IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

Agents Based Countermeasures to DDoS Attacks

Upinder Kaur[1], Dr. Payal Jain[2]

Assistant Professor, Department of Computer Science, G.M.N. College, Ambala Cantt, Haryana[1]

Lecturer, Department of Computer Science and Application, G.M.N. College, Ambala Cantt, Haryana[2]

Abstract: Distributed Denial of Service (DDoS) attack combines resources of multiple Zombies (Compromised Systems) to attack a single victim makes it impossible to work properly. DDoS is one of the various supreme challenges and the existing literature reveals the fact that although there exist various mechanisms to handle DDoS attacks but still there exist a gap amongst the security requirements & existing mechanisms. Therefore, a mechanism that is strong and reliable is desired. Software agents seem to be a strong candidate for defending DDoS attack. This work highlights the importance of software agents as a security staff for avoiding DDOS attacks. Also it proposes a multi agent framework detecting, protecting and source tracing DDOS attack.

Keywords: Distributed Denial of Service (DDoS), Compromised Systems, Software agents, DDOS attacks.

1. INTRODUCTION

With the movement of businesses form private to public networks. Electronic media gives summons to the unnecessary intrusion. According to a report[1] different way that the hackers might be using in 2009 will be through social media sites, Portable Document Format (PDF) and flash files etc. In spite of huge increase in direct IT security expenditures, which are expected to reach $79 billion annually by 2010[2], the impact of such attacks has not been reduced. Unfortunately there is no universal solution that can provide 100% security services due to internet's distributed nature [Pleeger, 1997][Losco, 1998]. Generality, Not exploitable & policy are some desirable requirements of framework for responding to DDoS attacks. A recent cyber attack is on UK MoD system security where a hybrid computer virus/worm [January, 2009] penetrated the security system. This paper is structured as follows: Section 2 introduces DDoS attack and discusses the current security scenario. Section 3 justifies the need of software agents as security staffers. Section 4 proposes multi agent framework for detecting, protecting and source tracing DDOS attack. Finally Section 5 concludes with pros and corns of proposed framework.

2. DDOS ATTACKS

Distributed Denial-of-Service (DDoS) attack in which the victim network element(s) are bombarded with high volume of fictitious, attacking packets originated from a large number of machines [Kim et.al]. A successful attack allows the attacker to gain access to the victim's machine, allowing stealing of sensitive internal data and possibly cause disruption and denial of service (DoS) in some cases. DoS incidents in any organization posses a big challenge and are increasing at a very high speed. [Gresty et.al]. Nearly 40 % of total attacks faced by business on Internet are Denial of service (DoS) attack. Out of the various categories of DoS attack such as flooding, software exploit, protocol based etc Distributed Denial of service attack is the most prominent. In fact DDoS attack uses series of Zombies to initiate a flood attack against an unsafe single site.

DDoS attack is initiated in 2-phases: -

- Recruiting phase: - Attacker selects the machine by injecting a malware.
- Action phase: - Selected machines send attack packets to the victim after the attacker's command [Branom 2007].

Trinoo, tribe flood network, stacheldraht, shaft, mstream etc [Gong, 2003] are some tools to activate DDoS attacks. Today protocol based initiated DDoS attacks are tough to handle because they don't require any special privileges on the part of attacker. Numbers of proposals are given to either defend or prevent against DDOS attack such as starting from increasing the resourced at defender side, implementing authentication policies at routers, filters, firewalls with hardware security appliances, Learning based mechanisms, agents based detection at host level or at immediate level etc but none of them has proved to be the best addressing all of the challenges therefore there is a strong need to bridge the existing gaps among various security solutions.

[1] Predicting Cybercrime In 2009!.htm
[2] Information Security Products & Services – Global Strategic Business Report, Global Industry Analysts, Inc., July 2007.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

3. RELATED WORK

This section presents the related works & explores various challenges in the DDoS attack.

An Electronic attacks on Ethiopia in 2007 shows extreme face of cyber attacks[1]. These were denial of service attacks, where an attacker floods the target network with bogus messages, causing its servers to slow or shut down [Lewis 2007].

Georgia Tech Information Security Center (GTISC) believes strongly that a proactive and collaborative approach to understanding emerging threats will be helpful in developing more effectual information security technologies and strategies [Ahamad 2008].

Lee described the DDOS attack architecture and propose taxonomies to characterize the scope of DDOS attack, the characteristics of software attack tools used and the countermeasures available. But suggested that with the expansion of Internet more comprehensive solutions and counter measures to DDoS attacks must be developed, verified, and implemented. [Lee et al, 2004]

Author in [Gresty] has described important issues, which make network DoS a difficult security problem & has also discussed various solutions and presents requirements for a framework for the management of response to network DoS incidents.

The work provided by Catherine suggested a frame work for evaluating a protocol for defending DoS attack involving resource exhausting that is intended to make maximum use of available tools that are applicable to cryptographic protocols & that can be applied to any protocol that uses authentication, weak or strong to protect against denial of service. [Meadows]

Researchers introduce a framework for classifying DoS attack based on header contents, ramp-up behaviors and novel techniques based on spectral analysis. With this they agree on when large attacks occur like root server attack additional-detection sites would provide more insight when projecting the prevalence of DoS activity on the internet [Hussain, 2003].

Although Parashar suggested an approach of detecting a DDOS attack within the intermediate network by using a gossip based communication mechanism to exchange information about the overall network attack observed. Finally concludes that if more intelligent gossip strategies are used than overhead while detection can be reduced. [Zhang, 2005]

Hacker can use different ways for executing attacks successfully. Author [Seufert and O'Brien 2007] explores the effectiveness of machine learning techniques in developing automatic defense against DDoS attacks based on artificial neural networks but these techniques has not been extended for multiple algorithms.

Stefan proposed a simulation environment which offers an agent based simulation approach, packet-based simulation of attacks and defense systems and capability to add new attacks and defense methods and investigate them but there is a strong desire to improve functionality of the simulation environment and further investigate new defense mechanism for better output [Kotenko and Ulanov, 2007].

4. SOFTWARE AGENTS AS SECURITY STAFFERS

"An agent is any hardware or software entity which is autonomous and has the ability to act on behalf of others, can perceive the changes in the environment and react according to them with the help of features like mobility, learning ability etc."

The software agents not only provide the competitive advantage by improving process quality but also integrate the new technology and specialized expertise.

Agent technology finds its applications in wide areas such as user interfaces, mobile computing, information retrieval and filtering, smart messaging, telecommunications and the electronic marketplace. The software agents are inherently

[1] Internet News Real time IT News – Is Cyber terrorism' aReal Threat.htm

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

autonomous, pro-active, reactive, benevolent and rational. The smart agents interact with each other in a multi-agent system in various ways. The clusters of agents in a multi-agent framework are competitive, cooperative, and task-oriented and can also provide an interface to users .

The characteristics that motivate the use of software agents as security monitoring functions are: autonomy, fault tolerant, resists subversion, configurable, robust, dynamic-configuration, and information providers, task-oriented, scalable, atomic and isolated. The agent architecture also reveals software reusability. Many security mechanisms have been proposed to mitigate agent-to-agent, agent-to-platform, and platform-to-agent security risks. Once designed, agents can interchange their roles in order to fulfill the user's demand.

The aim of incorporating software agents as an element of network security is to ensure that the business can continue to process legitimate traffic while under attack; and create a scalable, adaptable solution that addresses DDoS attacks now and in the future. The agent-based framework is proposed in the upcoming section.

5. PROPOSED FRAMEWORK

This section proposes multiagent framework, which aims to detect, prevent & perform source tracing of DDoS attack at a network site. A pictorial representation of the framework is given in a figure 1.

Primarily the proposed frame work coprises of 3 components namely **H**ost**A**gents(HA),**C**ontroller(C)and **F**ilter(F).

Host Agents (HA): Host has its own agents to gather information by having communication with filters. Filters will provide filtered information to HA be used by the concerned computer.

Controller: It process information gathered by MA periodically and if the filters detect any DDOS then it take appropriate action. It also check for that if agents should not acting as an compromised machine if it is then locate that master and communicate to rest of the networks or hosts therefore doing source tracing.

Filters: Filters hold the criterion of DDoS attack check. Also contains the block IPs & update it periodically & immediately in case an unauthenticated source is traced.

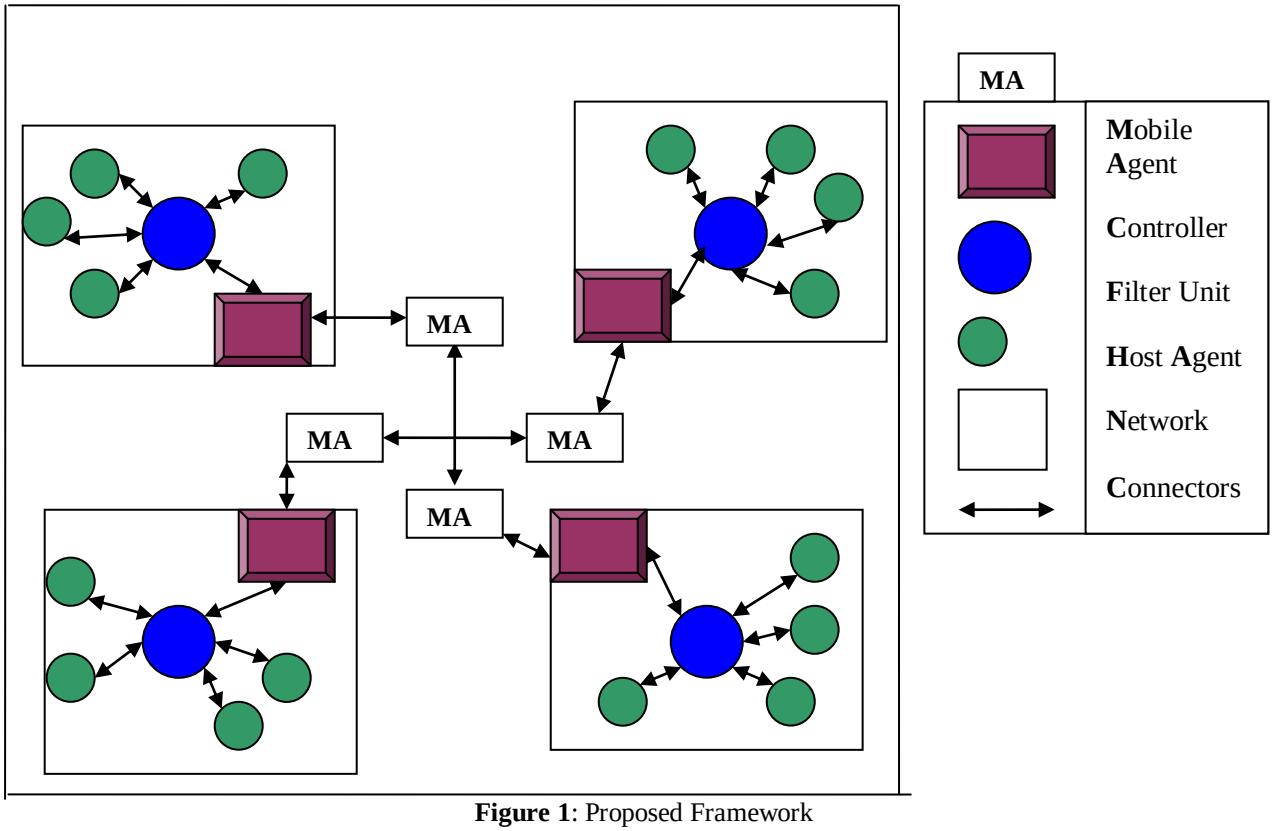

Figure 1: Proposed Framework

DOI10.17148/IJARCCE.2017.6868

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

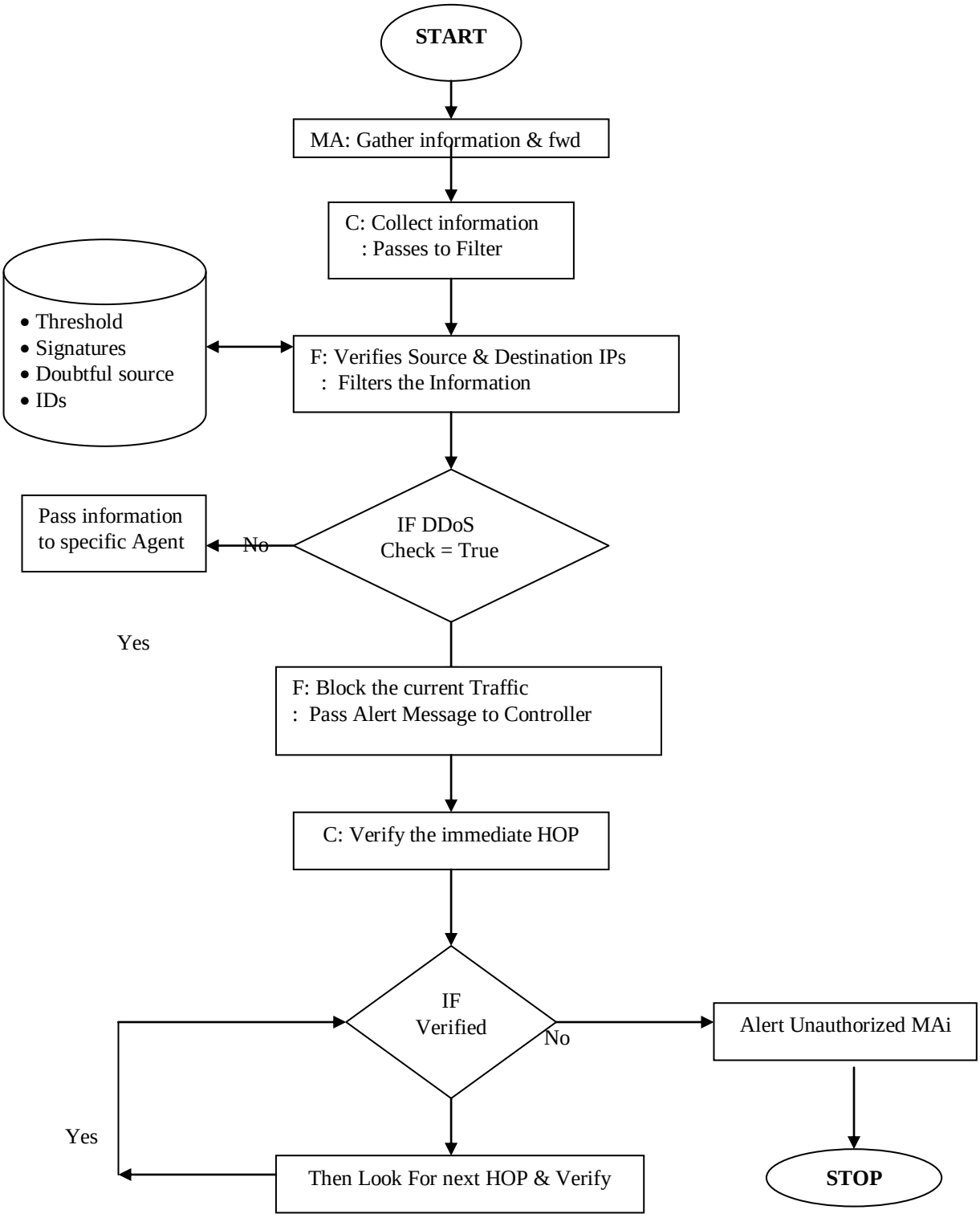

Figure 2: Flowchart of proposed framework.

5.1 Working

This framework works as after MA gathers information from its neighborhoods it passes it to the Controller. Controller forward it to the filter for its verification, filter after applying different detection mechanisms if found any DDoS scenario then informs the controller for the same else forward the information to the concerned software agent. In case of DDoS attack controller check the immediate HOP for the authentication. If it proofs its validation the next hop is checked otherwise alert is send to all nodes about the compromised hop. This framework uses Bottom-Up approach for source tracing. The algorithm, which shows the complete working of the framework, is given in the figure 2.

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 8, August 2017

6. CONCLUSION

Due to the migration from private intranet to the public Internet, organizations are becoming too much prone to the attacks initiated by the hackers for their erroneous purposes. Therefore, security of the original data becomes the biggest issue in front of the owner. This work presents a framework that detects, prevent & trace the source of the attack. Above framework has a capability of tracing a source apart of detecting an attack but still it is not sure that how many Software agents can be used. How we can trust the validity of an agent is a big issue that can be handle in a future.

REFERENCES

[1] Adam branom" Denial of service attack detection and mitigation"November 2007
[2] Alefiya Hussain, John Heidemann, and Christos Papadopoulos Frame Work for Classifying Denial of service attacks" SI-TR-2003-569, 25,Feb 2003{Hussain,johnh,christos}@isi.edu
[3] Catherine Meadows "A Frame Work For Denial of Service Analysis" Code 5543, Naval Research Laboratory. meadows@itd.nrl.navy.mil
[4] C. P. Pfleeger, "Security in Computing", ISBN:0131857940, Prentice Hall, 1997
[5] D Bénech, T Desprats, and Y Renaud, "KQML-CORBA based architecture for intelligent agents, communication in cooperative service and network management", Proc 1st IFIP Conference on Management of Multimedia Networks and Services, July 1997.
[6] D.W.Gresty,Q.Shi,M.Merabti,"Requirement for the General Framework For Response to Distributed Denial of Service Agents"
[7] Dr Fengmin Gong" Deciphering Detection Techniques: Part III Denial of Service Detection", , Chief Scientist, McAfee Network Security Technologies Group Jan 03
[8] Guangsen Zhang, Manish Parashar "Cooperative Defense against DDoS Attacks" fgszhang,parasharg@caip.rutgers.edu
[9] Igor Kotenko and Alexander Ulanov "AGENT-BASED SIMULATION ENVIRONMENT AND EXPERIMENTS FOR INVESTIGATION OF INTERNET ATTACKS AND DEFENSE" Proceedings 21st European Conference on Modeling and Simulation Ivan Zelinka, Zuzana Oplatková, Alessandra Orsoni ©ECMS 2007 ,ISBN 978-0-9553018-2-7 / ISBN 978-0-9553018-3-4 (CD)
[10] James A. Lewis, Director, Technology and Public Policy Program "Cyber Attacks Explained" June 15, 2007.
[11] Mustaque Ahamad, Dave Amster "Emerging Cyber Threats Report for 2009" GTISC Emerging Cyber Threats Report 2008
[12] Ousterhout, J, "TCL: An Embeddable Control Language", USENIX conference, 1990.
[13] P Maes, RH Guttman, and AG Moukas. "Agents that buy and sell," Communications of the ACM, Vol.42, No.3, March 1999, pp.81-91.
[14] P.A. Loscocco et al, "The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments", presented at NIST'98, 1998. http: /csrc.nist.gov/nissc/1998/ proceedings/paperF1 .pdf
[15] Stefan Savage UC San Diego, Fred B. Schneider Cornell University "Security is Not a Commodity: The Road Forward for Cyber security Research" Version 4: February 3, 2009
[16] Stephen M.Specht, Ruby B.Lee "Distributed Denial of Service: Taxonomies of Attack, Tools and Countermeasures" Proceedings of the 17th International Conference on Parallel and Distributed Computing Systems, 2004 International Workshop on Security in Parallel and Distributed systems, pp.543-550, September 2004.
[17] Stefan Seufert and Darragh O'Brien, "Machine Learning for Automatic Defence against Distributed Denial of Service Attacks" IEEE Communications Society ,publication in the ICC 2007 proceedings.
[18] Top Layer "The importance of Denial of Service (DoS) Security Appliances" September 2002
[19] Y Shoham, "Agent-Oriented Programming," Artificial Intelligence, Vol. 60, No. 1, 1993, Pp. 139-159.
[20] Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah and Jonathan H. Chao "Packet Score: Statistical-based Overload Control against Distributed Denial-of-Service Attacks"2002