DiCoDefense: Distributed Collaborative Defense against DDoS Flooding attacks

Saman Taghavi Zargar
Telecommunications and networking program
School of Information Sciences, University of Pittsburgh
Pittsburgh, PA, USA
stzargar@sis.pitt.edu

James Joshi
School of Information Sciences, University of Pittsburgh
Pittsburgh, PA, USA
jjoshi@sis.pitt.edu

***Abstract*—Detecting Distributed Denial of Service (DDoS) flooding attacks as soon as possible before they affect the victims, identifying the sources of the attacks, and finally stopping them by blocking or rate limiting the attack traffic is the ultimate goal of current defense mechanisms. The success in detecting and responding to DDoS flooding attacks is highly dependent on the data monitored by the employed traffic monitoring mechanisms, the degree of collaboration among various domains, and the response approach employed in various domains. In this poster, we present *DiCoDefense*, which is a distributed collaborative defense mechanism whose main goal is to detect and respond to high volume DDoS flooding attacks closer to the sources of the attacks.**

I. Introduction

According to CERT [1], the rapid growth of the Internet services has increased the number of possible attacks against these services. DDoS flooding attacks have been reported as one of the attacks with the highest occurrence rates over the past two decades and many Internet service providers and users have seriously suffered from these attacks. DDoS flooding attacks often originate from a group of organized and widely scattered zombies that simultaneously and continuously either (i) disrupt a legitimate user’s connectivity by exhausting bandwidth, router processing capacity or network resources; or (ii) disrupt a legitimate user’s services by exhausting the server resources (e.g., sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth) [2].

Traditional host-based (i.e., source-based or destination-based) and network-based defense mechanisms against DDoS flooding attacks, that were mostly centralized, have been found to be inadequate in detecting these attacks as soon as possible and before they reach their victims, identifying the attack sources, and finally stopping the attacks as close as possible to the attack sources [2]. In the host-based defense mechanisms, the key issues are either the lack of enough information at the sources to detect an attack in a timely fashion or inability of destinations to accurately detect and respond to the attacks before they reach the victims and wastes resources on the paths to the victims. Network-based defense mechanisms usually incur high storage and processing overhead at the routers; these overheads increase if each router performs redundant monitoring of the same traffic flows [3].

Therefore, in order to defend against sophisticated, coordinated DDoS flooding attacks, defense mechanisms should also form alliances and collaborate with each other. Hence, the best alternative to traditional systems would be hybrid defense mechanisms in which defense mechanisms can be deployed at multiple locations including sources, destinations or intermediate networks. Furthermore, a distributed defense mechanism can continue to function even if some of its components fail or are compromised, thus, providing better resiliency [2]. Hence, in this poster we present, *DiCoDefense*, a comprehensive distributed and collaborative defense mechanism to achieve aforementioned goals.

II. Overview

Figure 1 presents the *DiCoDefense* system architecture. *DiCoDefense* comprises of four critical components that are briefly explained here:

1- *Central server/Task Assignment Server (TAS)*: There is a central server in each autonomous system (AS) which is responsible for various tasks for the following components.

2- *DiCoTraM:* A distributed and collaborative traffic monitoring component which aims to monitor traffic flows in such a way that the monitored data on each router within each AS can be used for detection and response to high volume DDoS flooding attacks closer to the sources of the attacks. *TASs* within each AS are responsible for distributing the monitoring responsibilities among all the routers within each AS in order to coordinate the monitoring responsibilities among the routers. DiCoTraM also reduces the redundant monitoring overheads and the communication overheads. Such overheads are key concerns in systems that centrally collect the monitored data used to support the detection and response tasks. Figure 2. illustrates our proposed DiCoTraM architecture.

3- *DiCoDet*: A detection approach that distributes detection tasks to individual routers within each AS; by collaborating with its neighbors, these routers detect attacks. In doing so, routers within an AS generate and report alerts to their *TASs* upon detecting suspicious DDoS flooding activity. *TASs,* then, communicate with their immediate neighbors through a secure channel and confirm the suspicious DDoS activity hop-by-hop with the target AS. Servers within other ASs, depending on the level of trust they have with their neighbors, can perform preventive actions based on their defined response policy against reported flows (e.g., rate limit or block) upon getting notified. As part of our detection mechanism, our goal is to detect application-level DDoS flooding attacks [2] at the intermediate network level which was not possible before by employing Software Defined Networking (SDN) techniques. Leveraging SDN at the intermediate network enables layer 4 to layer 7 visibility which is mandatory in order to analyze the application-level traffic for application-level DDoS detection.

4- *DiCoRes:* A DDoS flooding response approach which is also distributed at individual routers within each AS and responds to the attacks based on ASs' response policy.

We have implemented both DiCoTraM and DiCoDet and are currently focusing on finalizing our experiments and presenting the results to the research community. We are still working on the details of the collaboration mechanism suitable for the *DiCoDefense* mechanism. Also, a trust calculation and negotiation mechanism between TASs to communicate alerts and efficient response policy for various situations is part of our current directions towards the complete implementation of our proposed *DiCiDefense* mechanism.

ACKNOWLEDGMENT

This research has been supported by Cisco systems' research award and the NSF award CCF-0720737.

REFERENCES

[1] CERT 2008 http://www.cert.org/stats/

[2] S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1-24. (available in Early Access- online Mar. 28, 2013). DOI 10.1109/SURV.2013.031413.00127

[3] S. T. Zargar and J. B. D. Joshi. A Collaborative Approach to Facilitate Intrusion Detection and Response against DDoS Attacks. In Proc. of the 6th Int'l Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom 2010).

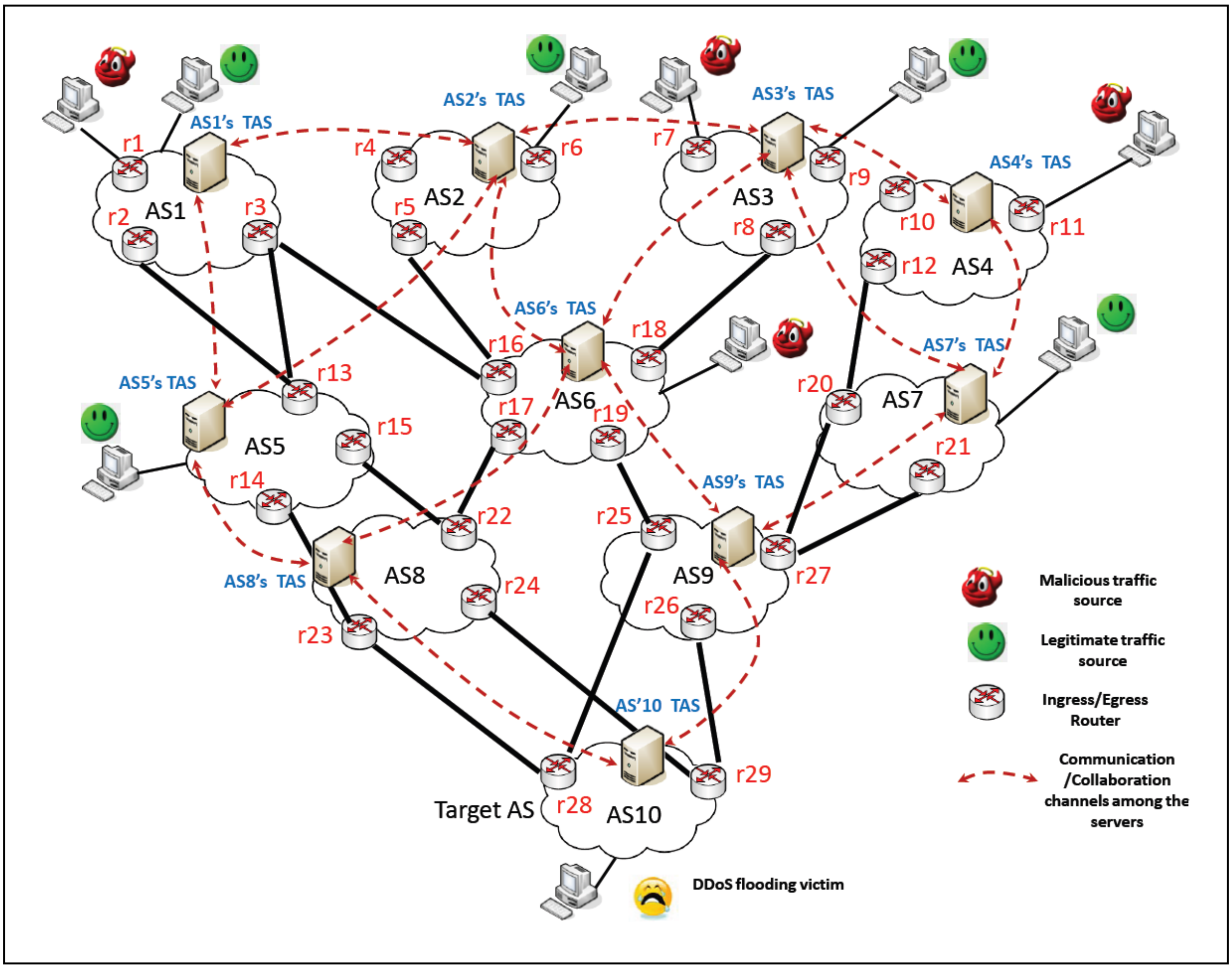

Fig. 1. DiCoDefense architecture.

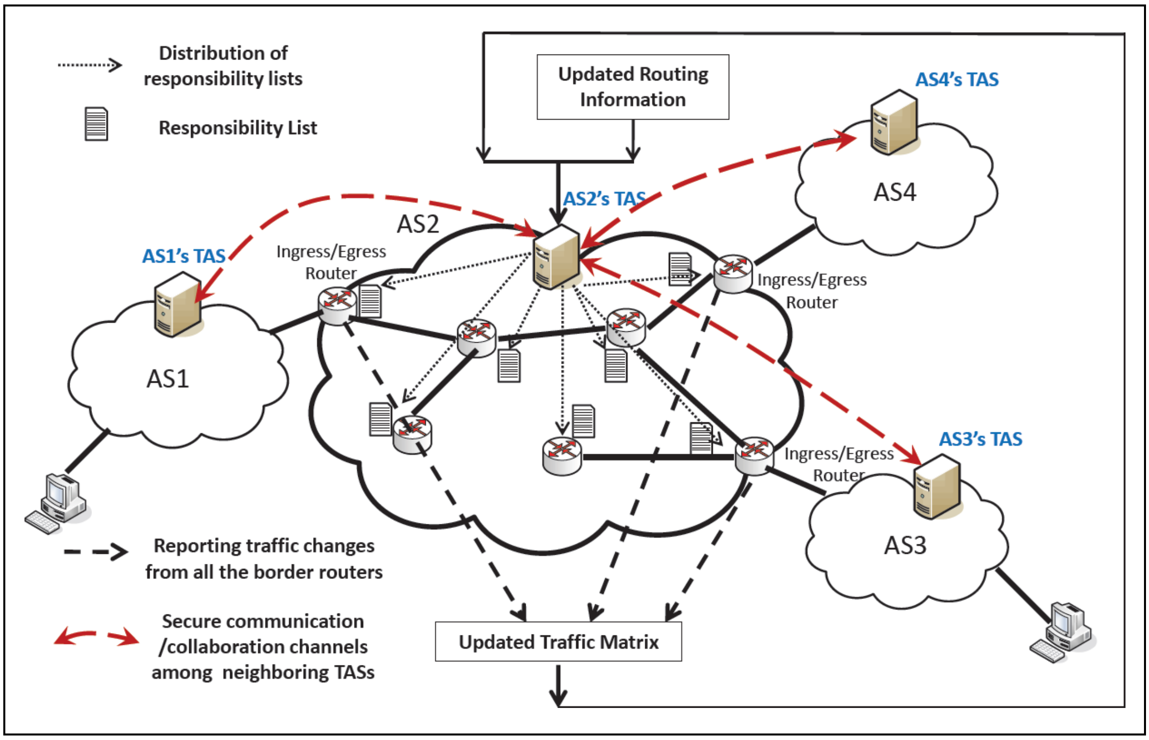
Distribution of responsibility lists
Responsibility List
Updated Routing Information
AS4's TAS
AS4
AS2's TAS
AS2
AS1's TAS
Ingress/Egress Router
AS1
Ingress/Egress Router
Ingress/Egress Router
AS3's TAS
AS3
Reporting traffic changes from all the border routers
Secure communication /collaboration channels among neighboring TASs
Updated Traffic Matrix

Fig. 2. DiCoTraM architecture.