INVESTIGATION OF COOPERATIVE DEFENSE AGAINST DDOS

Igor Kotenko and Alexander Ulanov
St. Petersburg Institute for Informatics and Automation, 39, 14 Liniya, St.-Petersburg, 199178, Russia

Keywords: Denial of Service and other attacks, DDoS Defense, Simulation of Internet Attacks and Defense.

Abstract: The paper considers a new approach and a simulation environment which have been developed for comprehensive investigation of Internet Distributed Denial of Service attacks and defense. The main peculiarities of the approach and environment are as follows: agent-oriented framework to attack and defense investigation, packet-based simulation, and capability to add new attacks and defense methods and analyze them. The main components of the simulation environment are specified. Using the approach suggested and the environment implemented we evaluate and compare several cooperative defense mechanisms against DDoS (DefCOM, COSSACK, and our own mechanism based on full cooperation). The testing methodology for defense investigation is described, and the results of experiments are presented.

1 INTRODUCTION

One of the most dangerous classes of the Internet attacks is Distributed Denial of Service (DDoS). The prospective DDoS defense system is supposed to work due to the cooperation of various network and global defense mechanisms functioning both in local networks and in the whole Internet.

The distributed cooperative DDoS defense mechanisms are the ones that implement the defense due to resource roaming (e.g. Server Roaming (Sangpachatanaruk, etc., 2004)), change of resources quantity, resource differentiation (e.g. Market-based Service Quality Differentiation (Mankins, etc., 2001), Transport-aware IP router architecture (Wang, etc., 2003)), authentication (e.g. Secure Overlay Services (Keromytis, etc., 2002)) and also the mechanisms that implement traceback (e.g. Gateway-based mechanism [Xuan, etc., 2001]) with packet marking or signature storing, including pushback, auxiliary packet generation, etc.

There are various defense methods with resource differentiation that use rate-limiting. They are in dedication of different traffic volumes for different protocols and lowering the load of defense system or target system (to allow them implement the countermeasures effectively). Applying the rate-limiting can be also the result of attack traceback mechanisms. Agents-limiters are distributed in the defended or ISP subnet and implement rate-limiting according to the given protocols. Such methods are mostly represented in cooperative defense mechanisms.

Our goal is to develop the simulation environment which can help investigate the Internet attacks and defense mechanisms and elaborate well-grounded recommendations on the choice of efficient defense mechanisms. In the paper we investigate the aspects of component cooperation for COSSACK (Papadopoulos, etc., 2003), DefCOM (Mirkovic, etc., 2005) and our own full cooperation approach as well as trying to develop *a new approach to the investigation of cooperative defense mechanisms based on agent-oriented packet-based simulation.*

The work is organized as follows. *Section 2* outlines suggested approach for simulation. *Section 3* defines the DDoS defense mechanisms investigated. *Section 4* describes the simulation environment developed. *Section 5* presents the testing methodology for defense mechanisms investigation. *Section 6* analyzes the results of experiments fulfilled. *Conclusion* surveys main work results and future research.

2 SIMULATION APPROACH

It is suggested to represent the investigated processes as an interaction of various teams of

Kotenko I. and Ulanov A. (2007).
INVESTIGATION OF COOPERATIVE DEFENSE AGAINST DDOS.
In *Proceedings of the Second International Conference on Security and Cryptography*, pages 180-183
DOI: 10.5220/0002128801800183

software agents in the dynamical environment defined on the basis of the Internet model (Kotenko, Ulanov, 2006). Aggregated system behavior is shown in local interactions of particular agents.

There are at least three different classes of agent teams: teams of agents-malefactors, teams of defense agents, teams of agents-users. Agents of different teams can be in indifference ratio, cooperate or compete up till explicit counteraction.

Agents of attack teams are divided, at least, into two classes: "daemons" that realize the attack and "master" that coordinates other system components. The class of attack is defined by the following parameters: a packet sending intensity and an IP-address spoofing technique (no spoofing, constant, random, random with real IP addresses).

According to the *general DDoS defense approach* suggested the defense agents are classified into the following classes: information processing ("sampler"); attack detection ("detector"); filtering ("filter"); investigation ("investigator"). Samplers collect and process network data for anomaly and misuse detection. Detector coordinates the team and correlates data from samplers. Filters are responsible for traffic filtering using the rules provided by detector. Investigator tries to defeat attack agents. Defense team jointly implements certain investigated defense mechanism.

Defense teams can *interact using various schemes*. Moreover, a new class of defense agent – "limiter" – is introduced. It is intended for the implementation of cooperative DDoS defense. Its local goal is to limit the traffic according to the team goal. It lowers the traffic to the attack target and allows other agents to counteract the attack more effective.

There are *three types of limiting*: *by the IP-address of attack target; by the IP-addresses of attack sources; according to the packet marking.* Detector sets limiting mode using detection data.

3 DEFENSE MODELS

The main attention in cooperative mechanisms is given to the *methods of distributed filtering and rate-limiting*. These methods help to trace the attack sources and drop the malicious traffic as far from attack target as possible.

DefCOM (Mirkovic, etc., 2005) works in the following way. When "Alert generator" detects the attack it sends the attack messages to the other agents. "Rate limiter" agents will start to limit the traffic destined to the attack target. "Classifier" agents will start to classify and drop the attack packets and to mark legitimate packets.

DefCOM is simulated as follows. "Alert generator" agent is based on "detector", "Rate limiter" – on "limiter" agent, agent "Classifier" – on "filter".

COSSACK (Papadopoulos, etc., 2003) consists two main agent classes: "snort" and "watchdog". "Snort" (IDS) prepares the statistics on the transmitted packets for different traffic flows; the flows are grouped by the address prefix. If one of the flows exceeds the given threshold then its signature is transmitted to "watchdog". "Watchdog" receives traffic data from "snort" and applies the filtering rules on the routers. Agent "snort" is based on the agent "sampler", "watchdog" – on the agent "detector". It makes the decision about attack due to data from "snort". Agent "filter" is used to simulate filtering on routers.

COSSACK cooperation is in the following: when "watchdog" detects the attack it composes the attack signature and sends it to the other known "watchdogs". "Watchdogs" try to trace in their subnets the attack agents that send attack packets; when they detect them the countermeasures are applied.

Proposed approach. There are used the following four classes of defense team agents: "samplers", "detectors"; "filters"; "investigators". Agent teams are able to interact using *various cooperation schemes*: no cooperation; filter-level cooperation; sampler-level cooperation; poor cooperation; full cooperation. *The main aspect of full cooperation is that team which network is under attack can receive traffic data from the samplers of other teams and apply the filtering rules on filters of other teams*.

Figure 1 shows the full cooperation defense system configuration proposed by the authors.

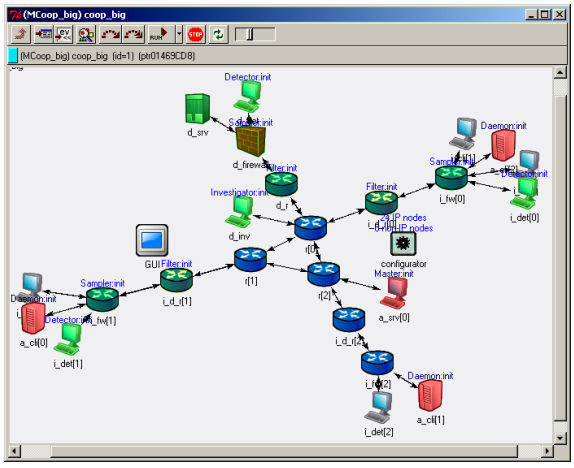

Figure 1: Proposed defense system configuration.

4 SIMULATION ENVIRONMENT

The simulation environment architecture consists of the following components (Kotenko, Ulanov, 2006): Simulation Framework, Internet Simulation Framework, Multi-agent Simulation Framework, Subject Domain Library.

Simulation framework is a discrete event simulator. Other components are expansions or models for Simulation Framework. *Internet Simulation Framework* is a modular simulation suite with the realistic simulation of Internet nodes and protocols. *Multi-agent Simulation Framework* allows realizing agent-based simulation. *Subject Domain Library* is a library used for imitation of processes from subject domain and containing modules that extend functionality of IP-host: filtering table and packet analyzer.

This architecture was implemented for multi-agent simulation of DDoS attack and defense mechanisms with the use of OMNeT++ INET Framework and software models developed in C++. Agent models implemented in Multi-agent Simulation Framework are represented with generic agent, attack and defense agents. Subject Domain Library contains various models of hosts, e.g. attacking host, firewall, etc., and also the application models (attack and defense mechanisms, packet analyzer, filtering table).

5 EXPERIMENTS

The developed simulation environment is used to investigate cooperative defense mechanisms. We are investigating the methods effectiveness, their functioning in various cooperative schemes and in different networks with different attacks.

The following *cooperation schemes* are investigated: *DefCOM*; *COSSACK*; *full cooperation*.

The following main admission for the simulation was made. Each cooperative defense mechanism (COSSACK, DefCOM or our approach) is based on its own attack detection method. We proposed to use for investigation of cooperative defense the same methods, e.g. Hop counts Filtering (HCF), Source IP address monitoring (SIPM), Bit Per Second (BPS), etc. The use of the same detection methods allows investigating various cooperative mechanisms in equal conditions.

The investigation is supposed to be done on the basis of analysis of the following main parameters: the amount of incoming traffic before and after filter of team which network is the attack victim; false positive and false negative rates of the defense team which network is under attack.

6 RESULTS OF EXPERIMENTS

Figures 2-4 show the traffic inside (line of squares) and before (other lines – of dots, rhombs and crosses) the attacked subnet for the DefCOM, COSSAK and full cooperation schemas accordingly. The Figure 2 consists of four graphs since the traffic was measured at the entrance to the subnet.

Attack starts at 300 seconds. The random real IP spoofing technique is applied as the most complicated for detection (the addresses for spoofing are taken from the same network). SIPM is used as the defense method. The router is placed there, it has four interfaces. The significant traffic increase is noticed in the beginning of attack (Figures 2-4). But in the area of 350 seconds the defense system detects the attack and traffic is being limited before the defended subnet ad being filtered in the source subnets (Figures 2-4).

DefCOM's rate limiter proceeds to limit the traffic because of the high attack traffic volume (Figure 2). But this cooperation schema succeeds to keep the traffic on the acceptable level due to limiting and to applying filtering rules. In COSSACK the filtering rules are applied and the attack signature is sent to the other defense components. In full cooperation the attack signatures are sent to other cooperating teams which apply the filtering rules in their subnets. The traffic on the entrance to the defended subnet is decreased due to their actions.

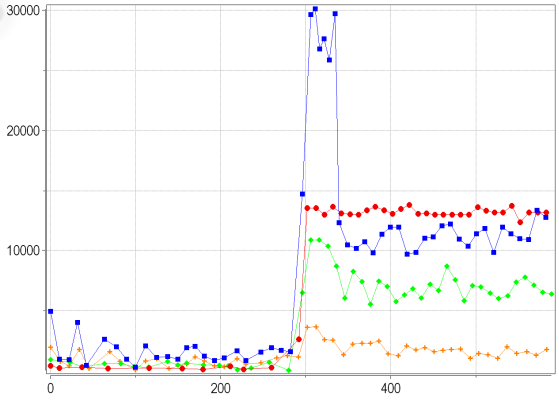

Figure 2: Traffic inside and before the attacked subnet for the DefCOM schema.

Experiments showed the effectiveness of various cooperative DDoS defense. The best cooperative schema is the *full cooperation*. Sampler cooperation played the key role in the defense. *DefCOM schema* shows the stable containment of attack traffic due to a limiter on the entrance to the defense subnet and

classifiers in the source subnets. *COSSACK schema* has the similar traffic level in the defense subnet, but outside it the traffic stays enough high.

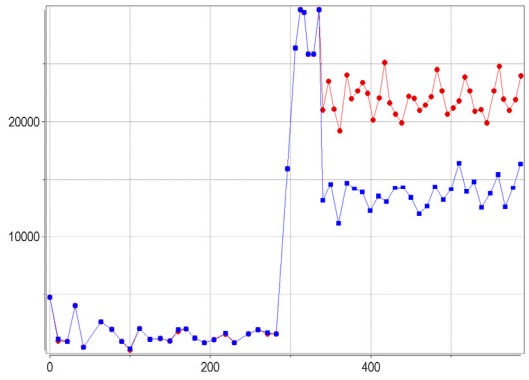

Figure 3: Traffic inside and before the attacked subnet for the COSSACK schema.

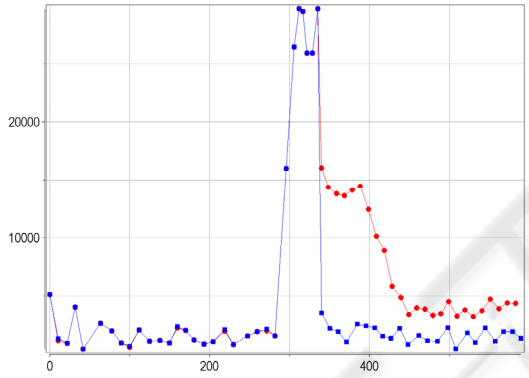

Figure 4: Traffic inside and before the attacked subnet for the full cooperation.

7 CONCLUSION

The main results of the paper consist in implementing the simulation environment developed by the authors for packet-level agent based simulation of various cooperative defense schemas against DDoS (DefCOM, COSSACK, and our own based on full cooperation). The goal of the paper was to evaluate the effectiveness of these schemas and compare them.

The multitude of experiments we implemented demonstrated that full cooperation shows the best results on blocking the attack traffic. It uses several defense teams with cooperation on the level of filters and samplers. DefCOM advantage is in using a rate limiter before the defended network. It allows lowering the traffic during attack and letting the defended system work properly. COSSACK is one of the examples of peer-to-peer defense network. It uses attack signatures transmission between agents to apply the filtering rules near the source.

Future work is concerned with improving the functionality of the simulation environment and investigating new cooperative defense mechanisms.

ACKNOWLEDGEMENTS

This research is being supported by grant of Russian Foundation of Basic Research (Project No. 07-01-00547), program of fundamental research of the Department for Informational Technologies and Computation Systems of the Russian Academy of Sciences (contract No 3.2/03), Russian Science Support Foundation and partly funded by the EU as part of the POSITIF project (contract No. IST-2002-002314) and RE-TRUST (contract No. 021186-2).

REFERENCES

Keromytis, A., Misra, V., Rubenstein, D., 2002. SOS: Secure Overlay Services. In *Proceedings of ACM SIGCOMM'02*, Pittsburgh, PA.

Kotenko, I., Ulanov A., 2006. Simulation of Internet DDoS Attacks and Defense. In *Proc. of ISC 2006. Samos, Greece. LNCS*, Vol. 4176.

Mankins, D., Krishnan, R., Boyd, C., Zao, J., Frentz, M., 2001. Mitigating Distributed Denial of Service Attacks with Dynamic Resource Pricing. In *Proceedings of the 17th Annual Computer Security Applications Conference. ACSAC'01*.

Mirkovic, J., Robinson, M., Reiher, P., Oikonomou, G., 2005. Distributed Defense Against DDOS Attacks. In *University of Delaware CIS Department Technical Report CIS-TR-2005-02*.

Papadopoulos, C., Lindell, R., Mehringer, I., Hussain, A., Govindan, R. 2003. Cossack: Coordinated suppression of simultaneous attacks. In *Proceedings of DISCEX III*.

Sangpachatanaruk, C., Khattab, S.M., Znati, T., Melhem, R., Mosse, D., 2004. Design and Analysis of a Replicated Elusive Server Scheme for Mitigating Denial of Service Attacks. In *Journal of Systems and Software*, Vol.73(1).

Wang, H., Shin, K.G., 2003. Transport-aware IP Routers: A Built-in Protection Mechanism to Counter DDoS Attacks. In *IEEE Transactions on Parallel and Distributed Systems*, Vol.14(9).

Xuan, D., Bettati, R., Zhao, W., 2001. A Gateway-Based Defense System for Distributed DoS Attacks in High Speed Networks. In *Proceedings of the 2nd IEEE SMC Information Assurance Workshop*, West Point, NY.