Defense Against Distributed Denial of Service Attacks in Computer Networks

氏名（本籍地）	DALIA MOHAMED NASHAT（ダリア ユハメド ナシュアット）
学位の種類	博　士（情報科学）
学位記番号	情　博　第　４６５　号
学位授与年月日	平成２２年　３月２５日
学位授与の要件	学位規則第４条第１項該当
研究科、専攻	東北大学大学院情報科学研究科（博士課程）情報基礎科学専攻
学位論文題目	Defense Against Distributed Denial of Service Attacks in Computer Networks （コンピュータネットワークにおけるDDoS攻撃に対する防御法）
論文審査委員	（主査）東北大学教授　亀山　充隆 東北大学教授　白鳥　則郎　　東北大学教授　加藤　寧 東北大学准教授　姜　暁鴻

論文内容の要旨

Chapter 1

Availability requires that computer systems function normally without loss of resources to legitimate users. One of the most challenging issues to availability is Denial-of-Service (DoS). The DoS threat started to materialize in the Internet with the massive attack against the University of Minnesota in 1999. The access links of the university were flooded by packets launched from many machines, the links were completely hogged up by the attack packets, and legitimate (non-attack) packets were dropped. Since then, many DoS attacks have been and continue to be launched.

Distributed Denial of Service (DDoS) attacks add the many-to-one dimension to the DDoS problem, making the prevention and mitigation of such attacks more difficult and the impact proportionally severe. A DDoS attack uses many computers to launch a coordinated DoS-attack against one or more targets. The DDoS attack is the most advanced form of DoS attacks. It is distinguished from other attacks by its ability to deploy its weapons in a distributed way over the Internet and to aggregate these forces to create lethal traffic. In a typical DDoS attack, the malicious client (attacker) first compromises relay hosts (masters), which in turn compromise attack machines (agents). The attack begins when the attacker sends an attack command to the masters through a secure channel to launch an attack against the targeted victim.

Chapter 2

The IP spoofing plays an important role in network attacks, in particular the flooding DDoS attack, for a number of reasons. First, the IP spoofing makes it hard to distinguish attack packets with spoofed source addresses from legitimate ones. Second, the IP spoofing makes the detection

of the flooding source very difficult, since it completely hides the IP address of the flooding source. Finally, the common types of DDoS attack, such as the TCP SYN flooding attack and the Distributed Reflection Denial of Service attack (DRDoS), are not possible without the IP spoofing.

The available source-end filtering schemes are not general enough to cover different types of IP spoofing. Also, those schemes are not suitable for the high-speed networks, since they need to verify every packet in the traffic (please refer to section 6 for related work). Therefore, a new source-end filtering scheme is highly desirable for the efficient detection of the DDoS flooding agents under different types of IP spoofing. In this paper we propose such a scheme by assigning a key for each IP address in the stub network.

Chapter 3

Over 90% of DDoS attacks use TCP protocol and the TCP SYN flooding attack is the most common one among them. The TCP SYN flooding exploits the TCP's three-way handshake mechanism and its limitation in maintaining half-open connections. The attacker attacks a victim's server by ordering agents to send at the same time a stream of flooding SYN packets with spoofed IP addresses, such that server's backlog queue for half open connections is exhausted and any new legitimate SYN packets will be dropped.

The available source-end detection schemes are not general enough to cover different types of IP spoofing. Also, those schemes are less sensitive and not suitable for the detection of low rate flooding sources (please refer to section 5 for related work). Therefore, a new source-end detection scheme is highly desirable for the efficient detection of the DDoS flooding agents under different types of IP spoofing. In this chapter we propose such a scheme by exploring in more detail the behavior of TCP SYN-SYN/ACK pair.

Chapter 4

The DDoS attackers launch the attack at the network layer to consume the network bandwidth or at the application layer to attack the victim web servers. Since many effective defense mechanisms have been proposed to protect the network from bandwidth attack, recently the attackers target the application layer and establish a more sophisticated type of DDoS attack to disable the legitimate clients from using this application. There are two common methods to launch the DDoS flooding attack in web service. First, attackers can consume the victim web server by sending a query for large amount of data. Second, attackers can cause the entire application to fail by overloading the server with a huge number of requests. We focus on the second method because it is the most widely used method to launch the DDoS attack on web service.

Recently, an efficient approach (Live Baiting) was proposed for detecting the identities of DDoS attackers in web service based on the group testing theory. Although Live Baiting uses low state

overhead without requiring either the models of legitimate requests nor anomalous behavior, its detection algorithm has two limitations. First, the detection algorithm assumes that all clients of the web service are suspects during the detection interval even if some of them are inactive. Thus, it leads to a high false positive probability especially for large web service with a huge number of clients. Second, the detection algorithm uses a fixed threshold based on the expected number of requests in each bucket during the detection interval without the consideration of daily and weekly traffic variations. Therefore, the detection decision is inaccurate and sensitive to site and access pattern.

In order to address the above limitations, we first consider the clients activity (Active and Non-Active) clients during the detection interval) and then propose a new adaptive threshold based on the Change Point Detection, such that we can improve the false positive probability and avoid the dependence of detection on sites and access patterns.

Chapter 5

We give a final perspective on our work and outline some future work in this area.

論文審査結果の要旨

ネットワークセキュリティにおける最も主要な脅威の一つとして、DDoS (Distributed Denial of Service) 攻撃がある。今日のDDoS攻撃では、攻撃パケットが異なる方式で改ざんされ、低頻度で送信されるため、その防御や検出が非常に困難になっている。著者は、パケットヘッダと通信トラヒックの解析による異常検出に着目し、ネットワーク層並びにアプリケーション層で適用可能なDDoS攻撃に対する防御法と検出法を提案し、その有用性を実証した。本論文はその成果を取りまとめたもので、全文5章よりなる。

第1章は緒言である。

第2章では、ネットワーク層における DDoS 攻撃パケットの遮断手法を提案している。本手法では、サブネットワーク内の個々のIPアドレスにキーを割り当て、それをパケットヘッダ解析で用いることにより、送信元IPアドレスが任意の方式で改ざんされたとしても、その攻撃パケットを短時間で遮断することを可能としている。実際に観測されたDDoS攻撃トラヒックを用いたシミュレーションと理論的分析により、任意の方式で改ざんされた攻撃パケットに対して遮断可能なパケット率が従来法よりも高いことを示した。これは、攻撃パケットの送信元サブネットワークの出入り口において DDoS 攻撃を防御する上で非常に有用な成果である。

第3章では、ネットワーク層における DDoS 攻撃トラヒックの検出手法を提案している。本手法では、パケットヘッダ及び応答パケット数頻度に関する情報から、要求パケットに対する応答パケットと再送パケットを区別することにより、低頻度の攻撃トラヒックを検出することを可能としている。DDoS攻撃トラヒックを用いたシミュレーションにより、従来法よりも高い検出率を実現し、検出時間を大幅に短縮可能なことを示した。これは、ネットワーク上のパケット中継機器において低頻度のDDoS攻撃の高速検出を可能にする重要な成果である。

第4章では、アプリケーション層におけるWEBサービスに対するDDoS攻撃検出法と防御法を提案している。本手法では、グループ検査理論と変化点検出法を併用することにより、攻撃者のIPアドレスを特定し、攻撃パケットを遮断することを可能としている。DDoS攻撃トラヒックを用いたシミュレーションにより、従来法に比べて誤検出率が極めて低いことを示した。このことは、実用上有用な成果である。

第5章は、結言である。

以上要するに本論文は、深刻な問題となっている DDoS 攻撃に対して、パケットヘッダと通信トラヒックの解析に基づく防御法並びに検出法を開発し、その有用性を明らかにしたものであり、情報基礎科学の発展に寄与するところが少なくない。よって、本論文は博士(情報科学)の学位論文として合格と認める。