An Approach to Identifying the Process of Implementing a Distributed Denial of Service Attack based on a Probable Graph Model

Dmitriy A. Bachmanov[a], Michael M. Putyato[b] and Alexander S. Makaryan[c]
Kuban State Technological University, 2 Moskovskaya St., Krasnodar, Russia

Keywords: DDoS, Cyber Threats, Denial Of Service, Botnet, Neural Networks, Bayes Theorem, Probability Theory, Probabilistic Analysis, Information Security, Network Attacks.

Abstract: Distributed Denial-of-service (DDoS) attacks are one of the key threats to modern cyberspace. The main difficulty of protecting against attacks of this type is that they are implemented with the help of legitimate requests. It is possible to filter out suspicious legitimate requests by using a network filter. The purpose of this article is to create and apply a graph probability model. This article discusses the approaches derived from mathematical modeling and probabilistic estimation. Mathematical and graph models are formed to calculate the probability of an attack

1 INTRODUCTION

Today, botnets, IP spoofing as well as combination of those methods are the main means of commiting a distributed DDoS (Denial of Service) attack. Most of modern systems cannot provide timely detection or use the methods of expert systems. In addition, this kind of attacks can also be carried out by using legitimate (legitimate) requests, which greatly complicates the process of detecting and preventing these incidents.

A denial-of-service attack is designed to disable any network resource by depleting server resources. At present day, the following attack implementations are distinguished (Sinkov, Medvedev and Nikolskaya, 2018) (Figure 1)

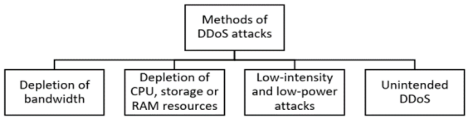

Figure 1: Methods of DDoS attack.

The first method, bandwidth depletion, can be divided into two categories of attacks:

- "Flood" attack. An attacker sends multiple packets and requests to which the network responds, causing bandwidth overflow. It is implemented within the network and transport layers of the OSI model (Open Systems Interconnection) (Moskovskij nauchno-issledovatelskij centr, 2006). Examples: ICMP flooding, UDP flooding, TCP (SYN) flooding.
- Traffic reflection and amplification-based attacks. Sending requests to multiple servers (bots) and receiving responses without additional checks. The real response, in terms of size in bytes, exceeds several times the expected response, and, for one request from 10 sources will come 10 responses. The problem of this attack (RDDoS) is that it can be detected only after a resource is unavailable, because the resource will return a response that it cannot accept.

The server resource exhaustion method is aimed at exploiting vulnerabilities in network protocols and flaws in network software. For example, exploiting flaws in XML parsers algorithms (XXE injections) or using sub-optimal regular expression processing

[a] https://orcid.org/0000-0003-3474-6831
[b] https://orcid.org/0000-0001-9974-7144
[c] https://orcid.org/0000-0002-1801-6137

Bachmanov, D., Putyato, M. and Makaryan, A.
An Approach to Identifying the Process of Implementing a Distributed Denial of Service Attack based on a Probable Graph Model.
DOI: 10.5220/0010620100003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 145-149
ISBN: 978-989-758-531-9; ISSN: 2184-9862

methods (XSS attacks) can completely deplete server RAM.

Low and Slow DDoS (LDDoS) attacks are the most difficult to detect because they cause a Denial-of-Service error on the victims network by opening multiple endless connections. This behavior is not an anomaly and does not require bandwidth depletion. Implemented at the transport and application layers of the OSI model.

Unintentional DDoS comes from users. Most often occurs after an influx of interested users to a poorly protected resource.

2 WAYS TO DETECT ATTACKS

One of the main criteria for the effectiveness of distributed denial of service attack detection systems is not only the accuracy of its identification, but also the time in which this attack was detected. The less time is spent on identifying the incident, the less the consequences of the attack and various types of losses are.

Due to the large number of types and methods of DDoS attacks leading companies are activly developing, a universal method, which could cope most effectively with this problem.

Having studied the research on the problem of detection of distributed denial of service attacks, an analysis was given (Behal and Kumar, 2016; Chen, 2020).

The first method from the list is the Signature method. It concludes in construction of characteristic relations of the "abnormal" behavior of traffic exchange and compares it with the incoming data. From the advantages we can highlight the greatest effectiveness against bandwidth-depletion attacks, or in local networks, where it is possible to make a list of source addresses, whose packets are guaranteed to be "normal".

The second is statistical methods. Of the advantages is the possibility of constructing a general model of "normal" behavior and comparing incoming traffic with it. Its disadvantages are a large number of false positives due to the unique characteristics of networks and traffic; lengthy calculation of data on the "normal" behavior; sensitive to the choice of statistical distributions.

In addition, methods based on attack detection using artificial intelligence have been increasingly studied recently (Palchevskij and Hristodulo, 2019; Diyazitdinova (Miftahova) and Gubareva, 2018).

First, the Neural Networks approach. The neurons of the network are pre-trained on data from the network users. Traffic out of the "normal" range is marked as anomalous. Signature analysis is more effective. However most of design approaches are heuristic, because they rarely lead to unambiguous solutions and network training leads to deadlocks.

The Bayesian networks approach, provides an combines Bayesian networks with statistical methods to predict outcomes or identify causal relationships. It is a graphical probabilistic model that describes multiple variables and their Bayesian relationships. The disadvantages are that it is not always feasible to determine all the interactions in Bayesian networks for complex systems.

The fuzzy logic approach is based on the fuzzy set hypothesis, according to which reasoning is estimated rather than precisely derived from classical logic. For this model, fuzzy estimates have been developed to detect DDoS attacks, which use the average time between packet receptions and also detect IP address violations in real time. But because of the peculiarities of the method, the small amount of data suitable for the analysis of distribution functions, in addition, there is a need for their forced normalization and compliance with additivity requirements, as well as the difficulty of justifying the adequacy of mathematical abstraction to describe the behavior of the actual values.

These approaches are extremely flexible, as they can be adapted to network parameters and to new data.

The Genetic Algorithms approach is to apply genetic algorithms - search algorithms based on the mechanisms of natural selection in nature. Such as selection, crossing-over, mutations, and inheritance. Genetic algorithms are able to tailor classification rules with knowledge gathered from incoming traffic and choose optimal parameters for the detection process to distinguish attacks from normal data. However it is worth highlighting their main disadvantage. A potential solution representation has to be chosen or developed to solve a specific problem and there remains the problem of defining the fitness function. In addition, there remains the problem of choosing GA parameters and there are no effective criteria for the termination of the algorithm.

The Nearest Neighbor Method detects anomalies that are far from normal instances and uses distance- or density-based measures to find similarities (or distance) between two or more data instances. Anomalies are classified using the k-nearest neighbor method. Its advantages are ease of implementation and the fact that the classification performed by this algorithm can easily be interpreted by presenting several nearest objects to the user. On the downsides, inefficient memory consumption and excessive

complication of the silver rule. It requires a linear number of operations on the sample length.

Hybrid systems combine several of the methods described above, which increases the speed and number of detected attacks, as well as reduces the number of false positives. They are capable of detecting attacks in which an attacker tries to replace attack patterns from the system databases. But this method is complex and expensive to implement.

Having analyzed the results of comparison and research of experts, we can conclude that the Bayesian networks method is the most appropriate to describe a typical DDoS attack detection system (Goldstein, Lampert, Reif, Stahl, Breuel, 2008; Polat, 2020; Vorobeva et al., 2018). The main advantage of this method is the ability to use any a priori information regarding the parameters of the model.

The information is expressed as an a priori probability or probability density function, and then, it is recalculated as an a posteriori distribution or model variables. In addition, this method is easy to understand and provides a "what if" scenario analysis for predictive modeling.

3 DETECTION SYSTEM MODEL

The main advantage of using Bayesian networks in the construction of a distributed denial-of-service attack detection system model is the ability to infer the probability of an attack by analyzing the traffic on the hosts that receive it (Federalnoe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. tri podhoda k interpretacii i ocenke neopredelennosti izmerenij).

The classic model of distributed Denial of Service attack detection system is shown in Figure 2.

Figure 2: Distributed Denial of Service attack detection system model.

The probabilistic model does not require any preprocessing, and the Bayesian method can be adapted to analyze network traffic, which will significantly speed up the process of identifying an attack.

The data collected by the sniffer can be used to determine evaluation criteria or parameters that help determine the specific type of attack. To date, there are ready-made model implementations based on this method (Bahiarov, 2018). This model proposes to introduce the following basic evaluations:

The first (P1) is a logical variable, which indicates the truth of the expression: whether the threshold of the total number of requests for the control period is exceeded.

The second one (P2) is also a logical variable, but it checks if another expression is true: if the network packet threshold for a certain protocol is exceeded in a certain period.

It is also possible to enter a formal 3rd parameter, corresponding to the number of requests from one IP address, which will help identify additional parts of the attack.

In this study, we propose to introduce a new criterion into the model that will increase the accuracy of attack detection, both in multi-agent systems and as an individual solution.

Traffic analysis and collection systems, in addition to collecting statistics on received requests, can also analyze the network infrastructure and act as a filter that, if certain conditions are met, will screen out requests at the receiving stage and prohibit their execution.

In addition, it is possible to allocate criterion P3 - which will be a logical variable that will show the truth of the expression: whether the check at the level of the primary network filter is passed.

Thus, the classic model of the detection system can be extended with one more element, some "filter" before the traffic is received by the analyzer (Figure 3).

Figure 3: An augmented model of distributed denial of service attack detection system.

The thresholds for the total number of requests and the number of requests for a particular protocol are defined as constants (normal values) based on the collected statistics of the protected service, due to the

fact that the current and maximum allowable load on the service may vary (REST strasti po 200, 2020).

The mathematical model of the 2 criteria can be represented by a general formula for detecting a distributed Denial of Service attack.

$$P(H_A|X) = \frac{P(X|H_A)P(H_A)}{P(X|H_A)P(H_A) + P(X|H_{nA})P(H_{nA})} \quad (1)$$

Where: hypothesis H_A – offensive attack, hypothesis H_{nA} – normal mode of operation, reason X – one of the parameters P1, P2 = TRUE.

It is also possible to calculate the probability of the absence or presence of an attack separately:

The formula for calculating the probability of expression for the normal number of requests received means there is no attack:

$$P(X|H_{nA}) = \frac{K_{nA}}{K_{nA} + K_A} \quad (2)$$

Where: K_{nA} – threshold value of queries, K_A – number of received queries.

The formula for calculating the probability of expression for the abnormal number of requests received means there is an attack:

$$P(X|H_A) = \frac{K_A}{K_{nA} + K_A} \quad (3)$$

Where: K_{nA} – threshold value of queries, K_A – number of received queries.

Taking as an example that the threshold value of requests for our service K_{nA} = 1000, and the resulting number of requests K_A = 2300, let us calculate the probabilities in formulas (2) and (3).

$$P(X|H_{nA}) = \frac{1000}{1000 + 2300} = 0{,}3$$

$$P(X|H_A) = \frac{2300}{1000 + 2300} = 0{,}7$$

Substituting these values into formula (1) at a priori standard probability value of 0.5 of attack, we get the following value $P(H_A|X)$.

$$P(H_A|X) = \frac{0{,}7 * 0{,}5}{0{,}7 * 0{,}5 + 0{,}3 * 0{,}5} = 0{,}7 \quad (1)$$

Since there can be more than 1 interaction protocol (e.g., HTTP, FTP, TELNET), the multipliers of variable P2 are divided into several branches (P2, P2, P2) and counted separately, depending on the specific type. P1 is calculated in a single instance, since the threshold of the total number of requests is not divided by any criteria.

All steps can be represented as a Bayesian network of trust, which will help determine the necessary calculations to obtain a value of confidence that a DDoS attack is in progress (Figure 4).

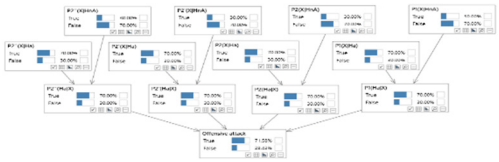

Figure 4: Bayesian trust network $P(H_A|X)$.

By setting a network identifier (filter), which will determine whether the request is from a bot or not, and concluding that the truth analysis of the variables P1, P2 will not change, when P3 = FALSE, and when P1, P2, P3 = TRUE we believe that at this time is a botnet attack, you can significantly increase the probability of identifying a distributed denial of service attack.

This allows us to represent the probability of occurrence of hypothesis H_A, provided that the request comes from the bot, in the form of an equation:

$$P(H_A|C_A) = P(C_A)\frac{P(C_A|H_A)}{P(H_A)} \quad (4)$$

Where is the reason C_A – bot request identification, hypothesis H_A – onslaught.

Taking into account the introduction of the new criterion, we derive a new formula for the probability of detecting a DDoS attack:

$$P\big(H_A|C_A, P(H_A|X)\big) = \frac{P(C_A, P(H_A|X), H_A)}{P(C_A)P(X|C_A)} \quad (5)$$

Where, hypothesis H_A – attack onset, cause C_A – Passing the surge protector, cause X – one of the parameters P1, P2 = TRUE.

(2) With the additions and optimizations, the Bayesian trust network will take a new form (Figure 5):

(3)

Figure 5: Bayesian trust network $P\big(H_A|C_A, P(H_A|X)\big)$.

Take the raw data with a standard probability value of 0.5, taking into account the credibility of the attack obtained in (1) and substitute in the formula (5) to get

the probability of a credible attack, taking into account the introduction of additional criteria

$$P(H_A|C_A, X) = \frac{0.5 * (0{,}21 + 0{,}7) * 0.7}{0.5 * 0{,}85} = 0{,}75 \quad (5)$$

When comparing the probabilities of the classical scheme and the augmented one, we can conclude that the current model allows more accurate identification of a possible threat, since another criterion is added to assess the credibility of the attack - C_A. Under the query analysis system, any solution can be installed to determine the query signature, such as the testcookie-nginx-module (Testcookie-nginx-module, 2020).

The further scenario is similar to the classic one - the detection system will display a notification of a possible attack on the user interface, which allows to identify a distributed denial-of-service attack at an early stage, since, as noted earlier, the Bayesian method allows to minimize the time to analyze the received traffic and provide the result.

4 CONCLUSIONS

The new equation allows to evaluate the effectiveness of measures used in order to find the most appropriate one. In future studies, this equation will help to evaluate new methods of protection or existing ones, with some refinements.

This algorithm, in its present form, can be used, as an auxiliary calculation of distributed DDoS attack detection probability, in more complex detection systems as a stand-alone solution, or as an addition to the existing mechanism for detecting cyber-attacks (Makaryan, Putyato and Ocheredko, 2020; Putyato et al., 2020).

REFERENCES

Sinkov A.S., Medvedev M.P., Nikolskaya K.YU. Analiz problemy obnaruzheniya raspredelennyh atak tipa "Otkaz v obsluzhivanii" // "Nauka nastroyashchego i budushchego", Mar 2018. S. 148-152.

Moskovskij nauchno-issledovatelskij centr (MNIC) Gosudarstvennyj Komitet Rossijskoj Federacii po svyazi i informatizacii. GOST R ISO/MEK 7498-1-99 Informacionnaya tekhnologiya (IT). Vzaimosvyaz otkrytyh sistem. Bazovaya etalonnaya model. CHast 1. Bazovaya model // gostrf. 2006. URL: http://www.gostrf.com/normadata/1/4294818/4294818276.pdf (Access Date: 14.01.2021).

Behal S., Kumar K. Trends in Validation of DDoS Research // International Conference on Computational Modeling and Security (CMS 2016), No. 85, 2016. pp. 7-15.

Chen J., Tang X., Cheng J., Wang F., Xu R. DDoS Attack Detection Method Based on Network Abnormal Behavior in big data environment // International Journal of Computational Science and Engineering, 2020.

Branickij A.A., Kotenko I.V. Analiz i klassifikaciya metodov obnaruzheniya setevyh atak // trudy spiiran, 2016. pp. 207-244.

Palchevskij E.V., Hristodulo O.I. Razrabotka metoda samoobucheniya impulsnoj nejronnoj seti dlya zashchity ot DDoS-atak // Programmnye produkty i sistemy, No. 3, 2019.

Diyazitdinova (Miftahova) A., Gubareva Yu. Issledovanie vozmozhnosti metodov iskusstvennogo intellekta pri raspoznavanii dos/ddos atak // problemy tekhniki i tekhnologii telekommunikacij. opticheskie tekhnologii v telekommunikaciyah, 2018. pp. 326-327.

Goldstein, Lampert, Reif , Stahl , Breuel. Bayes Optimal DDoS Mitigation by Adaptive History-Based IP Filtering // Seventh International Conference on Networking, Mar 2008.

Polat, Polat, Cetin. Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models // Open Access Journal, Feb 2020. pp. 1-16.

Vorobeva YU.N., Katasyova D.V., Katasyov A.S., Kirpichnikov A.P. Nejrosetevaya model vyyavleniya ddos-atak // vestnik tekhnologicheskogo universiteta, Vol. 21, No. 2, 2018. pp. 94-98.

Federalnoe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. tri podhoda k interpretacii i ocenke neopredelennosti izmerenij // https://files.stroyinf.ru/Data2/1/4293766/4293766795.pdf. 2014.

Bahiarov. Teorema Bajesa kak metod opredeleniya atak tipa otkaz v obsluzhivanii // Simvol nauki, 2018.

REST strasti po 200 [Electrionic resurce] // habr: [Web Site]. [2020]. URL: https://habr.com/ru/post/440900/

Testcookie-nginx-module [Electrionic resurce] // kyprizel: [Web Site]. [2020]. http://kyprizel.github.io/testcookie-nginx-module/

Makaryan A.S., Putyato M.M., Ocheredko A.R. Informacionnye sistemy i tekhnologii v modelirovanii i upravlenii // Analiz prakticheskoj realizacii mekhanizmov vyyavleniya kiberatak v siem-sisteme splunk. YAlta. May 2020. S. 252-256.

Putyato M.M., Makaryan A.S., CHerkasov A.N., Gorin I.G. Adaptivnaya sistema kompleksnogo obespecheniya bezopasnosti kak element infrastruktury situacionnogo centra // Prikaspijskij zhurnal: upravlenie i vysokie tekhnologii, 2020. pp. 75-84