Future Generation Computer Systems 29 (2013) 429–441

Contents lists available at SciVerse ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Thwarting DDoS attacks in grid using information divergence

P. Varalakshmi [a,*], S. Thamarai Selvi [b]

[a] Department of Information Technology, Madras Institute of Technology, Anna University Chromepet, Chennai-600 044 Tamil Nadu, India

[b] Madras Institute of Technology, Anna University Chennai, Chromepet, Chennai, 600 044 Tamil Nadu, India

ARTICLE INFO

Article history:
Received 17 September 2010
Received in revised form
24 September 2011
Accepted 24 October 2011
Available online 18 November 2011

Keywords:
Distributed Denial-of-Service
Trustworthy grid
Five-fold filter
Information divergence
Kullback–Leibler divergence
Trust value

ABSTRACT

The Grid is an emerging resource intensive environment that aims at utilizing resources efficiently and effectively. Distributed Denial-of-Service (DDoS) attacks on the Grid can have a devastating effect since there are several resource constraints in a Grid environment. A DDoS can cause large-scale damage to resources and availability of the resources to genuine Grid users. This paper proposes a five-fold DDoS Defense Mechanism using an Information Divergence scheme that detects the attacker and discards the adversary's packets for a fixed amount of time in an organized manner. The trust value is adjusted based on the attack intensity to ensure a trustworthy system. The mitigation is carried out by limiting the bandwidth of the attacking IP instead of completely blocking the attackers IPs. With this, the job success rate is more by the proposed approach compared to completely blocking the attackers IP approach.

1. Introduction

A DDoS attack can be characterized as a large-scale, coordinated attack that is launched indirectly through multiple compromised hosts (called zombies) on victim network resources, with the purpose of preventing legitimate users from using those resources. DDoS attacks consume resources rendering them unavailable to legitimate users thus mitigating the usefulness of the grid. A DDoS Defense Mechanism must be able to distinguish attack packets from legitimate ones with high accuracy, minimal resource consumption and low false positive and negative rates. Our work is specifically focused on detection and mitigation of DDoS attacks in the Grid which is purely on the Service Oriented Architecture (SOA) system. A DDoS in a Grid will be highly devastating since it is highly resource oriented. The increasing prevalence of SOA in the form of web services and grid services make these vulnerable as a prime target for attackers. DDoS attacks pose an immense threat to the Grid, and many defense mechanisms have been proposed to combat the problem. Attackers constantly modify their tools to bypass these security systems, and researchers in turn modify their approaches to handle new attacks. Our work aims at extending the Hierarchical Broker Architecture proposed by Varalakshmi et al. [1] and also providing a DDoS Defense to the Grid environment.

1.1. Progression of broker architecture

In a grid environment, a consumer makes a request for the resource it needs and a Resource Provider (RP) provides it. In order to make resource discovery easier as well as to monitor transactions, a new entity called a Resource Broker (RB) is introduced in the architecture. Accounting to single point failure, the presence of multiple brokers provides redundancy in the architecture and ensures the availability of resources even if one broker crashes. RP and consumers are registered with more than one Resource Broker.

Consumers present their request to a broker which calls for a suitable RP based on the resource request as well as policy requirements. The broker also forwards the request to other brokers in the same domain as well as other domains who in turn pick the most suitable RP registered under them. The broker may then choose the best RP from the nominated set of most suitable RP (chosen by it as well as other brokers) based on various parameters such as trust, satisfaction of policy requirement, resource queue length, QoS etc. However, as a broker gains monetary benefit from each individual transaction, it tends to favor an RP directly registered under it. This leads to a problem called as biased brokers. In order to overcome this problem, the Hierarchical Broker Architecture is adopted here for the grid environment.

* Corresponding author. Fax: +91 044 22232403.
E-mail addresses: varanip@gmail.com, sakthijayasundar@rediffmail.com (P. Varalakshmi), stselvi@annauniv.edu (S.T. Selvi).

0167-739X/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2011.10.012

In the Hierarchical Broker Architecture, neutral entities called Regional Resource Administrators (RRA) are responsible for publishing and discovery of resources. Brokers register themselves under more than one of the interested RRA and RPs register under more than one any of the interested brokers. Consumers present their request and policy-constraints to an RRA which picks the most suitable RP for the transaction through the brokers. The objective of forming RRA is to provide mechanisms to objectively manage the operations in a dynamic, competitive open grid environment, prone to disruptive and malicious behavior. The RRA does not derive any compensation from any of the entities (consumers as well as associated brokers) for the transactions undergone. It obtains compensation only from the registration, renewal and audit charges of the associated brokers. Such an arrangement of entities in the Hierarchical Broker Architecture releases the RRA from being considered biased in the choice of a suitable RP for the consumers' request. Since RRA are not benefited monetarily from individual transactions, they can maintain neutrality and choose a trustworthy RP for consumers' requests. RRAs are assumed here to be trustworthy entities like DNS. The trust-index of the RBs are also maintained at the associated RRAs to reflect the trustworthiness of the RBs discussed in [1].

1.2. Motivation of work

A brief introduction of the functioning of the Hierarchical Broker Architecture proposed by Varalakshmi et al. [1] has been described above. The general functioning of this architecture has been found to be vulnerable to DDoS attacks by malicious nodes within the grid which may cause much damage through traffic flooding. A good grid network design should minimize bandwidth usage to ensure good scalability. Therefore, a grid network is unlikely, under normal circumstances, to produce a sufficient amount of network traffic to flood a network and hence it is highly impossible for some untrustworthy node from the Internet outside the grid to cause a DDoS attack. An attacking computer may pose as an actively participating node on a grid. Through message requests in the grid application, a malevolent machine may use a grid network as a massive traffic generator. The effect may be similar to that of a broadcast of an ICMP Echo Request message. Additionally, due to the application level nature of grid computing, a request may involve multiple responses to the originally broadcast message.

A possible catastrophe may be avoided by implementing security measures in the grid network. Secure node intercommunication allows only trusted systems to communicate with the node and Source authentication must be provided to ensure the identity of a node can reduce the probability of possible attacks. While these measures cannot prevent a malicious user from taking control of a privileged system, and make the attacker capable of launching a large-scale DDoS attack to bring down the Grid. We propose an intuitive five-fold filter mechanism as a DDoS Defense for the Hierarchical Broker Architecture to secure it from DDoS attacks. The concept of information divergence is used to identify the divergence between the learned and the current profiles of traffic. Kullback–Leibler divergence which is one of the most efficient divergence techniques has been made use here. Though several techniques for DDoS Defense have been proposed, our proposed work aims at integrating a trust model to the DDoS Defense Mechanism and also the false negative and false positive rates have been highly reduced since we analyze the entire packet unlike previous works which consider only the header or the payload alone. Though there is a bearable processing overhead, a higher detection rate is possible by the proposed work.

2. Related work

The grid technologies that are currently available address authentication, authorization, resource access, resource discovery and other challenges discussed by Foster et al. [2]. However, there is a need for ensuring the availability of high performance grid resources by preventing DDoS attacks which hinder the overall performance of a system to a great extent. A multi-broker Grid architecture has been proposed by Qiming Li et al. [3] but it suffers from biasing from the resource broker. Hence a Three-tier Grid Architecture proposed by Varalakshmi et al. [1] has been made use of in this paper which comprises a third tier of Regional Resource Administrators (RRA). To render the RRA obsolete, attackers may commonly target an RRA with a DDoS attack by making a flood of registrations or resource requests.

DDoS attacks hog resources rendering them unavailable to legitimate users thus mitigating the usefulness of the grid. An article about the DDoS attack on commercial SUN grid in March 2006 [4] that brought down the entire grid to its knees within hours of its launch necessitating a login procedure change is discussed in byteandswitch.com. This focused the study of DDoS attack on the Grid. The various DDoS attacks and their Defense Mechanism available to tackle such attacks has been given a comprehended study by Jelena Mirkovic et al. [5]. The author introduces a scheme that discards packets based on the arrival of packets from a source. Rather than DDoS detection this helps in mitigating DDoS attack's effects.

In the past decade, a variety of studies and proposals on DDoS evading mechanisms have emerged in the literature. These schemes varied in their approaches and models. A lot of mathematical and statistical models have been proposed. Many of these approaches have been studied to detect and evade the offending network traffic. The general principle observed in all the proposed solutions is to detect the attack traffic without dropping the legitimate packets.

Wang et al. [6] utilizes a change point monitoring approach to detect DoS attacks. Their detection is effective and efficient in making a quick disruption of any abrupt change in traffic. Yu Chen et al. [7] also proposed a distributed change point based detection technique for DDoS attacks. The approach is to monitor the spatiotemporal pattern of the attack traffic. These approaches mainly involve modifying the system at the hardware level wherein scalability is a difficult factor in large systems.

Many modeling techniques with special emphasis on anomaly detection techniques were proposed by researchers. These included neural networks discussed by Ryan et al. [8]; clustering proposed by Toelle and Niggenmann [9]; and statistical Detection proposed by Yau et al. [10] and Chan et al. [11]. A statistical model based on multi resolution non-Gaussian modeling to detect DDoS attacks is proposed by Borgnat et al. [12].

In statistical modeling techniques, special coverage was given to the correlation between packets as an important feature in detection of DDoS attacks. Yu Chen et al. [13,7] propose a mechanism that deals with the changes in correlation to detect flooding attacks.

During IP spoofing packets with new randomly generated addresses may appear in the network. A novel scheme to detect a DDoS attack by monitoring the increase of new IP packets has been proposed by Jelena Mirkovic et al. [14]. A DDoS mechanism Packet Score (discussed by Yoohwan Kim et al. [15,16]), is a scheme that performs score based selective packet discarding based on a dynamic threshold. Conditional Legitimate Probability is used to compute the score of each packet. Varalakshmi et al. [1] studies the effectiveness of DDoS attacks on statistical-based filtering in a general context where attackers are smart. It considers various cases such as the static (or) dynamic property of the attacker and the filter.