INVESTIGATION OF THE IMPACT OF DDOS ATTACK ON NETWORK EFFICIENCY OF THE UNIVERSITY OF ZAKHO

Sulaiman Mohamed Sulaiman [1] and Shavan Askar [2]
[1] Computer science Dept., Faculty of science, University of Zakho, Kurdistan region – Iraq.
[2] Electrical & Computer Eng. Dept. , University of Duhok. , Kurdistan region – Iraq.

(Accepted for publication: November 9, 2015)

Abstract:

In this paper an investigation was conducted to have an insight into the impact of the DDoS attack on the network efficiency of the University of Zakho, in particular, after deploying a fiber infrastructure and a datacenter with services such as web server, email server, and ftp server. Tests were conducted on one of the most popular DDoS attacks, that is, the flooding attack that has many types based on the start-of-the-art research in this field. For the evaluation purpose, two Internet services were chosen which are namely; file transfer service and E-learning video service. OPNET was used as a simulation tool to simulate Zakho University network and to conduct attacks because of its high reliability and reputation in this field. Results showed that DDoS attack has a big adverse impact on the legitimate users' accessibility for both services. Where the file traffic download reduced from 6000 Bytes/s in the case of no attack into only 500 Bytes/s in the case of attack which makes an approximate of 92% loss in the network traffic. In addition, video throughput is reduced from 180KB/s in the case of no attack into less than 20KB/s in the case of attack which makes around 89% loss that is considered a huge degradation in the network performance.

Keywords: *Campus Network; DDoS Attack; OPNET*

I- INTRODUCTION

Internet users are growing rapidly in recent years, and this rapid increase in the number of users is due to Internet penetration into our daily life via applications and services that the worldwide network offers. This huge number of users and the ease of accessing into the Internet is a double-edged sword because it is vulnerable to illegal access to the contents of Internet such as data processor systems or flooding traffic in the server or many types of attacks that will be described in the following sections.

Currently, Distributed Denial of Service (DDoS) attacks are common threat to websites, servers, and networks. In the recent fifteen years, DDoS attacks become more difficult to be mitigated (Amir et al.,2013).

This paper describes different types of DDoS attacks and evaluates the flooding type of DDoS attack using OPNET simulator which was chosen because of its high reliability to obtain accurate results. University of Zakho was considered as a victim of the DDoS attack.

II- RELATED WORK

In this section, an insight into the DDoS detection and prevention schemes is given to better clarify the importance of this paper when compared to the start-of-the-art of the DDoS research area.

A design that discusses the effect of DDoS attack is presented by Sajal Bhatia in 2013. Detection and synthesizing flash events were conducted. It mainly focused on the differences between DDoS attack and Flash (Bahtia and sajal,2013). In 2012, Sung-ho Kim proposed the entropy–based detection mechanism against DDoS attacks that ensures transmission of normal traffic. In addition, DDoS attacks were prevented by prohibiting abnormal traffic. OPNET was used as a simulation tool; it was concluded that entropy has superiority over other mechanisms in detecting DDoS attacks (Jun and Jae-Hyun 2011). In 2014, a method was proposed by Duraipandian to defend against DDoS attacks. Their paper discussed Hop-Count Filtering (HCF) technique; high throughput and low dropping were obtained from the proposed mechanism (Duraipandin and Palanisany, 2014) In 2014 Bingshuang Liu investigated Distributed reflective denial of service (DRDoS) which deals with UDP reflection and amplification. A new type of attack is introduced which has the capability to generate hundreds of gigabytes of unwanted traffic. Attacks are supposed to be able to store data on reflector nodes before the flooding phase starts in order to increase the amplification factor of an attack (Bingshuang et al,. 2014). In 2014, Different types of TCP SYN Flood DDoS Defense mechanisms were compared by Kolahi, Samad. Results showed that the

router based TCP Intercept support better defense while Anti DDoS Guardian presented worst defense results (Kolahi et al,. 2014). In 2014, A hybrid method to detect DDoS attack using Genetic Algorithm (GA) and Artificial Neural Network (ANN) were described by Barati. The above-mentioned neural algorithm techniques were deployed for feature selection and attack detection respectively. Results showed acceptable performance for detecting DDoS attack with high accuracy and deniable false Alarm (Barati et al,. 2014). In this paper, a simulation for the futuristic University of Zakho is conducted and DDoS tests were also made on this network to have an insight into effect of such attacks on the network performance.

III-DDoS ARCHITECTURE

Distributed Denial of Service lunched malicious traffic by a group of attackers to affect victim; according to this principle DDoS attack consists of some layers which are namely; the attacker, the master, zombies, and the victim. Each layer has a specific function and risk.

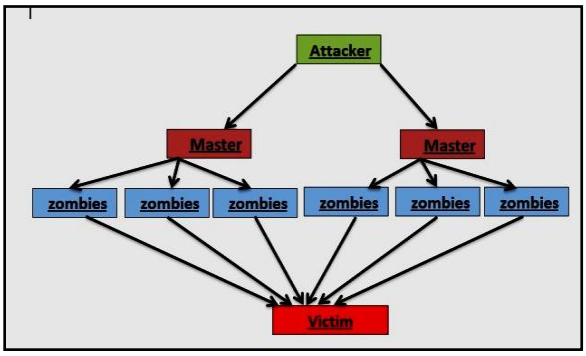

Fig. 1: DDoS Architecture

The plan of attacking and selection of the victim are decided by attacker first, and then the role of zombies is to increase the traffic or payload in such a way that it does affect the victim.

The individual attacking capacity of each compromised machine is aggregated by zombies, then to be used against a common target, by that, magnifying the effect of attack (Jun and Jae-Hyun 2011). Figure 1 showed DDoS structure and its Layers.

These slaved computers (zombies) are managed by the bot-master via ordered Command and Control channels, and then they are simultaneously used to attack a target server using the public Internet infrastructure (Bahtia and sajal,2013).

IV- DDoS FLOODING ATTACKS

This paper investigates the most popular DDoS attack, that is, attack conducted via flooding the network resources whether they are bandwidth or computing resources. This leads to preventing legitimate users from accessing services. However, this type of attack is in addition classified into many types that are listed in the following sub-sections (Fu and Zhang, 2012).

A. **TCP SYN flooding Attack** The first type of flooding attack is the "TCP SYN flooding". In this attack, the attackers used design flaws in the three-way handshake of the TCP protocol. A client first sends a SYN packet to the other client that is usually a server. A server, upon receiving the connection request, opens a new session and allocates resources for this connection and responds to the client with a SYN/ACK packet. The client then responds with an ACK packet to complete the three-way handshake. In this time, the server waits for ACK; if there is no ACK the server offers the resource to be allocated for a predefined timeout. In this case, the attacker will open and flooding a server with a huge number of TCP connections that in turn affects the server by reserving resources unnecessarily that leads to denying legitimate users from accessing (Bahtia and sajal,2013).

B. **UDP Flood** According to the same principle that is mentioned above, UDP flood attack is another type of DDoS attacks in which the victim is flooded with several of unwanted UDP packets. As a result, the victim is prevented from the intended services because of a problem of scarcity in the required bandwidth. The attacker deploys many strategies in order to assure that the attack will be succeeded. On the other hand, many victim sites do not regularly receive incoming UDP traffic and can discard attack packets by deploying simple filtering rules.

C. **ICMP Flood (SMURF ATTACK)** In this type of attack, the attacker flood victim with ICMP Echo requests. The resources and bandwidth are limited by broadcasting these Echo requests to all nodes of the target network system. Each Echo request has an echo replay; attackers in this type are changing IP address of the Echo replay to be the victim's address in order to conduct a flood in the bandwidth of victim (Fu and Zhang , 2012).

D. HTTP Flood Attack In this type of attack, the application layer is infected by huge traffic of TCP/IP stack. The attack comes in a shape of

a large number of 'seemingly legitimate' HTTP requests, commonly GET and POST, to the target server requesting web pages (Vardos I 2009).

V- SIMULATION OF DDoS ATTACK

OPNET is used as a simulation tool to perform DDoS attack. The University of Zakho was taken as an example for the scenario of attack against a file server.

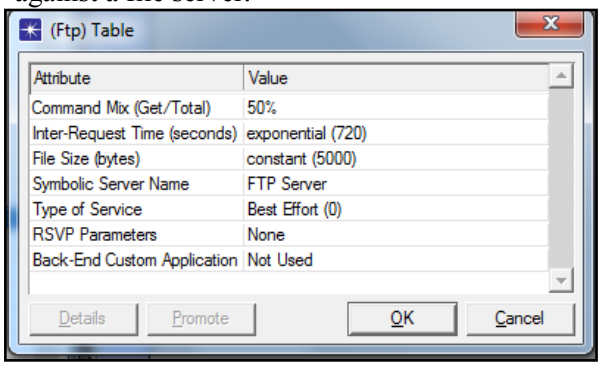

Fig. 2: File Application for Normal Users

The goal of the simulation is to have an insight into the detection scheme in addition to the impact of the attack on the campus network. Two scenarios were simulated utilizing OPNET simulator; the first one is without attack and the second one is with an attack. CPU time, response time of the server, sent traffic,
Received traffic is all measurements were taken into consideration and presented as graphs for the above-mentioned scenarios. The built file servers are shown in Figure 2 and Figure 3. Figure 2 shows a file server for normal users while Figure 3 shows a file server for abnormal users.

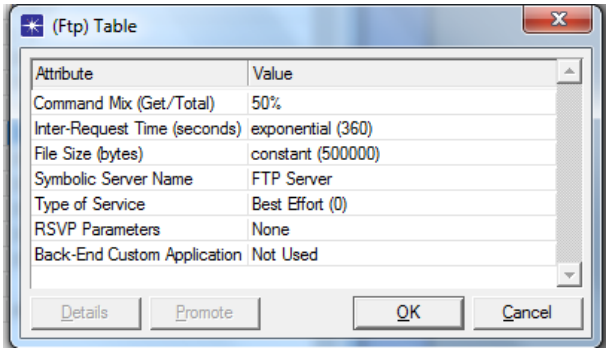

Fig. 3: File Application for Abnormal Users

The first scenario "no attack" starts at time "10 sec", and then the attack starts at time "20 sec" with different loads scenarios for all DDoS botnet (Zombies) attackers. The comprehensive topology and all users – normal users and Zombies- are all shown in Figure 4 in which Zombies are trying to attack the file server of the University of Zakho.

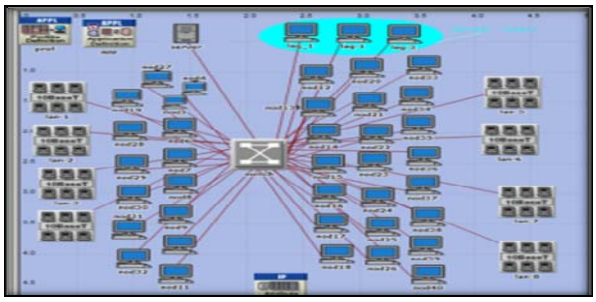

Fig. 4: The Simulated Scenario

VI- DDoS ATTACK SCENARIO RESULTS

Two scenarios were simulated for the purpose of analyzing network performance and traffic behavior. The first scenario "No Attack" is pretended to analyze the behavior of the file server traffic in the case of sending packets to three normal users. This is shown in Figure 5, in which the rate of traffic sent from users is around 18000 Bytes/sec in a form of three shipments, each user generating traffic of 6000 Bytes/sec. All start at 10 sec for whole simulation time.

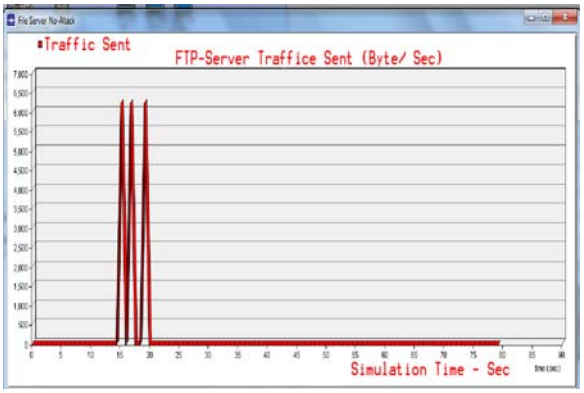

Fig. 5 FTP-Server Sent Bytes/sec

Figure 6 presents two kinds of traffic, namely; first traffic of 750 Bytes/sec form the "No-attack" users and 75 Bytes /sec from the attack users. Figure 6 depicts how DDos could influence the server and traffic behavior in the network that, in consequence, has an adverse impact on the Data-security and network efficiency

Figure 7 shows the impact of DDoS attack on legitimate users. A comparison of the received traffic by normal users is shown in both cases, attack and no attack. Results showed that 6000 Byte/sec is received in the case of –NoAttack- and this is represented in red color. On the other hand and in the case of attack, only 500 Byte/sec is received in which is shown in blue color.

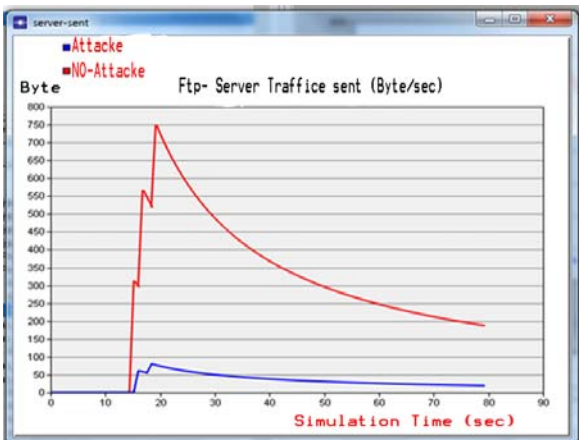

Fig. 6: Ftp-Server Traffic Sent in Both Cases – Attack and No Attack-

Figure 7 clearly shows the effect of DDoS on the University of Zakho users when they try to obtain one of the Internet services that is a File Transfer Service.

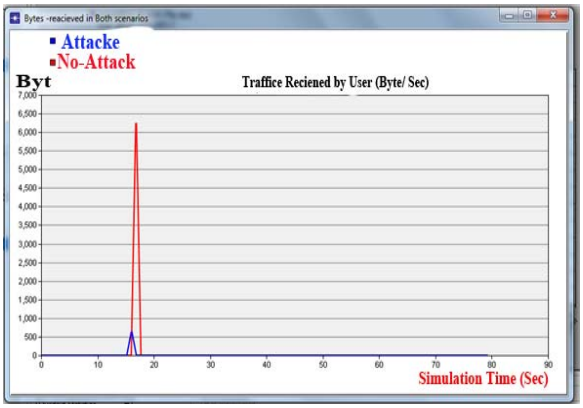

Fig. 7: Comparison of the Received Traffic by the Normal between Attack and No Attack Scenario.

In addition to the file server service, another investigation is conducted to have an insight into the effect of DDoS on video applications. Zakho University is expected to run a video server for E-learning purpose. For this reason, this service is taken into consideration. Video server could be affected when a group of zombies attack a single target server-node destination. Two scenarios were simulated, one with an attack and the other without attack. Results are shown in Figure 8 which depict the impact of DDoS attack on a video server. Results shows that a legitimate user can receive video throughput of 180.000 Bytes/sec when there is no attack, whereas, the throughput became unstable and ranging around 20.000 Bytes/sec only in the case of attack.

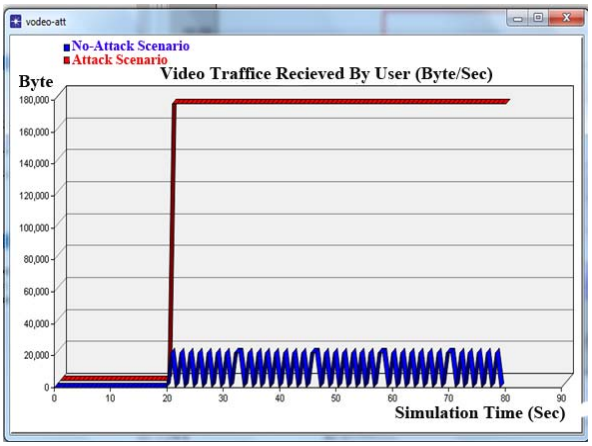

Fig. 8: Comparison of the Received Video Traffic by a Normal User between Attack and No-Attack Scenarios

VI- CONCLUSION

In this paper, a DDoS attack effect on a futuristic University of Zakho network was studied and simulated utilizing OPNET simulator. It was assumed that the proposed network would be a developed network in the essence of having facilities of developed universities such as a nice datacenter with its own email, web, and file servers. Based on this scenario, student's, employee's, staff's data as well as lectures and other E-learning materials will be accessed via the Internet. Therefore, it would be expected that the University of Zakho network would be a tempted aim for many hackers to attack to prevent students, staff, and employees (legitimate users) from accessing their materials. Two applications were considered as a case-study of the applications, which are file transfer and E-learning. Results showed that the download capability of a user reduced by 93% after the attack in the case of file transfer scenario. In addition, the DDoS attack reduced the video download for a legitimate user by 89% which means that plans should be considered to prevent such attack because those kinds of attacks can degrade the efficiency of the University of Zakho network considerably.

References

-"Aamir, M., & Zaidi, M. A. (2013)". A survey on DDoS attack and defense strategies: from traditional schemes to current techniques. *Interdisciplinary Information Sciences, 19*(2), 173-200.

-“Bhatia, S. (2013)”. Detecting distributed Denial-of-Service attacks and Flash Events.

-"Jun, J.-H., Oh, H., & Kim, S.-H. (2011)". DDoS flooding attack detection through a step-by-step investigation. Paper presented on Conference of the Networked Embedded Systems for Enterprise Applications (NESEA), 2011 IEEE 2nd International.

-"Duraipandian, M., & Palanisamy, C. (2014)". An Intelligent agent based defense architecture for DDoS attacks. Paper presented on Conference of the Electronics and Communication Systems (ICECS), 2014 International.

-"Liu, B., Berg, S., Li, J., Wei, T., Zhang, C., & Han, X. (2014)". The store-and-flood distributed reflective denial of service attack. Paper presented on Conference of the Computer Communication and Networks (ICCCN), 2014 23rd International.

-"Kolahi, S. S., Alghalbi, A., Alotaibi, A. F., Ahmed, S. S., & Lad, D. (2014)". Performance comparison of defense mechanisms against TCP SYN flood DDoS attack. Paper presented at the Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on.

-"Barati, M., Abdullah, A., Udzir, N. I., Mahmod, R., & Mustapha, N. (2014)". *Distributed Denial of Service detection using hybrid machine learning technique.* Paper presented at the Biometrics and Security Technologies (ISBAST), 2014 International Symposium on.

-"Fu, Z. (2012)". Multifaceted Defense Against Distributed Denial of Service Attacks: Prevention, Detection, Mitigation: Chalmers University of Technology.

-"Vordos, I. (2009)". Mitigating distributed denial of service attacks with Multiprotocol Label Switching--Traffic Engineering (MPLS-TE). Monterey, California. Naval Postgraduate School.

پوختە:

دڤێ لاپەری دا ئەم رابوین ب ڤەکولینەکا بەرفرەه لدور کارتێکرنا هێرشا (DOS) ل سەر چونیەتیا تورا ئینترنێتێ ل زانکویا زاخو ، وب تایبەت پشتی بدوماهی هاتنا دیزاینا ژێرخانا ئابوریێ بوڤێ توریێ ویاپێکها تیە ژتێلیێت روناهیێ (Fibre Optic) کوهاتینە بکارئینان ژبو گرێدانا ئاڤاهێن زانکویێ ب ناوەندا کومپیوتەری ڤە . وزێدە باری ڤێ چەندیێ تورا ناڤبری چەندین خزمەتگوزاریێت دی پێشکێش دکەت وەکی خزمەتگوزاریا پەیجێن ئینترنێتێ (Web) خزمەتگوزاریا ئیمێلی (Email) ، وڤەگوهاستنا بادەکا (File Transfer) . دڤێ ڤەکولینێ دا مەچەند تاقیکرن ئەنجام دان ل سەر ئیك ژگەلەك جورێن DDoS یا بەلاڤە ئەوژی هێرشا ب هێزیا هاتنا پێزانیا (Flooding Attacks) دگەل جورێن لاوەکی یێن گریدای ب وێ ڤە ب پشت بەستن ل سەر نوتیرین ڤەکولینن هاتینە ئەنجام دان دڤێ بواریدا. ژبو هەلسەنگاندن وجیاوازیێ، مەدوو خزمەتگوزاری هەلبژارتن ئەوژی (خزمەتگوزاریا ڤەگوهاستنا بادەکا، وخزمەتگوزاریا ڤیدیویێ یا دهێتە ب کارئینان دڤێرکرنا ئەلیکترونی دا (E-learning) ومە پروگرامێ OPNET بکارئینا ژبو تورازانکویا زاخو وهەر هوسا ژبو هێرشێن DDoS ژئەگەریێ باوەریێ و ب ناڤودەنگیا زێدەکوهەی دڤێ بولری دا . ئەنجام دیاربون کوهێرشا DOS کارتێکرنەکا نەرینی یازێدە هەلگرتنا بادەکا کێم دکەت ژ (6000بایت/چرکە)دەرەوشا نورمال دا بو (500بایت /چرکە)دەرەوشا هێرشان دا کو دبیە ئەگەریێ بەرزەبونا (نێزیکی)92٪ژهاتوچویا توریێ وزێدە باری ڤێ چەندیێ لەزاتیا چوگوهاستنا ڤیدیویا ژ KB/180 دچرکێ دا دەرەوشا نورمال دا بو کێمتر ژ KB/20 د چرکێ دا د رەوشا هێرشان دا کو نێزکی 89٪ ژرێژا بەرزەبونێ دپێزانینا ندا و ئەچە دهێتە زانین خراب بونا زێدە دتوریێ دا .

الخلاصة:

في هذه الورقة تم إجراء تحقيق بصورة مكثفة حول تأثير هجوم DoSعلى كفاءة شبكة جامعة زاخو ، وبالتحديد بعد اكمال تصميم نموذج البنية التحتية لهذه الشبكة والمتكون من الالياف الضوئية (Fiber Optic) المستخدم لربط ابنية الجامعة المختلفة مع مركز الحاسبة ، بلاضافة الى ذلك ، تقدم الشبكة مجموعة من الخدمات مثل خدمة صفحات الويب المتشعب (Web)، خدمة البريد الإلكتروني (Email)، وخدمة نقل الملفات (File transfer). في هذا البحث تم اجراء الأختبارات على واحد من أكثر انواع DDoS شيوعا وهو هجوم فيضان تدفق البيانات (Flooding Attacks) مع الفئات الفرعية التابعة لها استنادا على احدث البحوث المقدمة في هذا المجال . لغرض التقييم والمقارنة ، تم اختيار اثنين من خدمات الشبكة وهي (خدمة نقل الملفات و خدمة الفيديو المستخدم في التعليم الالكتروني E-learning). تم استخدام برنامجOPNET كأداة لمحاكاة شبكة جامعة زاخو وايضا للقيام بمحاكاة هجمات DDoS بسبب موثوقيته والشهرة العالية التي يتمتع بها البرنامج في هذا المجال. اظهرت النتائج ان هجوم DoS له تاثير سلبي كبيرعلى وصول المستخدمين الشرعيين لهذه الخدمتين. حيث انخفض مستوى تحميل ملف من 6000 بايت / ثانية في الحالة العادية إلى 500 فقط بايت / ثانية في حالة الهجوم مما ادى الى فقدان 92٪ في حركة مرور الشبكة تقريبا. وبالإضافة إلى ذلك، تم تقليل سرعة نقل الفيديو من 180 / KBثانية في الحالة العادية الى أقل من 20 / KBثانية في حالة الهجوم اي حوالي 89٪ كنسبة ضياع في البيانات والذي يعتبر تدهور كبير في أداء الشبكة.