Assiut Univ. J. of Mathematics and Computer Science *Printed ISSN 1687-4897*
47(1), pp1- 13(2018)

DETECTION OF APPLICATION LAYER DDOS ATTACKS BASED ON BAYESIAN CLASSIFIER

S.Khairi[*], Dalia.Nashat[*]

[*]*Department of Mathematics, Faculty of Science, Assiut University, Egypt*

Tel: 01067489645, (sahar_ahmed7258@yahoo.com ***)***

Tel: 01091000758, (dnashat@yahoo.com ***)***

Received: 24/9/2018 **Accepted:** 26/12/2018 **Available Online:** 7/7/2019

One of the major challenges in networks security is detecting network attacks. The HTTP flooding attack is the most common type of DDoS attacks that targets application layer. The malicious DDoS packets are encapsulated with the huge amount of normal traffic, so this type of attack is considered the hardest one for detection. The available detection techniques for the HTTP flooding attack usually used similarity methods for traffic attributes or machine learning algorithms but these techniques are not effective especially for large scale networks. In this paper, a new detection technique is presented based on conditional probability and Bayes' theorem. First the probability value for every normal traffic attribute is calculated. Then, we compute the conditional probability for the same attribute in any incoming connection given the occurrence of the same value in the previous normal traffic. Finally, the total probability is calculated by using the Bayes' theorem to classify it either as normal or abnormal connection. The performance of the proposed technique is evaluated by extensive simulation in terms of its detection rate, probability of false positive and false negative.

MSC (2010): 53C50, 53C40.

Keywords: *Intrusion Detection Systems, DDoS Attacks, HTTP Flooding Attack, Bayes' theorem*

1. Introduction

The real threat to network security today is cybercriminals, especially distributed denial of service (DDoS) attack, which is considered one of the most dangerous and widespread attack type. DDoS attack means denial (prevent) service about legitimate users though exhausting network resources such as routers, links, servers and others.

DDoS attack launched through attacker which first compromises relay hosts (masters), that in turn compromise attack machines (agents) as illustrated in Fig.1.The attacker begin the attack by ordering agents to send at the same time a stream of malicious packets to victim to exhaust his resources or disable the service [1].

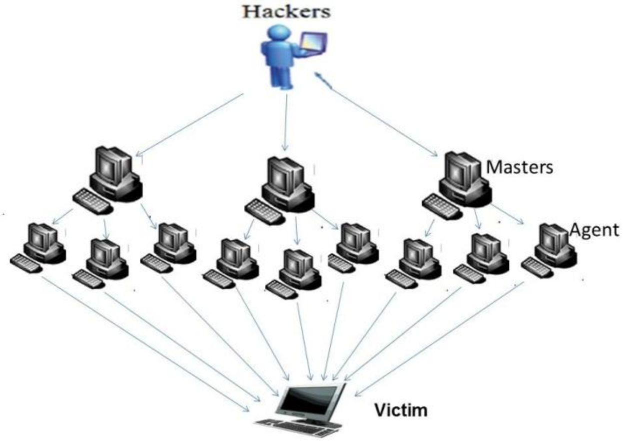

Figure 1: DDoS attack skeleton.

The DDoS attack shut down some of the most high profile web sites for example, Spamhaus 2013, BBC DDoS Attack 2015, Dyn DDoS attack 2016, Kerbs on Security 2016, Blizzard DDoS attack 2017 and Memcached attacks of March 2018 [2].

Nowadays this attack becomes stronger than before. The ATLAS network tracked 124,000 events each week between January 2015 and June 2016. In the first six months of 2016, ATLAS spotted 274 attacks over 100Gbps and 46 attacks over 200Gbps [3]. Arbor Networks reported that a US service provider suffered a 1.7 Tbps attack on March 2018 [4].

The HTTP flooding attack is one of the prevalent types of DDoS attacks that target the application layer in network. It is the hardest type to detect because the attacker takes advantage of the HTTP connections to make the malicious traffic is encapsulated within the huge amount of normal traffic [5] Therefore, our work will focus on the detection of HTTP flooding attacks.

The HTTP flooding attack is executed as illustrated in Fig.2. The attacker sends a huge number of requests to the victim (i.e. servers) through attacker or his slaves (agents). This huge number of requests exhausts the server resources and makes it unable to response to the incoming requests [6, 7].

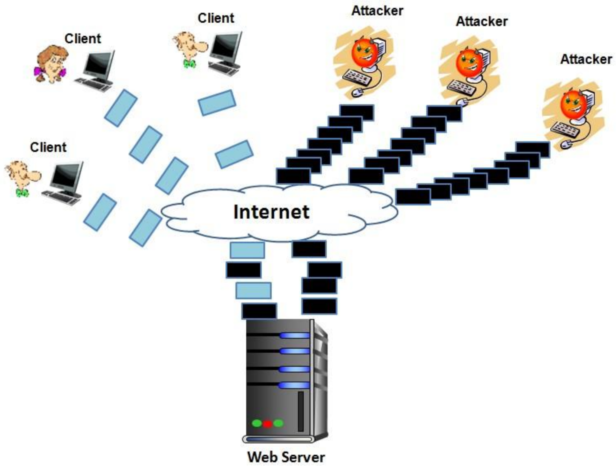

Figure 2: Architecture of HTTP Flooding attack.

The available detection schemes for HTTP flooding attack in most cases depend on two techniques. Firstly, monitoring internet traffic and system services for malicious activities or anomalies. They usually used fixed threshold for a communication patterns like source ip, connection time, arrival rate of users and periodicity connections [5, 8, 9, 10]. Secondly, using machine learning algorithms or neural network methods. In the present work, we try to avoid the drawbacks of the previous detection techniques like using fixed threshold for a communication patterns which can be avoided by attackers. Also, using machine learning algorithms which need a large amount of data and time for training.

In the proposed technique, first the probability value for every normal traffic attribute is calculated. Then, we compute the conditional probability for the same attribute in any incoming connection given the occurrence of the same value in the previous normal traffic. Finally, the total probability is calculated by using the Bayes' theorem to classify it either as normal or abnormal connection. Therefore we can appreciate how far it is normal based on previous measurements of all attributes in the normal case. The new detection system also does not require significant training data.

Many DDoS attack detection schemes have been proposed so far, like [11-17]. The authors in [11] proposed a technique using Bayesian classification algorithm and snort to predict if the given event is attack or not. This technique depends on observing previously stored network events and the Snort is used to detect known attacks. This module has low false positive and low false negative. The detection scheme in [12] used Nave Bayes model to detect network attack. The nave Bayes model is simplified Bayesian probability model, where they have a hypothesis that the given data belongs to a particular class. Then they calculate the probability for the hypothesis to be true.

Shuang et al. [13] proposed a framework to detect Remote Access Trojan (RAT) at the network borders. They use time slicing algorithm to cut the IP flow into flow slices, then frequent sequence mining was used to filter heartbeat and nave Bayes to classify the slices. They evaluated the performance of their scheme by using a week of their lab continuous traffic data and also two types of internet traffic storage.

The detection method in [14] is based on particle filter. The first step in this method get one step prediction by nonlinear flow model and the optimal estimation value is obtained by particle filter. By comparing the threshold and the difference between the estimated value of the particle filter and the one step prediction, the DDoS attack can be detected.

Nunan et al. [15] introduced an automatic classification of cross-site scripting (XSS)attacks on Web pages by extracting and analyzing predictive features of the web document content and URL, They used Naive Bayes and SVM for classification.

Authors in [16] presented a method for using Bayesian multiple hypothesis tracking to classify intrusion detection system events into attack sequences. Oke et al [17] used multiple Bayesian classifiers to take individual decisions for the monitored features of the traffic and combined them in an information fusion phase to detect DoS attacks in incoming traffic. They have presented the design of a generic DoS detection scheme which uses multiple Bayesian classifiers and the biologically inspired Random Neural Network. After selecting the input features, they obtained an estimation of probability density functions as histograms for each feature and they computed likelihood ratios. These ratios can be interpreted as first-level decisions for each feature.

2. The Conditional probability and Bayes theorem

Suppose we have two events V and N. If the occurrence of event V doesn’t affects the occurrence of event N, these events are called independent events [18]. In this case the probability is

$$P(V \cap N) = P(V) * P(N) \qquad (2.1)$$

Either if the probability of the event N changes when we take the first event V into consideration, we can say that the probability of event N is dependent of the occurrence of event V. In other words, we try to calculate the probability of the occurrence of event N given that V has already happened [18, 19].

$$P(N|V) = \frac{P(N \cap V)}{P(V)} \qquad (2.2)$$

Where *P (N∩V)* is probability of the occurrence of both *N* and *V* . If we need to know the probability of the event *V* given *N*, we need to know *P (V |N)*, so the Bayes theorem will be required.

The Bayes theorem describes the probability of an event based on the prior knowledge of the conditions that might be related to the event [19]. If we know the conditional probability of *P (V |N)*, we can use the Bayes rule to find out the reverse probabilities *P (N |V)* as follow:

$$P(V|N) = \frac{P(N \cap V)}{P(N)} \qquad (2.3)$$

From (2.2) and (2.3)

$$P(N \cap V) = P(V|N) * P(N) = P(N|V) * P(V) \qquad (2.4)$$

$$P(N|V) = P(V|N) * \frac{P(N)}{P(V)} \qquad (2.5)$$

We can generalize the formula further. If $\boldsymbol{V_1}$, $\boldsymbol{V_2}$, $\boldsymbol{V_3}$,……., $\boldsymbol{V_n}$ independent events in sample S, that for every event $N \subset S$

$$P(N) = \sum_{i=1}^{n} P(V_i) * P(N|V_i) \qquad (2.6)$$

Equ.2.6 known as theorem of total probability also if $\boldsymbol{V_1}$, $\boldsymbol{V_2}$, $\boldsymbol{V_3}$,……., $\boldsymbol{V_n}$ independent events in sample S, If occurrence one of them generate another event ***N***. where ***N*** occurs when one of these independent events have been occurred [18]

$$P(V_r|N) = \frac{P(V_r)P(N|V_r)}{\sum_{i=1}^{n} P(V_i)*P(N|V_i)} \qquad (2.7)$$

Equ.2.7 known as Bayes theorem. We can use these theorems in computing rang of normality for network connection given its attributes as described previously.

3. The proposed detection technique (CATP).

In the new detection scheme (CATP), we try to benefit from statistical concepts which described in section.2 to classify the network traffic either normal or abnormal. As illustrated in Fig.3 which illustrates the flowchart of our proposed detection technique inside one time interval. Depending on the previous idea, we calculate the probability for a connection based on its attributes as follows:

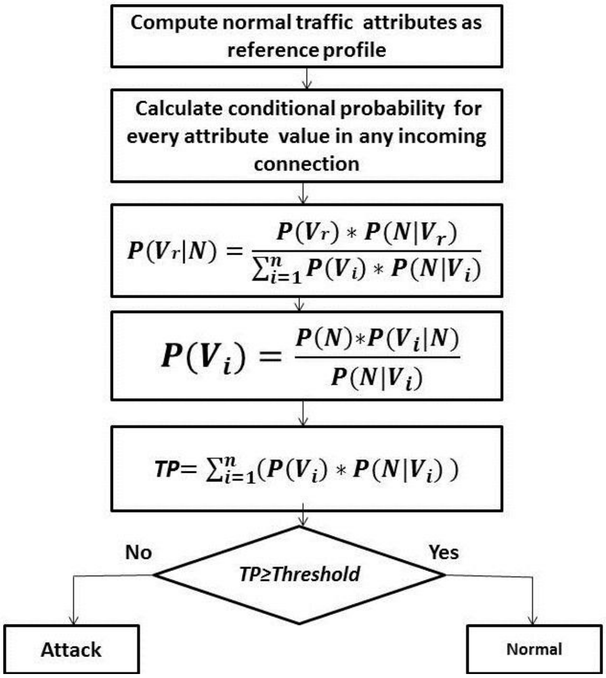
Compute normal traffic attributes as reference profile
Calculate conditional probability for every attribute value in any incoming connection
$P(V_r|N) = \frac{P(V_r) * P(N|V_r)}{\sum_{i=1}^{n} P(V_i) * P(N|V_i)}$
$P(V_i) = \frac{P(N)*P(V_i|N)}{P(N|V_i)}$
$TP = \sum_{i=1}^{n}(P(V_i) * P(N|V_i))$
No
TP≥Threshold
Yes
Attack
Normal

Figure 3: The CATP algorithm in one time interval.

Step1: During normal cases, we measure various values of attributes for server's users and their traffic and keep the statistical attributes as a reference profile matrix. In our case study we try to choose attributes that cannot be avoided by attacker. Therefore, we use *Request number* which represents the number of requests that arrives to the server in interval time, *Response number* which represent the number of responses that server can send to its clients, *open connections number* which represent the number of open connections.

Step2: For every attribute in reference profile matrix, we calculate the probability for every value and keep it in a new matrix.

$$P(value) = \frac{N_v}{N_a} \qquad (3.1)$$

N_v is the Number of the occurrence of this value and N_a is the Number of all values.

Step3: We calculate the conditional probability for every attribute in any incoming connection given occurrence the same value for the same attribute in the previous normal traffic using Bayes theorem.

$$P(V_r|N) = \frac{P(V_r)P(N|V_r)}{\sum_{i=1}^{n} P(V_i)*P(N|V_i)} \qquad (3.2)$$

Here *P(*V_r*)* calculated by using equ.3.1, *P(N |*V_{r}*)* calculated by using Poisson distribution as follows

$$F(x,\lambda) = \begin{cases} \frac{\exp^{-\lambda}*\lambda^{x}}{x!}, & \mathrm{x} = 0,1,2,3,\ldots \\ 0 & , O.W \end{cases} \qquad (3.3)$$

Where λ is the average of the same attribute values in normal case and x it is incoming attribute value (Vr) . Here (N |Vr) means normal (N) given attribute value (Vr), so we use Poisson to calculate probability with normal average.

step4: *P(Vi)* for every attribute calculated by using Equ.2.5

step5: The total probability for a connection calculated by using Equ.2.6

step6: The total probability for a connection is compared with the threshold (0.015613) to classify it either as normal or abnormal connection.

The threshold is calculated based on the attribute values of the target server in ideal case [5] without exhausting its capacity. Therefore, the threshold is computed as described from step 2 to step 5 in the previous algorithm by using the attributes values in ideal case. Therefore, we use Ideal Request number which represent the ideal number of requests that arrives to server in interval time, Ideal Response number which represent the maximum number of responses that server can send to its clients in the interval time, Ideal open connections number which represent the number of open connections in the time interval that the server can’t manage in ideal normal case.

4. Experimental results

To evaluate the performance of our technique, we perform our detection scheme on real- life Internet traces collected from the traffic archive of Clark Net WWW server. As show in table .1

Table 1: Traffic Information

Time duration	Start time	End time
Week1	00:00:00 Aug 28, 1995	23:59:59 Sep 3, 1995
Week2	00:00:00 Sep 4, 1995	23:59:59 Sep 10, 1995

To study the performance of our scheme under the HTTP flooding attack, we conducted the simulation by making injection of HTTP flooding traffic with aggregate attack rates 25 req./sec, 50 req./sec, 100 req./sec, with different attack duration. In our experiment, we used one hour traffic trace from the week1 from table.1 and detection interval time is d=10 sec.

As illustrated in Fig.4 shows the dynamics of incoming request packet distribution in normal and HTTP attack traffic with different attack rate and different attack duration. In Fig.4.a attack started at interval 30 and ended at interval 150 with total duration 120 intervals (i.e.1200 sec) and attack rate 100 req./sec. In Fig.4.b attack started at interval 160 and ended at interval 165 with total duration 6 intervals (i.e. 60 sec) and attack rate 200 req./sec.

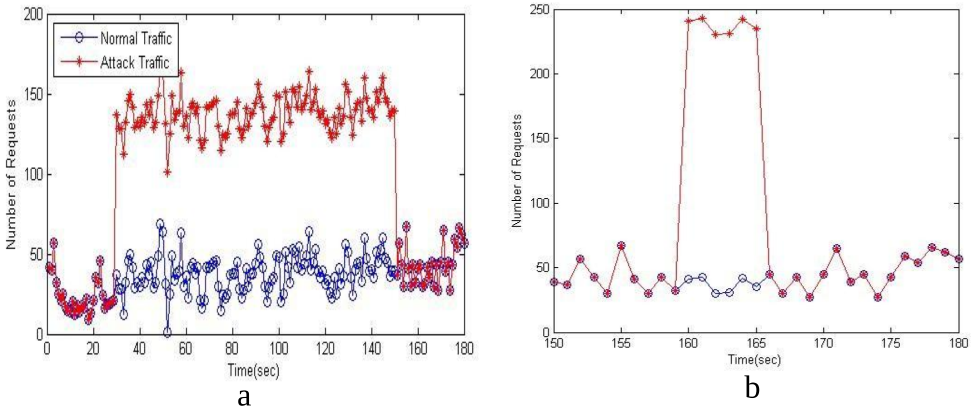

Figure 4: The dynamics of incoming requests packets in attack duration 120 and 6 intervals

Our detection technique success to detect HTTP flooding attacks with high detection rate, low false positive and low false negative As show in Fig.5 the detection rate of our technique with different attack rates 25req./sec, 50req./sec and 100req./sec for attack duration 1200 sec in Fig.5.a and rates

60req./sec, 50req./sec and 75req./sec for attack duration 6 sec in Fig.5.b. it is clear that the new technique achieves high detection rate. Also, we can easily see from figures that detection rate increases with increasing attack rate in both attack duration 120 and 6 intervals.

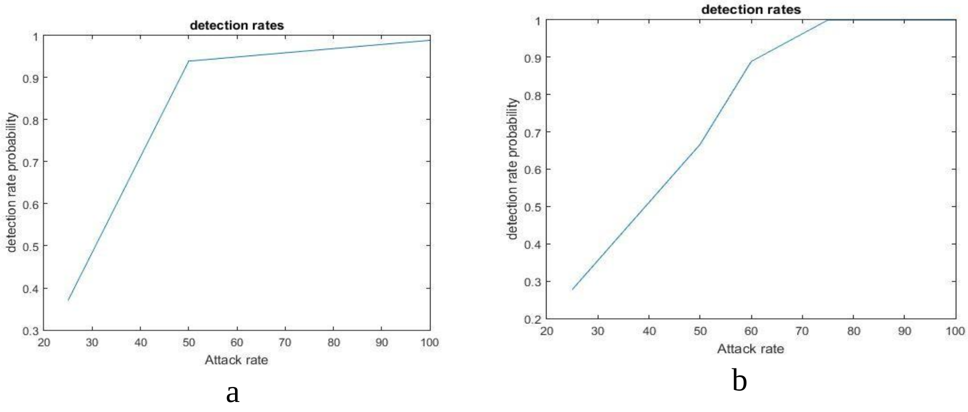

Figure 5: detection rate in attack duration 120 interval and 6 intervals

Fig.6 shows false positive probability for our technique with different attack rates 25req./sec, 50req./sec and 100req. /sec for attack duration 1200 sec in Fig.6.a and rates 25req./sec, 50req./sec, 60req./sec, 75req./sec and 100req./sec for attack duration 6 sec in Fig.6.b . It indicates that the new technique achieves low false positive probability. Also we can easily see that false positive probability decreases with increasing attack rate.

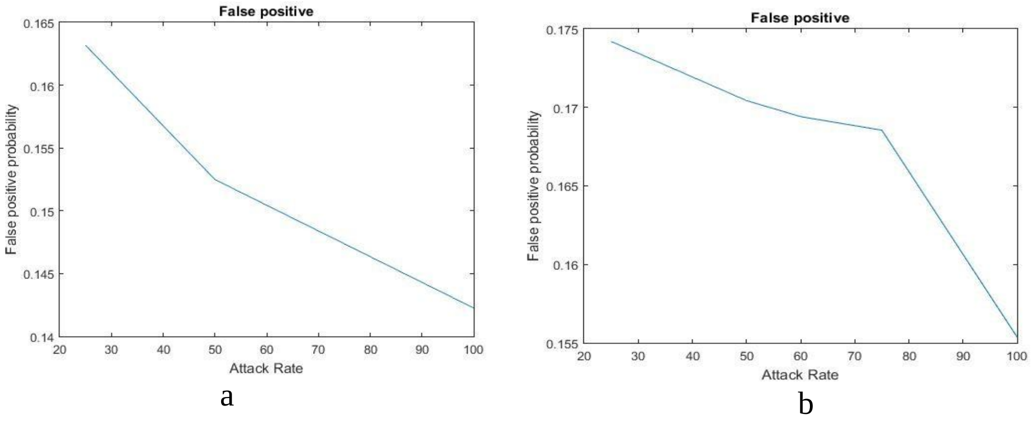

Figure 6: False Positive in attack duration 120 interval and 6 intervals

Fig.7 shows false negative probability for our technique with different attack rates 25req./sec, 50req./sec and 100req. /sec for attack duration 1200 sec in Fig.7.a and rates 25req./sec, 50req./sec, 60req./sec, 75req./sec and 100req./sec for attack duration 6 sec in Fig.7.b. It is clear that the new scheme achieves low false negative probability. Also we can easily see that false negative probability decreases with increasing attack rate.

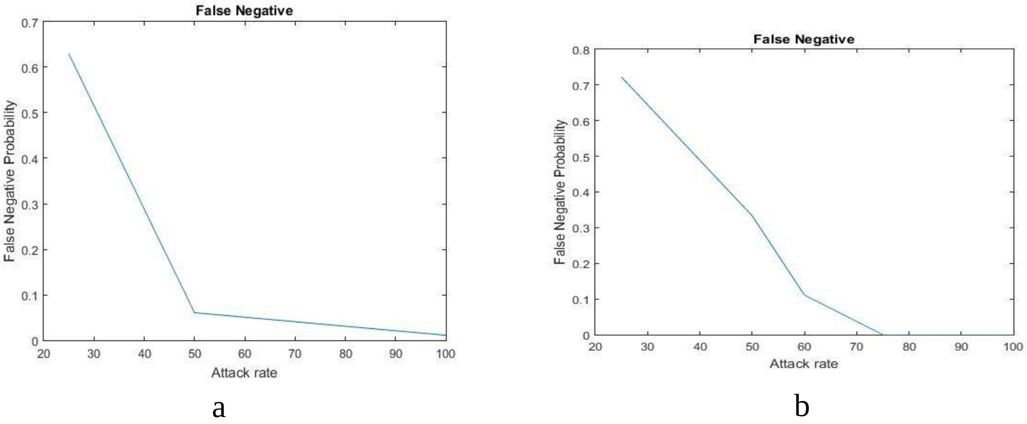

Figure 7: False Negative in attack duration 120 interval and 6 intervals

To further evaluate the performance of the proposed technique, we compare it with the connection score technique 2012 [5]. As shown in table.2

Table 2: Comparison between the CATP and connection score

Scheme	attack Duration	false positive	false negative	detection rate
Connection score	60 sec	0.24	0.0633	0.9367
CATP scheme	60 sec	0.164444	0.037037	0.962963
CATP scheme	1200 sec	0.13772	0.035813	0.964187

We can easily see that our technique success to detect all HTTP flooding attacks with 0.164444 false positive probability, 0.037037 false negative probability and 0.962963 detection rate in attack duration 60 sec. On the other hand, the connection score scheme has 0.24 false positive probability, 0.0633 false negative probability and 0.9367 detection rate for the same attack duration. Also we can show that comparison through Fig.8. Therefore, our technique can significantly achieve higher detection rate probability and reduce the false positive and false negative probability.

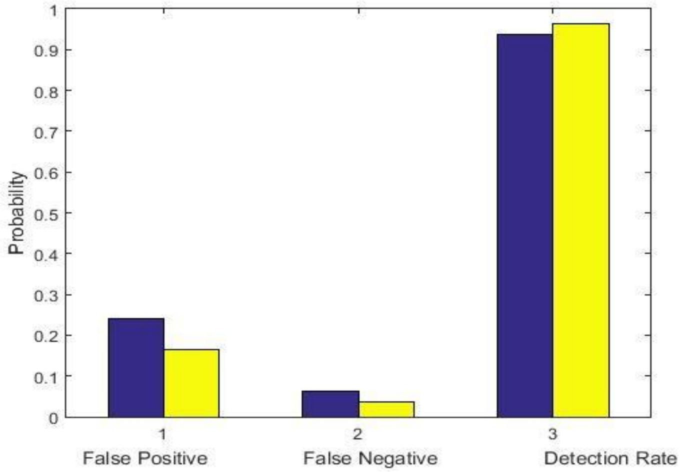

Figure 8: Comparison between The CATP and connection score.

5. Conclusion

This paper proposed The CATP detection technique of HTTP flooding attack. We demonstrated through extensive experiments that by using the conditional probability and Bayes' theorem the CATP can guarantee a very good sensitivity to HTTP flooding attack and thus significantly outperforms the available connection score technique in terms of detection rate. We also found that due to its good sensitivity, the new technique achieves low false positive and false negative probability.

References

[1] D. Nashat, X. Jiang, and S. Horiguchi, "Router based detection for low-rate agents of ddos attack," in High Performance Switching and routing, 2008. HSPR 2008. International conference on, pp. 177-182, IEEE, 2008

[2] M.Pramatarov,"https://www.cloudns.net/blog/significant-ddos-attacks recent-years/," 2018.

[3] B. David, "https://www.tripwire.com/state-of-security/incident-detection/ attackers-Launched-124000-ddos-events-per-week-over-past-18-months finds-report/,"2016.

[4] Lain Thomson, “https://www.theregister.co.uk/worlds biggest ddos attack record Broken after just five days/,2018.

[5] H. Beitollahi and G. Deconinck, “Tackling application-layer ddos attacks,” Procedia Com- puter Science, vol. 10, pp. 432–441, 2012.

[6] 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. 15, no. 4, pp. 2046–2069, 2013.

[7] D. Nashat, X. Jiang, and M. Kameyama, “Group testing based detection of web service ddos attackers,” IEICE transactions on communications, vol. 93, no. 5, pp. 1113–1121, 2010.

[8] J.-S. Lee, H. Jeong, J.-H. Park, M. Kim, and B.-N. Noh, “The activity analysis of malicious http-based botnets using degree of periodic repeatability,” in Security Technology, 2008. SECTECH’08. International Conference on, pp. 83–86, IEEE, 2008.

[9] S. Khattab, S. Gobriel, R. Melhem, and D. Moss´e, “Live baiting for service-level dos at- tackers,” in INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp. 171–175, IEEE, 2008.

[10] B. Wang, Z. Li, D. Li, F. Liu, and H. Chen, “Modeling connections behavior for web- based bots detection,” in e-Business and Information System Security (EBISS), 2010 2nd International Conference on, pp. 1–4, IEEE, 2010.

[11] C. N. Modi, D. R. Patel, A. Patel, and R. Muttukrishnan, “Bayesian classifier and snort based network intrusion detection system in cloud computing,” in Computing Communica- tion & Networking Technologies (ICCCNT), 2012 Third International Conference on, pp. 1–7, IEEE, 2012.

[12] M. Panda and M. R. Patra, “Network intrusion detection using naive bayes,” International journal of computer science and network security, vol. 7, no. 12, pp. 258–263, 2007.

[13] S. Wu, S. Liu, W. Lin, X. Zhao, and S. Chen, “Detecting remote access trojans through external control at area network borders,” in Proceedings of the Symposium on Architectures for Networking and Communications Systems, pp. 131–141, IEEE Press, 2017.

[14] Z. Wu, J. Jiang, and M. Yue, “A particle filter-based approach for effectively detecting low-rate denial of service attacks,” in Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2016 International Conference on, pp. 86–90, IEEE, 2016.

[15] A. E. Nunan, E. Souto, E. M. dos Santos, and E. Feitosa, “Automatic classification of cross- site scripting in web pages using document-based and url-based features,” in Computers and Communications (ISCC), 2012 IEEE Symposium on, pp. 000702–000707, IEEE, 2012.

[16] D. J. Burroughs, L. F. Wilson, and G. V. Cybenko, “Analysis of distributed intrusion detection systems using bayesian methods,” in pcc, pp. 329–334, IEEE, 2002.

[17] G. Oke, G. Loukas, and E. Gelenbe, “Detecting denial of service attacks with bayesian classifiers and the random neural network,” in Fuzzy Systems Conference, 2007. FUZZ- IEEE 2007. IEEE International, pp. 1–6, IEEE, 2007.

[18] S. Ross, A First Course in Probability. 1967.

[19] D. GUPT “ https://www.analyticsvidhya.com/blog/2017/03/conditional-probability- bayes-theorem/,” 2017.

الكشف عن هجوم الحرمان من الخدمة فى طبقة التطبيقات باستخدام مصنف بييز

سحر خيرى أحمد* وداليا محمد نشأت*

***قسم الرياضيات - كلية العلوم - جامعة أسيوط (مصر)**

هاتف: ٠١٠٦٧٤٨٩٦٤٥ - بريد إليكتروني Sahar_ahmed7258@yahoo.com

هاتف: ٠١٠٩١٠٠٠٧٥٨ - بريد إليكتروني dnashat@yahoo.com

فى هذا البحث تم تقديم طريقة لإكتشاف هجوم الحرمان من خدمة الانترنت والذى يتم إطلاقه فى طبقة التطبيقات لشبكات الحاسب ويعتبر هذا النوع من الهجوم على الشبكات من أكثر أنواع الهجوم إنتشاراً والأصعب فى الأكتشاف . لذالك نحن نقدم فى هذا البحث طريقة لإكتشاف هذا النوع من الهجوم باستخدام نظرية بييز والإحتمال المشروط.

ولقد حققت الطريقة المقدمة معدل إكتشاف عالى مقارنة بطرق أخرى تم تقديمها من قبل.