DETECTING DDOS ATTACK IN AN AGENT-BASED VIRTUAL KNOWLEDGE COMMUNITY

G. O.Ogunleye
Department of Mathematical Sciences (Computer Science Programme), Redeemer's University, km 46, Lagos-Ibadan, Expressway, Redemption Camp., Ogun State, Nigeria

O.S. Adewale, B.K. Alese
Department of Computer Science, The Federal University of Technology, Akure, Ondo State, Nigeria

ABSTRACT: Virtual knowledge community (VKC) is a virtual place where agents can meet, communicate and interact among themselves. However, security is a basic challenge in a VKC networked environment. Distributed Denial of Service (DDoS) is currently a prevailing threat in the network communities. In this paper, we set up an experiment using the vmware workstation and Java Agent Development (JADE) as our test-beds to ascertain the detection of DDoS in VKC environment. Our contribution in this paper is to monitor the arrival rate of each of the source ip address. Consequently, ip address that has the highest occurrence within a particular time is suspected to be a DDoS attack. A graph is embedded in our work to illustrate our approach.
KEYWORDS: DDoS, Mobile Agent, VKC

I. INTRODUCTION

Distributed Denial-of-Service attack (DDoS) is one of the most prominent threats facing internet community. DDoS attack usually attempts to overwhelm the victim so as to deny their services to legitimate users. It is categorized into three types, TCP SYN [BW04], UDP, and ICMP flooding. First and foremost, TCP SYN flooding attack always target at the exhaustion of system resources. Zombie agents disperse several SYN packets spoofed with inaccessible source addresses such as in TCP 3-way handshaking. Afterwards, the backlog queue of the victim is bombarded with SYNs. Finally, it becomes a denial-of-service state as the system waits on ACKs endlessly. Some years ago, commercial popular sites such as Yahoo, Amazon and eBay were being compromised and were out of service for many hours due to the DDoS attack on February 2000 [SHH07]. Subsequently, DDoS attacks have grown in size, frequency, sophistication and severity. In general, DDoS attack employs different number of Zombies to originate a flood attack against an unsafe single site or system. DDoS attack can be originated in 2-phases: recruiting and action phases [CMO04]. Recruiting phase is when an attacker selects the machine by injecting a malware while Action phase is when some selected machines send attack packets to the victim after the attacker's command. Mobile agents are "self-contained and distinctive computer independent programs, bundled with their code, data, and execution state that can move within a heterogeneous network of computer systems. They have the ability to suspend their execution on an arbitrary point and transport themselves into another computer system [-[***96]. Mobile agents have distinct features which can help DDoS detection in different ways. A virtual knowledge community is an environment or platform where agents share and exchange knowledge [***00]. Virtual Knowledge Communities (VKC) is made up of community of communities, agents and community. These agents share resources and communicate with themselves. While the VKC domain might seem exciting and promising, measures of trust and security must be applied to each agent to establish a secure connection for securing agents and resources in such a distributed environment. These singular features along with growing concerns for security attacks, involves a prompt solution in securing knowledge agents. Presently, there have not been effective ways of protecting bandwidth attacks in VKC due to the following reasons. IP and TCP can be used as dangerous tools quite easily. Since all web traffic is tcp/ip base, attackers can release malicious packets without being traceable. The only way to solve this problem is attack detection which is the main focus of this work. Because of the underlying nature of the VKC network where agents exchange resources through the internet, a abrupt increase of the traffic may be mistaken as an attack. In this, a coherent increase in traffics may not necessarily be attacks but just 'flash crowd' events where a large number of agents connect to the VKC network at the same time. Our aim in this paper is to monitor each of the source ip address in an agent based VKC network. However, there is a need for better approach of detecting bandwidth attacks. The only approach is to monitor the number of source ip addresses instead of the local traffic volume. The ip address that has the highest occurrence within a specified time is regarded as a malicious source ip address. This will thereafter help us to trace the attacker to a particular source. We illustrate our approach with a chart. The architectural

framework for the whole work and the results are presented in this research paper. The paper is organized as follows: related work are presented in section 2, section 3 presents the system design for our approach, results are shown in section 4, conclusions and future work are drawn in 5, and references are given in Section 6.

II. RELATED WORKS

A. *Network Security and threats*

Network security can be seen as a collection of services which [PR96]:
• Maintain the confidentiality and integrity of the message as well as the network;
• Provide for the authentication of users and services; and
• Make sure of non-repudiation by users and the non-denial of services.
A threat is simply a bridge of one or more security service. There are two categories of threats (or attacks) to a network environment. These are [Far07] Active and Passive attacks. This classification is based on their effect on the system. In an active threats or attacks, there is an attempt to change the data and harm the system. This form of attack can easily be detected but it is difficult to prevent. Passive attacks on the other hand are aimed to obtain information only. No modification is made to the data after interception. However, harm may be done to the receiver or sender of the message. For example, an attack may try to intercept a customer's account details. The system itself is not affected during the process. Before designing a secure system, it is important to identify the threats against which protection is required. Some researchers identified some security threats [PR96]:

- Identity interception is the observation of the identity of one or more parties involved in a communication for misuse.
- Replay attack is the recording and subsequent replay of a communication at some later point in time.
- Masquerading is the impersonation of a user to gain access to information, or to gain accidental privileges. This includes active attacks such as replay and modification of messages.
- Data interception is the observation of user data during a communication by an unauthorized user.
- Data manipulation is the unauthorized replacement, insertion, deletion or disordering of user data during communication.
- Repudiation is the denial by one of the entities involved in a communication of having participated in part or all of a communication. This may be dangerous in the case of electronic commitments.
- Mis-routing is the misrouting of a communication path intended for one user to another.
- Denial of service is the prevention or interruption of a communication or the delay of time-critical operations. For example, an intruder may suppress all messages directed to a particular destination or may generate extra traffic.
- Traffic analysis is the observation of information about a communication between users. The observation may include the absence/presence of traffic, frequency, direction, sequence, type and amount of traffic.

B. *DDoS*

Distributed Denial of Service Attack is infected by a malicious code act simultaneously and coordinated under the control of a single attacker in order to break into the victim's system, exhaust its resources, and force it to deny service to its customers [CMO04].

Types of DDoS
Attacks can generally be grouped as flood attacks and logic or software attacks.
Flood attacks operate by continuously sending large amounts of data to the victim or target machine. This flooding is designed to consume processing power and memory of the victim and/or network bandwidth and packet buffers. The latter kinds of attacks act by sending a number of malformed packets that exploit some vulnerability of software loaded at the victim.
These attacks can be easily counteracted by correcting or patching the software.
TCP SYN flood, UDP Flood, ICMP Flood and Smurf attacks are examples of flood attacks.
Whereas, Ping of Death, Tear Drop, Land and Echo/Chargen attacks can be an examples of logic or software attacks. These examples are by no means exhaustive list of DDoS attacks as there are different variations of these as well as other types of attacks.

C. *Flood Attacks*

TCP-SYN Flood: this attack utilizes the three way handshaking of TCP connections. An attacker initiates a connection request with spoofed IP address to the target machine. The target machine then replies accordingly and waits for a reply that never comes. This will hold up crucial resources of the target

machine like memory and processing power. As a result, users of the target machine will be denied of the services delivered to the attacker.
UDP Flood: as UDP is a connectionless protocol, an attacker can send a tampered packet to a random port of the target machine. When the victim receives this packet and finds no application is waiting on the port, it will generate destination unreachable ICMP packet. This packet is then sent to the source address of the received packet which is a bogus one. If the number of packets sent by the attacker is very large, most of the resources at the victim will be held up or eventually the machine will go down.
ICMP Flood: this type of attack generates a bunch of pings and UDP packets targeted at the victim. This bombardment will slow the network connectivity and eventually leads to loss of connectivity. Most of the connections of the target machine will be lost as a result. Smurf Attack: in this case an attacker sends forged ICMP echo packets to broadcast addresses of vulnerable networks. All the systems on these networks reply to the victim with ICMP echo replies. If the number of packets generated by the attacker is large, the bandwidth available to the target is rapidly exhausted, effectively denying its services to legitimate users.

D. Adaptive Security Model for Detecting DDOS Attack in Virtual Knowledge Communities

[OAA12] developed a DDOS attack models for detecting attack traffics in VKC and proposed measures to deal with such an attack but the security of the whole system is yet to be presented which is the main focus of this paper.

E. Detection of DDoS Attacks using Data Mining

[GC11] discussed various detection algorithms which are using data mining concepts and algorithms such as intrusion detection for DDoS detection and prevention.

F. Intrusion Detection Model in MANETs using ANNs and ANFIS

[MT11] proposed different approaches to implement and improve the security level of Mobile Ad hoc Networks. They designed a mechanism for intrusion detection and security framework to detect a security attack. In a type of attack considered in this research, an intruder node injects a large amount of junk packets into the network and causes a denial in the services of the attacked node to the network. The model was developed using 2 method of detection – ANFIS and ANNs – in a simulated environment. It was showed that almost all of models could detect Dos attack effectively.

G. Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks

[SHH07] suggested the effective DDoS defense system which used the collaborative scheme among distributed IDRSs located in the vicinity of the attack source or victim network. In the scheme, both victim and source-end (Intrusion Detection and Response System) IDRS work synergistically to identify the attack and avoid false alarm rate up to great extent. Additionally, the author proposed the duplicate detection window scheme to detect various attacks dynamics which increase the detection threshold gradually in early stage.

H. Virtual Knowledge Communities

[MC09] called the VKC as the virtual place where agents can meet, communicate and interact among themselves. However security is a fundamental concern for virtual communities. Quite a number of researchers that have worked in the VKC and agent based environments [P+07, End07] have all pointed out the necessity for better solutions to intrusions and other security problems associated with this research area.

III. METHODOLOGY

Our DDoS detection system detects security breaches through some rules which we have pre-entered in the system. The rule is if { condition } then { act }. This means if the percentage of a particular ip_address occurs outrageously more than the others within the same time slots, then such ip_address is log out of the network. We set up an experiment to demonstrate the bandwidth attack as shown in figure 2.
When shadow agents receive a command from the master server agent, they begin to send an attack to the resource. The shadow agent in this approach represents the zombie agents. The Data Collection agent sits at the victim's end to record various attack traffics. The data collected is summarized in one second intervals. The summary includes the total number of packets arrived, the total number of TCP SYN packets and the total number of distinct source ports. Figure 1 shows the architecture for the DDoS detection in VKC environment.
From the architecture, when the attack is initiated by the Attacker agent by sending the attacking command, the command is replicated by the shadow agent also known as the zombie agents.

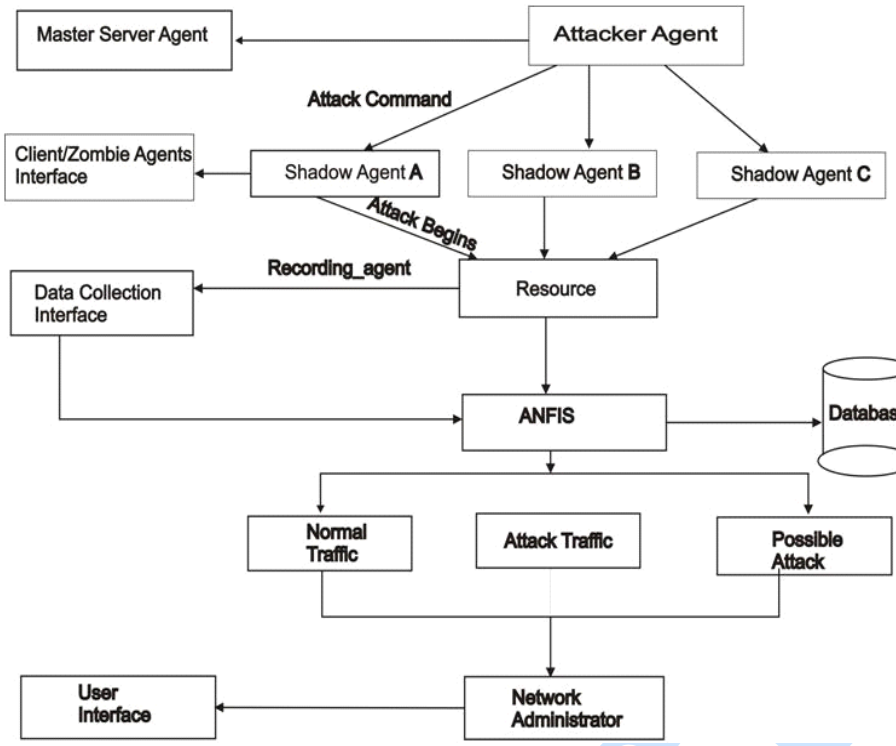

Figure 1: DDoS detection in VKC environment

The resource that was attacked is the bandwidth available. The recording agent which is the data collection interface sits at the victims end to record the various traffics generated. The traffic classification categorizes traffic into normal, attack and possible attack. The benchmark for the classification is already embedded in the chart which is based on the ip_addresses that take more than 50% of the bandwidth consumption.

The algorithm for the behavioral properties of the agents is shown as follows.

-Attacking agent initiates attack command

-Attack command is started and being replicated by the shadow agents

-Recording agent starts to record various network activities

-Trafffic is displayed through the Tcpdump agent who shows the total tcp syn attacks generated, the total number of distinct source ports.

-A chart is generated with the percentage consumption of bandwidth usage of each of the ip_ address

-If an ip_address has the highest percentage consumption within the same duration time that is > 50%

-Then DDoS is suspected and connection from suspected ip_address is terminated.

IV. SYSTEM IMPLEMENTATION

The Java Development Kit, Netbeans IDE 6.5, Vmware workstation, Mint, Ubuntu and Linux Windows 7 operating systems were the tools for the implementation. All the three operating systems were installed on the Vmware workstation. Thus, the victim agent which is our target agent was developed on JADE platform in Windows 7 which was flooded with DDoS attack. The system has the capability of generating both the attack and normal traffics.

We ran the application on Mint operating system, to generate one zombie attack. Furthermore, the attack was likewise run simultaneously both on Mint and Ubuntu operating systems, to generate two zombie attacks. Thus, metasploit was used as our attacking tool and was installed on Mint and Ubuntu operating system. Metasploit floods the attacking or target agent with tcp syn flood attack to generate attack traffics.

The total tcp syn flood attack was calculated coupled with the total number of distinct source ports. Figure 2 shows the tcp syn flood attack generated in mint operating system. The attack was set for just 10 seconds due to the degrading effect of the attack on the network.

The same approach was also repeated on the Ubuntu operating system as we can see in Figure 3. The same duration time was used as well.

Figure 4 represents the total packets, the total tcp syn packets and the total distinct source ports. This is shown in the output window of the Netbeans.

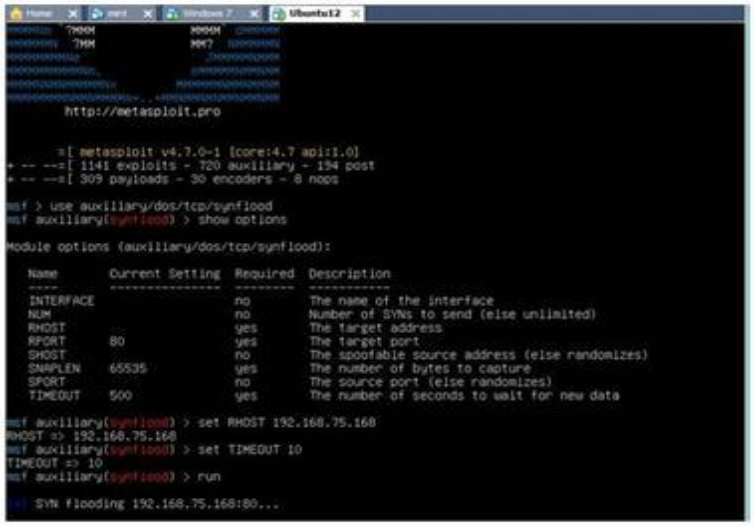

Figure 2: The Mint operating system showing the tcp syn flood attack

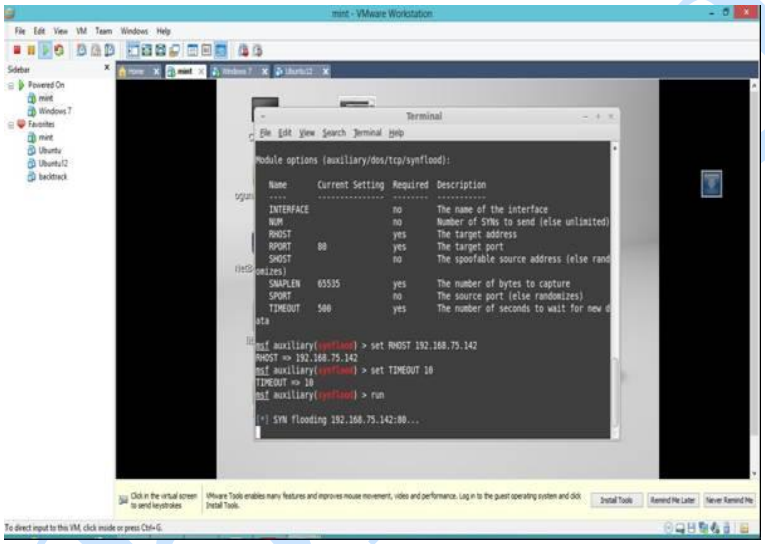

Figure 3: The Ubuntu operating system showing the tcp syn flood attack

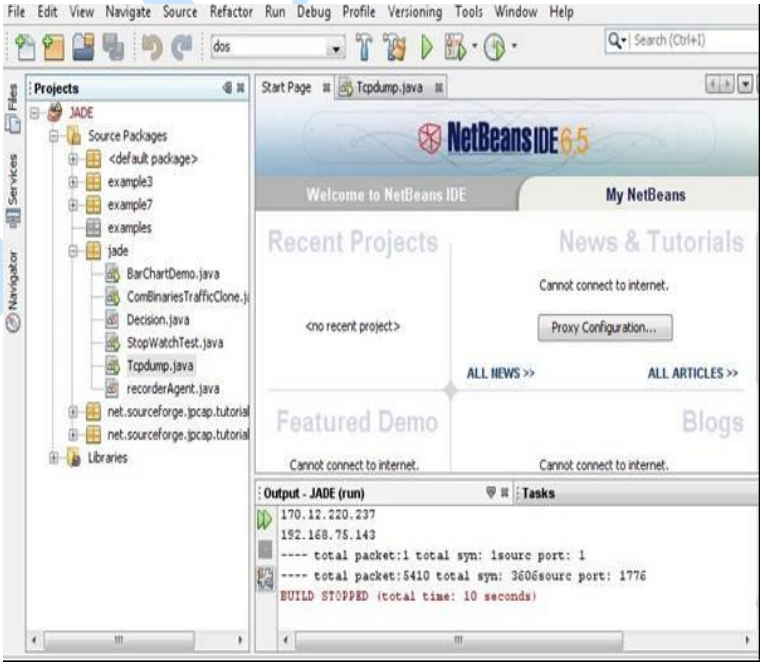

Figure 4: Total packets, total number of tcp syn packets and the total source ports

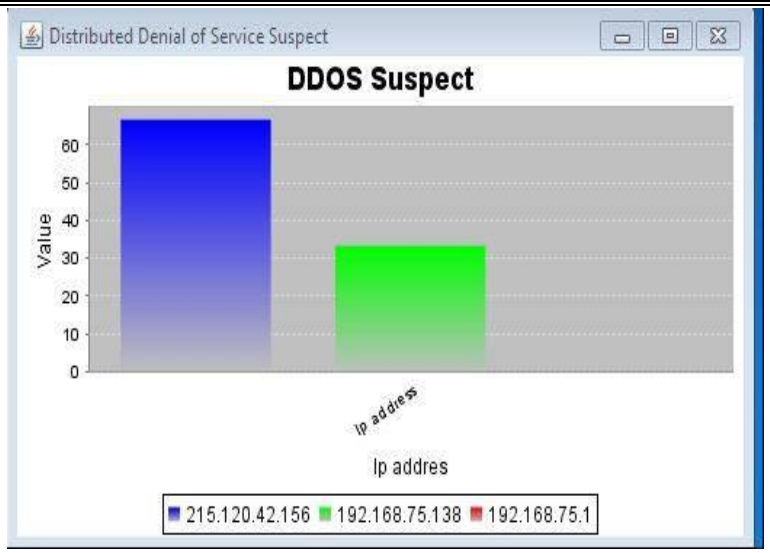

Figure 5: DDoS chart for one zombie attack in VKC network

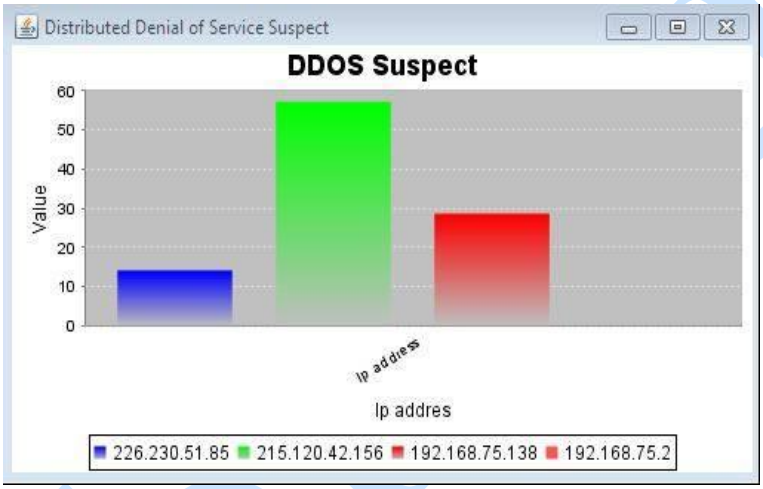

Figure 6: DDoS chart for two zombies attack in VKC network

We used a parameter as a benchmark for categorizing into normal traffic, attack traffic and possible traffic. In figure 5 and 6, we have the percentage value on the vertical axis and ip address on the horizontal axis. The threshold was taken to be 50%. Any ip_address that shoots up more than 50% bandwidth consumption with the time slots as others is regarded to be a threat and at such, it is suspected to be a DDoS attack.

In the chart, if the source ip address output of any agent is greater than 50% and occupy a large percentage of the total bandwidth; in that case we suspect a DDoS attack. When the output is between 35 and 49%, we suspect a possible attack. But when the output is below 35%, we assume that it is a normal traffic network. Figure 5 shows the chart for one zombie attack. The ip_address with 215.120.42.156 takes 65% of the bandwidth consumption compared to other ip_addresses within the same duration time slot.

The same procedure was also repeated for two zombies attack. The attack was simultaneously launched on Ubuntu and Mint operating system for 10 seconds.

Figure 6 is a real scenario of a DDoS attack. The chart is shown in figure 6. ip_address 215.120.42.156 had 55% while Ip_address 226.230.51.85 had just 15%, ip_addresses 192.168.75.138 and 192.168.75.2 have 29%. Thus, ip_address with 55% was suspected to be a DDoS attack and hence such an ip_address is suspected to be a malicious one and in that it is log out of the network. Ip_addresses with 15% and 29% were taken to be normal traffic.

V. CONCLUSION

With the development of computer networks, DDoS attacks have become a threat to the network users especially in a competitive environment and therefore there is a need to develop a more robust system capable of detecting and preventing the effect of this malicious attack. We have simulated how to detect DDoS attack in VKC network. Results were only performed for one and two

zombies' attacks. We classified an ip_address that occupied more than half of the bandwidth as being suspicious and as such is categorized into attack traffic. Efforts are currently ongoing to use more sophisticated approach to detect DDoS attack in this multi-agent environment called VKC network. Furthermore, future direction would involve gathering data to categorize traffics into normal or attack with the use of adaptive neuro-fuzzy inference system popularly known as ANFIS.

REFERENCES

[BW04] **P. Braun, R. Wilhelm** - *Mobile Agents: Basic Concepts, Mobility Models and the Tracy Toolkit*, published by Morgan Kaufmann (December 22, 2004), ISBN-10: 1558608176.

[CMO04] **P. Charalampos, M. Michalis, Z. Olga** - *Distributed Denial of Service Attacks*, National Technical University of Athens, Retrieved from http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html (2004).

[End07] **R. Endsuleit** - *Robust and Private Computations of Mobile Agent Alliances*, PhD Dissertation, University of Karlsruhe, June 2007. Retrieved from iaksww.ira.uka.de/calmet/dissertationen/diss_endsuleit.pdf (2007).

[Far07] **B. Farouzan** - *Cryptograpgy and Network Security*, New Delhi: McGraw-Hill, 2007.

[GC11] **Kanwal Garg, Rshma Chawla** - *Detection Of DDoS Attacks Using Data Mining*, in International Journal of Computing and Business Research (IJCBR), Volume 2 Issue 1, 2011.

[MC09] **P. Maret, J. Calmet** - *Agent-Based Knowledge Communities*, International Journal of Computer Science and Applications, Vol. 6, No. 2, pp 1-18, 2009.

[MR04] **J. Mirkovic, P. Reiher** - *A Taxonomy of DDoS Attack and DDoS Defense Mechanisms*, ACM SIGCOMM Computer Communications Review, Volume 34, Number 2, April 2004, pp. 39-53.

[MT11] **Zahra Moradi, Mohammad Teshnehlab** - *Intrusion Detection Model in MANETs using ANNs and ANFIS*, International Conference on Telecommunication Technology and Applications Proc. of CSIT, 2011.

[OAA12] **G. Ogunleye, O. S. Adewale, B. K. Alese** - *An adaptive security model for detecting DDOS attack in virtual knowledge communities*, Computing and Information Systems Journal, University of the West of Scotland, United Kingdom, Vol. 16 No. 1, pp 31-38, 2012.

[PR96] **M. Prabhu, S. Raghavan** - *Security in computer networks and distributed systems*, Computer Communications, Vol. 19, No. 5, pp. 379-388, 1996.

[P+07] **J. Portillo-Rodriguez, V. Aurora, P. S. Juan, P. Mario, N. A. Gabriela** - *Fostering Knowledge Exchange in Virtual Communities by Using Agents*, Springer Berlin / Heidelberg, (Lecture Notes in Computer Science), Volume 4715 pp. 32-39, 2007.

[SHH07] **B. Song, J. Heo, C. Hong** - *Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks*, IEICE TRANS. COMMUN., VOL. E90–B, NO.10, 2007.

[***00] *** - Coordinate Center CERT Advisory CA: denial-of-service developments, Available at http://www.cert.org/advisories/CA-2000-01.html, 2000.

[***96] *** - Emergency Response Team, CERT Advisory CA-TCP SYN Flooding Attacks, http://www.cert.org/advisories/CA-1996-21.html, Sept. 1996.