community. This notion allows an increased availability of data and knowledge within the various communities.

The concept of knowledge cluster is used to represent a piece of knowledge from the agent's repository. Agents share and exchange knowledge clusters. A community consists of a domain of interest (a knowledge cluster), a leader (an agent), a policy and an unspecified number of member agents. The leader has created this community to achieve a goal (corresponding to the domain of interest). Each community is associated to a single policy which defines the community and which is up to the community leader. For instance, depending on the policy, a message buffer stores for a given duration or under given rules exchanged messages within this community.

Quite a number of researchers that have worked in the VKC and agent based environments (Boella et al. 2006; Portillo-Rodrguez et al., 2007; Endsuleit, 2007) have all pointed out the necessity for better solutions to intrusions and other security problems associated with this research area.

3. System Design

The main basic concepts of VKCs are the Community of Communities, Agents and Community. Community of communities is a yellow page system. Agents can hold and manage a Community of communities, or just refer to one or several Community/ies of communities. This allows agents to check existing communities and to join them according to their centers of interest. Also, within a community of communities other specific communities can be dynamically created and terminated by the agents according to their goals.

A community is a place where agents can meet and share knowledge with other agents who share a similar domain of interest. It comprises of 'community of communities' of which all agents are a member, and within this global community, communities can be created and destroyed dynamically by agents, as and when necessary. There are different types of communities which are explained below:

CommunityOfCommunities. This class is implemented by agents through which other agents have access to a list of existing communities. An agent owner of a class instance manages a list of communities, and each time an action is made that implies a modification of this list, a message is sent to update it.

MembersOfCommunity. Each agent has exactly one instance of this class for each community it is member of, and uses it as an interface to operate within each one of these communities.

LeadersOfCommunity. This class has exactly the same role as the MemberOfCommunity class but seen from the point of view of the community's leader. Since the latter is also a member of the given community, it preserves a MemberOfCommunity nevertheless.

CommunityBuffer. Each community has a CommunityBuffer to (eventually) store the messages sent by the agents. A policy describes the management related to this buffer (access right, duration of messages).

3.1 Light and monitoring agents

Light and monitoring agents are introduced into the communities. The light agent acts as the central security server where all the agents in the communities must register before joining any of the communities of their choice. This is necessary in order to know the total number of agents in all the communities. The light agent creates the monitoring agents whose functions are to monitor all the knowledge sharing activities of the agents. The monitoring agent in turn report to the light agent of any suspected agent in any of the communities. Each of the monitoring agent is connected to an alarm which is triggered to inform the light agent in case of any intruder in the community. If any interloper is noticed, it is the work of the light agent to go to the particular community where the intruder is detected and carry out the necessary action. The light agent might decide to terminate the impostor or to do otherwise. Figure 1 fully explains the prototype. The algorithm for the described method is shown in figure 2.

In figure 2, A, M, L and C represent the number of agents (A_1, A_2…Ai) in the community; the number of monitoring agents in the community (M_1, M_2 …M_k); the number of light agents in the community and the community respectively. Whenever the monitoring agent is not locally present in the community, that community is declared as unsafe and this is usually reported to the light agent. However, all agents (in parallel) such as the ones which have registered with light agents (internally or externally) and are connected to the monitoring agent are declared in the community as safe. Anytime in the community that an intruder is detected by the monitoring agent, it then signals an alert to the light agent which takes the necessary action of either terminating the intruding agent or allow knowledge sharing activities to continue in the community.

 ISSN 1913-8989 E-ISSN 1913-8997

4. Results and Discussion

All agents used in our proposed system as highlighted in section 3 of this paper were created under the Java Agent Development Framework (JADE) system, a Java based software development framework that conforms to Federation of Intelligent Physical Agents (FIPA) standards for intelligent agents (JADE, 2008). The efficiency of JADE platform for agent development has been tested in a scenario where the number of agents and messages are increased, to test the efficiency of agent creation and scalability. Full implementation of our proposed system is currently an on-going work. The implementation addresses the problem of intrusion detection to forestall security lapses that may occur from intruders in the knowledge sharing activities of the agents.

The agent based intrusion detection in virtual knowledge community approach enables agents to exchange data in a formal manner with other agents on a peer-to-peer basis. As long as agents are in the same community, they have the potential to exchange knowledge, and since agents can join any community they wish to, they have the possibility to exchange knowledge with any agents in the entire organization in a formal manner, as long as they share a domain of interest, meanwhile taking care of any possible intrusion.

It also noteworthy to state that our design clearly addressed some crucial security issues raised in numerous papers such as (Boella et al. (2006), (Portillo-Rodrguez et al. (2007) and (Maret and Calmet, 2009). In Boella et al. (2006) normative multi-agent systems for secure knowledge management based on local access-control policies are studied. The authors argue that their approach respects the autonomy of the knowledge providers into the virtual community composed of multiple knowledge providers. In Portillo-Rodrguez et al. (2007), authors propose a three-level multi-agent architecture for considering reputation and trust within communities of practice where knowledge is exchanged. (Maret and Calmet, 2009) proposed a general model that extends the abstraction of an agent, such that it becomes an actor within a knowledge community. Agents themselves, software or human, are the members of the virtual knowledge sharing communities. The system did not take care of the security policies to ensure that only trustworthy agents can access the communities, to prevent malicious attacks from untrustworthy agents. Likewise, our design is different from a theoretically sound approach to forbid the intrusion of agents as well as the capture of exchanged information presented by Endsuleit (2007). It is inspired by methodologies available for cryptographic protocols. Although the complexity analysis shows that this approach is feasible to be implemented, this would require still extensive efforts.

5. Conclusions and Future Work

Intrusion detection in virtual knowledge communities has been studied with the introduction of light and monitoring agents to solve this problem. The paper has indicated the need to provide better security mechanisms in multi-agent communication during the sharing of knowledge. Full implementation of the work is still ongoing and future work will also focus on developing a more intelligent and robust systems in heterogeneous networks.

References

Abraham, A., Jain, R., Thomas, J., & Han, S. Y. (2007). Distributed soft computing intrusion detection system. *Journal of Network and Computer Application*, *30,* 81-98.

Anderson J.P. (1980). *Computer* Security Threat Monitoring and Surveillance. *Technical report*, James P Anderson Co., Fort Washington, Pennsylvania.

Boella G., Van D., & Torre L. (2006). Security policies for sharing knowledge in virtual communities. *IEEE Transactions on Systems, Man and Cybernetics* Vol.36, N.3, 2006, pp439- 450.

Debar, H., Becker M., & Siboni D. (1992). "A Neural Network Component for an Intrusion Detection System." *Proceedings of the IEEE Symposium on Research in Security and Privacy***,** Oakland.

Endsuleit R. (2007). *Robust and Private Computations of Mobile Agent Alliances*. PhD Dissertation, University of Karlsruhe, June 2007. Retrieved from iaks-www.ira.uka.de/calmet/dissertationen/diss_endsuleit.pdf

JADE, (2008). Jena's development team. [Online] Available: http://jena.sourceforge.net/index.html.(2008)

Karen Scanrfone and Peter Mell. (2007). *Guide to Intrusion Detection and Prevention Systems (IDPS).* Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8930, February 2007.

Kuo Huang , Yu-Fang Chung (2007). *Efficient migration for mobile computing in distributed networks.* Elsevier*,* February 2007.

Lee W.and Stolfo S. (1998). *Data Mining Approaches for Intrusion Detection.* In Proceedings 1998 7th USENIX Security Symposium, January, 1998.

Maret Pierre and Calmet Jacques (2009). Agent-Based Knowledge Communities. *International Journal of Computer Science and Applications Technomathematics Research Foundation* Vol. 6, No. 2, pp 1-18, 2009.

Onashoga S., Adebayo D., Sodiya S. (2009). A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems. *Issues in Informing Science and Information Technology*, Volume 6, 2009.

Portillo-Rodrguez J., Aurora V., Juan P. S., Mario P. & Gabriela N. A. (2007). *Fostering Knowledge Exchange in Virtual Communities by Using Agents*. Springer Berlin / Heidelberg, (Lecture Notes in Computer Science), Volume 4715 pp32-39.

Sodiya A. S., (2006). Multi-level and Secured Agent-based Intrusion Detection System. *Journal of Computing and Information Technology* - CIT 14, 2006, 3, 217–223.

Sundaram, A. (1996, February). An Introduction to Intrusion Detection Crossroads. *The ACMStudent Magazine.* Retrieve from acm.org/Crossroads.

Wang, H. Q., Wang, Z. Q., Zhao Q., Wang G. F., Zheng R. J., and Liu, D. X. (2006). *Mobile agents for network intrusion resistance*. APWeb Workshops 2006, LNCS 3842, pp 967-970.

Zoran Putnik and Zoran Budimac. (2000). *Mobile agents – a new and advanced concepts*. Proceedings of the TARA 2000 Conference Novi Sad, Yugoslavia, September 6-7, 2000. VOL. 30, No. 2, 2000, 113-123.

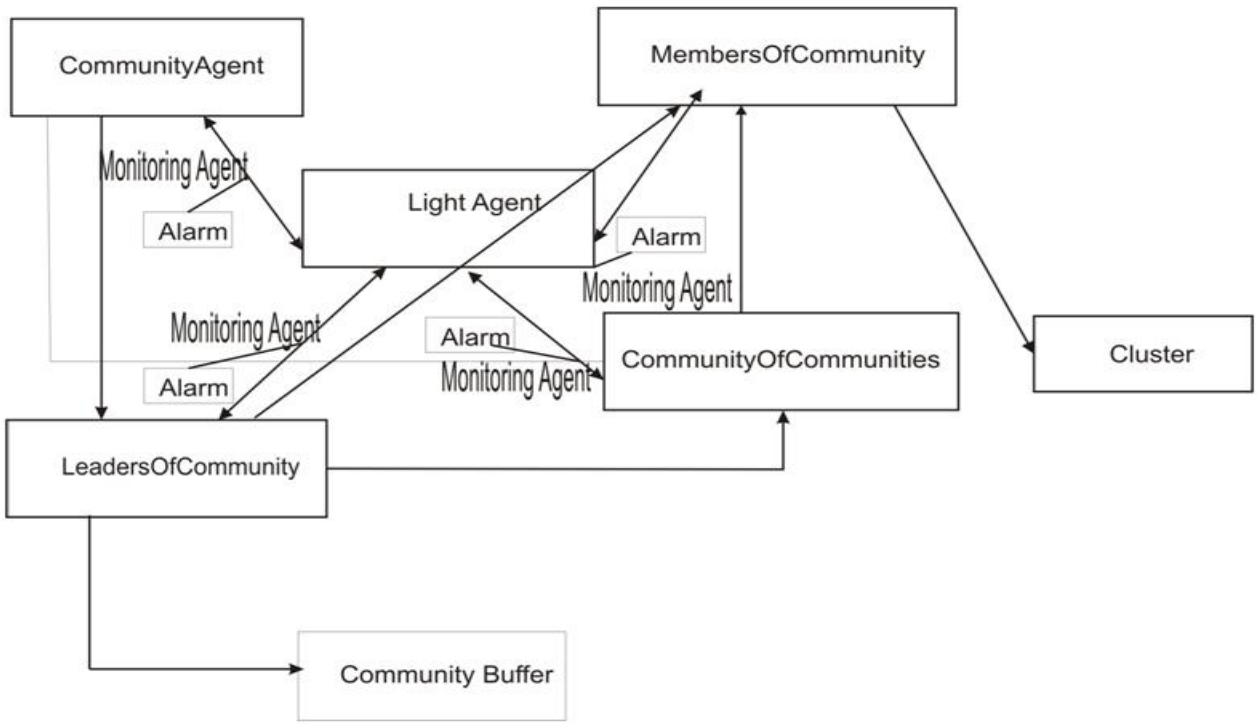

Figure 1. Architecture of Intrusion Detection in Virtual Knowledge Communities

```
If Monitoring agent M1 is not locally present in the community C
        Then declare the community as unsafe and report to the light agent L
    Else
        for all agents(in parallel) such as  Ai which has registered with L
            (internally or externally) and connected to Monitoring agent M
            Then declare the community C as safe
            End for
    End if
    A community on detecting an intruder
    If  Monitoring agent M on detecting an intruder in a community C
        Then
                Trigger the alarm and send light agent to community of Agent A
        Else
            Knowledge sharing activities continue
        End if
```

Figure 2. Algorithm for Intrusion Detection in VKC