Simulation Models for the Evaluation of Detection and Defense Protocols against Cyber Attacks

Preparation of Doctoral Consortium Contributions

Lorena Molina Valdiviezo

University of Calabria, Department of Computer Engineering, Modelling, Electronics and Systems (DIMES), Vía P. Bucci, Rende, Italy

National University of Chimborazo, Faculty of Engineering, Riobamba, Ecuador

Keywords: DDoS Attack, Network Security, Network Simulation, Application-Level Simulation.

Abstract: Issues related to Cyber Security aspects, mainly focused on the security of computer systems and the services they offer, have gained considerable importance. The companies and even national governments, are incessantly affected by these issues to ensure the integrity of information systems and data managed through occurring in networked environments. Distributed Denial of Service (DDoS) flooding attack is one of the most diffused and effective threat against services and applications running over the Internet, in this sense, the research is primarily aimed at the study (assessment and validation) of hybrid models for detection, defense and response (R) for DDoS attacks, especially in the application layer, and the identification of new strategies. This research is based on modelling and simulating different scenarios using NeSSi2 and ns-3 as network simulation tools.

1 STAGE OF THE RESEARCH

In modern society, the exchange of information by means of equipment and computer systems and the parallel specialization of hackers has reached levels that make crucial the issues related to information security (Cyber Security).

Security is a continuous process in the protection, detection and defense against cyber attacks. Security is not a one-time single-points fix, but a rather a cycle, so in this sense, it is fundamentally a modeling and simulation approach against cyber attacks. This research will focus especially on Distributed Denial of Service (DDoS) flooding attacks occurring in networked environments. (Zargar et al. 2013)

Denial of Service attack is an attempt by an attacker to exhaust the resources available to a network, so that users cannot gain access application or service. Distributed Denial of Service (DDoS) attack takes place when many compromised machines infected by the malicious code simultaneously and are 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. (Patrikakis et al. 2004).

There are two categories of DDoS attacks, typical DDoS attack and DRDoS attacks. A DDoS attack, consists of master zombies and slave zombies. The hosts are compromised machines that have arisen during the scanning process and are infected. The attacker sends an attack command to master zombies and activates all attack processes on those machines, which are in hibernation, waiting for the appropriate command to wake up and start attacking. The zombies network commands them mount a DDoS attack against the victim, send attack commands to slave zombies through the processes. The slave zombies begin to send a large volume of packets to the victim, flooding its system with useless load and exhausting its resources, (see Fig.1). An attacker prefers to use source IP addresses for two major reasons: first, the attackers want to hide the identity of the zombies network so that the victim cannot trace the attack, and the second reason concerns the performance of the attack (Yu et al. 2010).

DDoS attacks continue to grow in size, frequency and complexity, forcing network-dependent companies to implement a plan for

Valdiviezo L..
Simulation Models for the Evaluation of Detection and Defense Protocols against Cyber Attacks - Preparation of Doctoral Consortium Contributions.

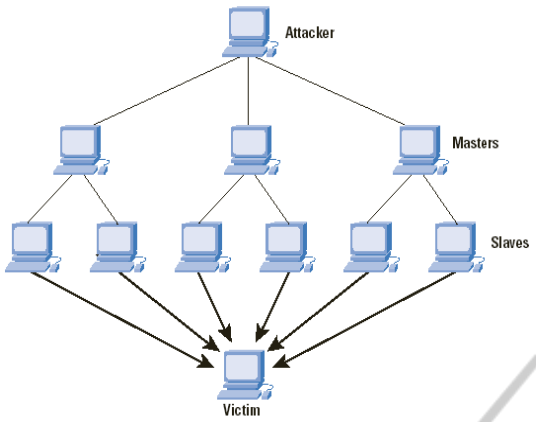

Figure 1: DDoS Attack.

protection, detection and defense, so in this sense, we have developed and implemented some basic models of DDoS attack scenarios using the NeSSi2 (Schmidt et al, 2008) and ns3 (nsnam, Carneiro et al. 2011) network simulators. We are investigating the behavior of an extension (Furfaro et al. 2014) of the Stop-It (Liu et al. 2008) defense protocol in order to develop an improved hybrid protocol and evaluate it under different scenarios.

The operation of the StopIt mechanism (see Fig. 2) applied to a general communication architecture consisting of more Autonomous Systems (AS) connected throughout secure connections in order to avoid the address spoofing; each server who wants to activate the StopIt has to be equipped with an algorithm to detect an attack. Each AS owns a StopIt server within its domain and all the StopIt servers use IGP to exchange data with their AS and BGP to learn the presence of other StopIt servers in the neighbourhood. (Furfaro, et al. 2014)

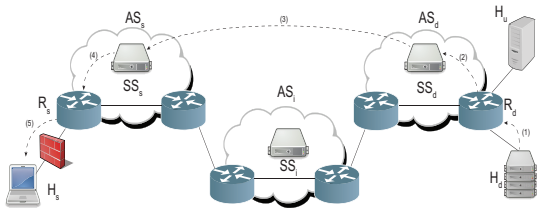

Figure 2: StopIt operation.

We validated the integration of the DiffServ model within the StopIt mechanism to overcome the main limitation of this standard filter-based technique with the aim of facing both direct and indirect DDoS attacks.

In the section 5.2 is simulated network and the results.

2 OUTLINE OF OBJECTIVES

The main goal of this research is to develop simulation models for the evaluation of mechanisms for the detection and defense against cyber attacks occurring in networked environments. The experience matured during the analysis of existing solutions will allow to acquire expertise in devising innovative defense and response strategies. The investigation will be initially focused on Distributed Denial of Service, which represents one of the most diffused and effective type of cyber attack.

Furthermore, this research work aims to make available to the community a benchmark that will allow to evaluate detection and defense mechanisms in computer networks so that it can ensure the quality of service.

The sub goals of this research are:

- Studying literature on Cyber Security and Network Simulation.
- Learning how to use existing Network Simulators.
- Studying literature on DDOS detection and response algorithms.
- Performing Comparative evaluation of Hybrid DDOS detection and response algorithms.

3 RESEARCH PROBLEM

Due to the advancement of technology and the excessive growth of the network, cybernauts are exposed to frequent attacks. That is why we are required to do an investigation to determine or establish defense mechanisms, using a simulation tool to simulate attacks and defenses.

Data networks are used to any human activity, this has given rise to individuals, organizations, nations, and governments depend on communication infrastructure to make their activities, this leads to the need to protect information.

A few years ago, the US-CERT (United States Computer Emergency Readiness Team) has received reports of users and administrators to network services on the anomalies and attacks on their systems; 73.4% were searches for access to resources, identification of ports, protocols, services or any combination to exploit vulnerabilities teams (Duarte, 2012).

The problem is to ensure that the tools (authentication protocols, encryption algorithms of information, digital signatures, attack detection algorithms, etc.), are placed to ensure the secure

exchange of information through the network and to provide the systems operating on it, the capability of defense and reaction to the attacks so that they work properly and are robust, it means able to respond appropriately even to anomalous situations compared to scenarios for which they were designed. The validation of the behavior of a software system is a complex engineering problem of crucial importance: it is known that the costs associated with the presence of a malfunctioning are higher if this is found late during the life cycle of the system. In the case of software for the secure exchange of information and for the defense against cyber attacks the problem is even more acute because the cost of corrective maintenance are added together, in the worst case, those related to illegal access by third parties to sensitive information exchanged on the network and / or inoperability of the system under attack. For these reasons it is essential to ensure the correct operation of the security software before it is used, possibly already in the planning stage. Where the complexity of the software does not allow to verify the correctness, appropriate validation tools should be used, which achieve good levels of confidence about the operation of it.

Several attacks are directed against service availability. These attacks impede the normal operation of the target systems. DDoS flooding attacks work by sending a large amount of messages to a destination, which is the victim of the attack, in order to consume its resources, e.g. by issuing requests that require a large processing time, by exhausting the available communication bandwidth or by exhausting its memory. Once a resource is exhausted, the legitimate clients can not use the service. Attackers can send a variety of packets, which could be similar to legitimate traffic and adopt, to a certain extent, the structure and arbitrary statistic, which greatly facilitates the concealment of the attack.

This leads to study and develop strategies to identify and face DDoS attacks in real time.

4 STATE OF THE ART

The most widely used techniques to study the behavior of software systems in the design phase, based on the definition, by means of formal specification languages, models, to an adequate level of abstraction such as to be capable of verification compared to formal requirements. In the case of complex systems, these techniques are not practically applicable and are often used to prototype by means of simulation tools.

There are different tools for information security such as firewalls and intrusion detection and defense system able to cope with a variety of cyber attacks, such as viruses, worms and other cyber attacks.

With regard to the DDoS attacks, there are several models of identification that are classified according to where the detection takes place and the response to the attack: at the source, at the destination or hybrid strategies. These are the ones that turn out to be more effective but also more difficult to implement and put in place.

In recent years the major threats to the Internet and data networks have been the attacks by worms and distributed denial of service (DDoS), identifying several models have been developed since 2000 and continue research to find mechanisms detection and defense in the network. (Duarte, 2012).

The author cites the need to insert devices in network intrusion detection systems (NIDS) in order to conduct an audit and a forensic analysis by reviewing the records (Nehinbe, 2010).

The research of (Zargar et al. 2013) exposed the need of a comprehensive, collaborative and distributed defense mechanism approach after they categorized the different DDoS flooding attacks and classified according to the ability to prevent, protect, detect, and respond to DDoS flooding attacks in real-time and as close to the attacks sources.

In this sense, the research is primarily aimed at the study (assessment and validation) of hybrid models for detection, defense and response (R) for DDoS attacks, especially in the application layer, and the identification of new strategies.

5 METHODOLOGY

The adopted methodology is based on the following steps:

1. Study of simple attack scenarios. At this stage, techniques used to execute DDoS attacks are studied and analyzed.
2. Modelling and Simulation. This phase is devoted to the development of basic simulation models of networked systems that allow to evaluate the behaviour of the involved nodes under various DDoS attack scenario.
3. Defense strategy design and implementation. During this stage, suitable defense strategies

are developed, e.g. by proposing enhancements to existing techniques.

4. Evaluation. During this phase, the devised strategies are evaluated by exploiting the developed simulation models in order to identify existing issues and to fix them by making the appropriate adjustments to improve the defense mechanism.

The above methodology exploits NeSSi2 and ns-3 as the network simulation tools.

The description of the modelling and simulation performed under different scenarios is described in the following sections.

5.1 Modelling with NeSSi2

We developed a simulation model of DDoS attack scenarios directed to a DNS server by using the NeSSi2 simulation environment.

NeSSi2, is an agent-based simulation environment, providing telecommunication network simulation capabilities with an extensive support to evaluate security solutions such as IDS. Special common attack scenarios can be simulated in NeSSi2. Worm-spread scenarios and botnet-based Distributed Denial of Service (DDoS) attacks are only two of the supported example attacks. (Grunewald et al. 2010)

NeSSi2 is built upon the JIAC (Hirsch et al., 2009) framework, a service centric agent-framework. The network entities, i.e. routers, clients, servers, or IDS (nodes in the following) are simulated with the aid of JIAC agents. Relying on configuration parameters and hardware characteristics, each agent simulates one or more nodes.

The application directs the malicious attack carried out by means of a certain number of hosts (zombies) of which has previously obtained control (botnets). The considered DDOS attack occurs in flood mode, or does in a way of inundating of packets the receiver in order to saturate its tail of arrival and the band at his disposal. This is achieved by ensuring that the hosts in the botnet to send to the appropriate DNS server as a response to queries that involve generating large packets. To generate these responses, the server is forced to employ a greater amount of bandwidth and computational resources at its disposal.

In this scenario, the attacker generates the establishment of several UDP streams towards the victim using a service port that is already active, so as to be more transparent to the machine on which it is hosted in the meantime will continue to carry out their tasks unaware. The attacker controls the zombie machines on which installs a simple service "echo" which generally uses a well-known port. When the attacker will have made its botnet send UDP packet through a specific port on a control signal that will interpret the zombie to start the bombardment.

The statistics obtained on NeSSi2 show that:

- The Server after a first initial period, is in crisis, beginning to deny the offer and blocking packets.
- The denial of packets leads to a degradation of service in terms of dropped packets divided according to demands of regular type:
  - Of the incoming packets are distinguished.
  - Packets that require a regular service
  - The packages targeted only to destroy the service.

5.2 Modelling with ns-3

The ns-3 is a discrete-event network simulator for Internet systems. It is free software, licensed under the GNU GPLv2 license, and is publicly available for research, development, and use. The ns-3 project, started in 2006, is an open-source project developing *ns-3*. (ns-3 Manual).

In the ns-3 simulator, we developed components by introducing suitable classes, that inherit from the ns-3 Application base class, which respectively act as a DNS server (victim), StopIt servers, routers supporting packet filtering and DNS clients as shown in Fig. 3. The behavior of the DNS Server is represented by the finite state automaton (see Fig. 4), is modelled by the DNSServer class which is able to process up to n requests in parallel. If the DNS server is in the Available state, it handles requests as soon as they arrive; in the case contrary, when there are no more available processing resources, the server switches to the Busy state and stores the incoming requests into a limited buffer. If the buffer gets filled, requests are dropped. (Furfaro et al. 2014).

We had simulated a network (see Fig 5), that onsists of three parts as in (Kumar and Selvakumar 2009). The first part contains ten ASs, each made up of 50 hosts, where the traffic sources are located in. The 50% of such ASs is corrupted and belongs to the botnet. The second part is the intermediate network and the third part contains only the victim's AS.

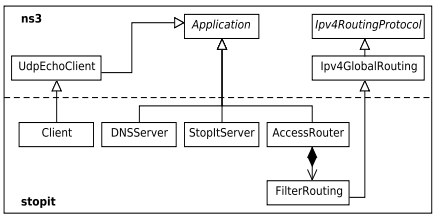

Figure 3: StopIt class hierarchy.

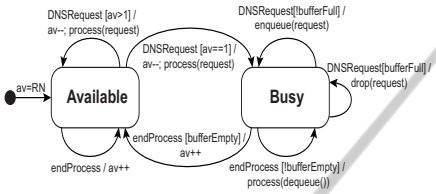

Figure 4: Finite State Automaton.

We included 24 VoIP sources (using the ilbc_mode_30 codec at 13.33kbps), 230 HTTP sources and 230 DNS sources. DiffServ handles both DNS and HTTP sources as Best Effort traffic and VoIP sources as Assured Forwarding. In the other case, DiffServ to face an indirect DDoS attack, DNS traffic is handled as coming from high priority sources. We measured its bandwidth occupation in the simulated attacks. (Furfaro et al. 2014).

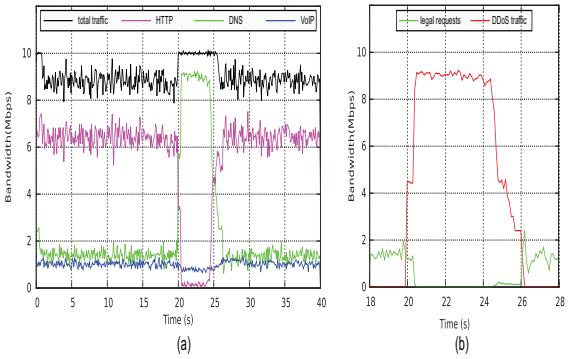

Figure 6: Direct DNS DDoS Attack.

As show in Fig 6, the black curve is the total used bandwidth, the purple line represents the HTTP traffic, the blue line is the VoIP traffic and the green one the DNS traffic. In the simulated scenario, the attack begins at t = 20 s and it is detected after 3s.

During the time interval between the begin of the attack and the StopIt response, the DNS traffic increases and saturates the available bandwidth at expense of the HTTP packets, as show in Figure 7.

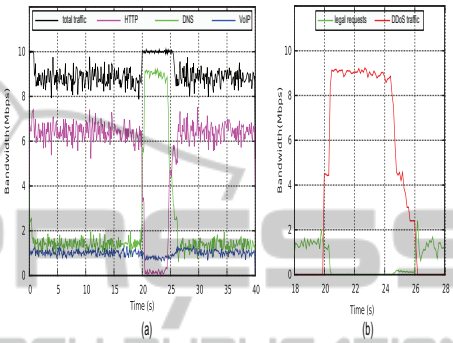

Figure 7: Detail of legal and malicious DNS Traffic.

Figure 8 depicts a scenario where the attack is achieved indirectly by flooding a host that belongs to the same AS of the victim with the aim of exhaust the available bandwidth of a shared link.

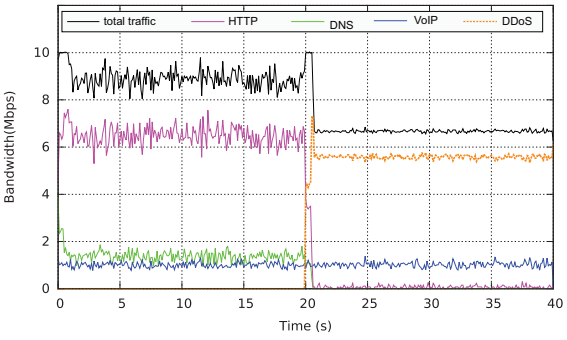

Figure 8: Indirect DDoS Attack (StopIt).

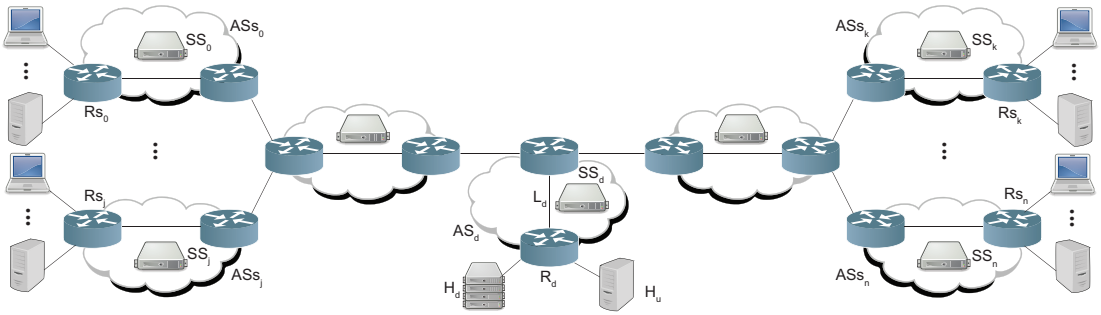

Figure 5: Simulated Network Topology.

Figure 9 shows how the proposed defense strategy, by exploiting the cooperation of StopIt and DiffServ, re-insures the necessary bandwidth to the DNS server after the time needed to detect the anomalous behavior and to dispatch the StopIt requests.

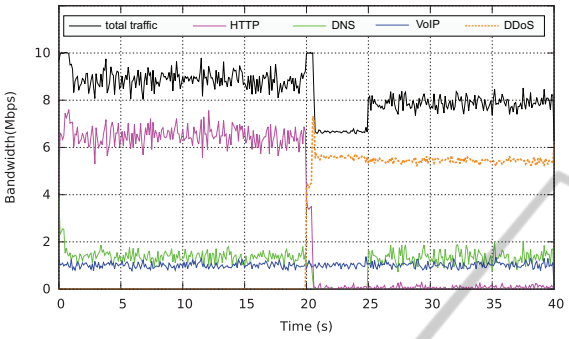

Figure 9: Indirect DDoS Attack (Stopit + Diffserv).

6 EXPECTED OUTCOME

As a result of the research we aim to define the appropriate simulation models for the prototyping and validation of software tools for the prevention, detection, defense and response to attacks on the security of computer systems. In particular, we will experiment with the definition of software models for computer security specified mediating formal languages, derived from finite state automata at a level of abstraction that allows formal verification, for example by means of model-checking techniques, properties expected from such systems.
An attempt will also use the same models in the context of existing tools for simulation of network systems (such as ns-3, NeSSi2) in order to validate and predict the behavior in more realistic operational scenarios.

As future work we plan to extend our research by designing suitable detection algorithms that may directly run on edge network devices and exploit StopIt features to block illegal sources also in the case of indirect attacks. (Furfaro et al. 2014).

REFERENCES

Carneiro, G., H. Fontes, M. Ricardo. 2011. Fast prototyping of network protocols through ns-3 simulation model reuse. *Simulation Modelling Practice and Theory* 19 (9): 2063 – 2075.

Duarte, José. 2012. Identificación de Ataques Informáticos a través de Redes Bayesianas. Editorial académica española. ISBN:978-3-659-00652-4

Furfaro, A., Pace, P., Parise, A., Molina, L. 2014, July. Modelling and Simulation of a defense strategy to face indirect DDoS flooding attacks. *7th International Conference on Internet and Distributed Computing Systems.*

Grunewald, D., Lützenberger, M., Chinnow, J., Bye, R., Bsufka, K., Albayrak, S.2011. Agent-based Network Security Simulation (Demonstration). DAI-Labor | TU Berlin | Ernst-Reuter-Platz 7 | 10587 Berlin, Germany.

Hirsch B., Konnerth, T., Heßler A. 2009. Merging agents and services — the JIAC agent platform. *In Multi-Agent Programming: Languages, Tools and Applications, pages 159–185. Springer.*

Kumar, P., S. Selvakumar. 2009, March. Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback *Mechanisms. In Advance Computing Conference*, 2009. IACC 2009. IEEE International, 1275–1280.

Liu, Xin., Yang, Xiaowei, Lu Yanbin. 2008. To Filter or to Authorize: Network-Layer DoS Defense against Multimillion-node Botnets. *ACM SIGCOMM'08, Seattle, Washington, USA.*

Ns-3 Manual. 2014. Release ns-3.20. http://www.nsnam.org/docs/release/3.20/manual/ns-3-manual.pdf.

Neinbe, J. 2010. Log Analyzer for Network Forensics and Incident Reporting. *International Conference on Intelligent System, Modeling and Simulation.* IEEE Computer Society 978-0-7695-3973-7/10, p356-361.

Patrikakis, C., Masikos, M., Zouraraki O. 2004. Distributed Denial of Service Attacks. *The Internal Protocol Journal.* Volume 7, Number 4, p13-35..

Peng, T., C. Leckie, K. Ramamohanarao. 2007, April. Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems. *ACM Comput*. Surv. 39 (1).

Ramroop S. 2011. A DiffServ model for the NS-3 simulator. http://www.eng.uwi.tt/depts/elec/staff/rvadams/sramroop/index.htm.

Schmidt, Stephan., Bye, Rainer., Chinnow, Joël. 2008. Application-level simulation for network security. *DAI-Labor, Berlin Institute of Technology*.

Yu, S., Zhou W. 2010. Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks. *Sixth Annual IEEE International Conference on Pervasive Computing and Communications.*

Zargar, S. T., J. Joshi, D. Tipper. 2013. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials 15 (4): 2046–2069.*