DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy C-Means Clustering

Sergii Lysenko[1][0000-0001-7243-8747], Oleg Savenko[1][0000-0002-4104-745X] and Kira Bobrovnikova[1][0000-0002-1046-893X]

[1] Department of Computer Engineering and System Programming
Khmelnitsky National University,
Instytutska, 11, Khmelnitsky, Ukraine
sirogyk@ukr.net,savenko_oleg_st@ukr.net,
bobrovnikova.kira@gmail.com,
http://ki.khnu.km.ua

Abstract. A new technique for the DDoS botnet detection based on the botnets network features analysis is proposed. It uses the semi-supervised fuzzy c-means clustering. The proposed approach includes the learning and the detection stages. Analysis is based on the extracted from the network traffic features that may indicate the presence of the DDoS botnets' presence in the network. Experimental results demonstrated that the proposed technique ensures the DDoS botnet detection at the rate at about 95%.

Keywords: Botnet, Botnet Detection, DDoS, DDoS Botnet, corporate area networks, Fuzzy C-means Clustering, Cyber Attack.

1 Introduction

Today one of the most dangerous type of the malware is the botnet - a group of infected Internet-connected devices with malware and used to control it from a remote location without the knowledge of the device's owner. One of the malicious purposes botnets are used are the spam or DDoS attacks [1, 2]. DDoS botnets' attack is considered as the biggest threat to IT industry, and increasing of the intensity, size and frequency of the attacks are observed every year. DDoS botnets' attacks can primarily compromise the availability of the system services leading to financial damage or affecting the reputation of the corporate area networks. That is why there is a strong need for development of the efficient techniques for DDoS botnets' detection to impede these attacks.

2 Related Works

Today there are many attempts for the development of the DDoS botnet detection techniques. In [3] an overview of DDoS attacks that can be carried out in cloud environment and possible defensive mechanisms and tools are presented.

In [4] an approach for the detection and mitigation of known and unknown DDoS attacks in real time environments is proposed. An Artificial Neural Network (ANN) algorithm to detect DDoS attacks based on specific characteristic features (patterns) that separate DDoS attack traffic from genuine traffic was chosen.

In [5] research is related to DDoS attack mitigation solutions in the cloud. In particular, a comprehensive survey with a detailed insight into the characterization, prevention, detection, and mitigation mechanisms of these attacks were presented. A comprehensive solution taxonomy to classify DDoS attack solutions was presented. A definite guideline on effective solution building and detailed solution requirements to design the defense mechanisms was provided.

In [6] basically three contributions were offered: an abstract model for the aforementioned class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment was introduced; an inference algorithm that is shown to provide a consistent estimate of the botnet possibly hidden in the network was devised.

The work [7] outlines an evaluation tool and evaluates an amplification attack based on the Trivial File Transfer Protocol (TFTP). Mitigation methods to this threat have been considered and a variety of countermeasures are proposed. The approach presents the adjustment of the attack, detection and its mitigation.

In [8] an analysis of Mirai's botnet were provided. The Mirai represents a new type of the botnet that can compromise enough low-end devices to threaten even some of the best-defended targets. To address this risk, technical and nontechnical interventions were proposed.

The main drawbacks of the described above approaches are the low rate of the detection efficiency of the DDoS botnets' detection in the situation of the network employing for the purpose of the attacks performance, when the attack traffic is very much similar to legitimate traffic.

3 Previous Work

During the last years, several attempts to solve the problem of the botnet detection in the corporate area networks (CAN) were made. Approaches [9, 10] proposed the botnet detection the using the multi-agent system. The conclusion about botnet's presence was drawn using the fuzzy logic, taking into account the botnet features in the several network hosts. The botnet detection technique [11] involved the DNS-based analysis. The approach employed the passive DNS-monitoring and active DNS probing in the network. That enabled the possibility of the botnets, which used the cycling of IP mapping, "domain flux", "fast flux", DNS-tunneling evasion techniques. Based on the proposed technique the botnet detection tool BotGRABBER was developed. It abled the gathering of the DNS-traffic and analyzing the features obtained from the payload. Conclusion about possible botnet‘s presence was drawn using the clustering analysis. Approach [12] presented an evolution of the BotGRABBER system. It was enhanced by the possibility of the of the botnets localization in the CAN by the means of the combination analysis of the DNS-traffic and the behavior of the malicious software in the network hosts. Nevertheless, the main drawback of the BotGRABBER system is that it deals with the malicious DNS-traffic, and do not take into account the features of the DDoS botnets, that may employ the networks for DDoS execution. The further research is to extend the functionality of the BotGRABBER system with ability to analyze the network traffic and to detect the botnets that execute DDoS attacks.

4 DDoS Botnet Detection Technique Based on the Use of the Semi-Supervised Fuzzy C-Means Clustering

A new technique for the DDoS botnet detection based on the botnets network features analysis is proposed. It uses the semi-supervised fuzzy c-means clustering. The proposed approach includes the learning and the detection stages. Let us consider the steps of the learning stage:

1. Knowledge formation based on the features that may indicate DDoS botnet attacks in the network;
2. Presentation of the knowledge about the cyberattacks as a set of feature vectors;

The detection stage of the technique consists the following steps:

1. a gathering of the inbound and outbound network traffic;
2. an extraction of the features from the network traffic that may indicate the presence of the DDoS botnets' presence in the network and building a feature vector;
3. a construction of the feature vectors based on the information obtained from the network traffic;
4. the implementation of the semi-supervised fuzzy c-means clustering of the obtained feature vectors in order to label them to one of the clusters which assigns the specified DDoS botnets attack;
5. a localization of the hosts, infected with DDoS botnets.

4.1 Knowledge Formation Based on the Features that May Indicate DDoS Botnet Attacks in the Network

Let us denote the set of attacks, performed by the DDoS botnet as $A = \{a_m\}_{m=1}^{N_A}$, where a_1 – the ping flooding attack; a_2 – the smurf attack; a_3 – the TCP SYN flood attack; a_4 – the fragmented UDP flood attack; a_5 – the DNS amplification attack; a_6 – the TCP reset attack; a_7 – the ICMP flood attack; a_8 – the SIP INVITE flood attack; a_9 – the encrypted SSL DDoS attack; a_{10} – the ping sweep attack; a_{11} – the DNS spoofing attack; a_{12} – the ping of death attack; a_{13} – the R-U-Dead-Yet DDos attack (R.U.D.Y.), where N_A – the number of attacks, performed by DDoS botnets.

Let us denote the set of features, that may indicate DDoS botnet attacks and are to be analyzed as $B = \{b_j\}_{j=1}^{N_B}$, where N_B – the number of features. The list of features is presented in Table 1. Let us denote the set network hosts attacked by the DDoS botnets as $H = \{h_i\}_{i=1}^{N_H}$, where N_H – the number of network hosts. Thus, the function of the DDoS botnet attack identifying f can be presented as: $f : h_i \times b_j \to a_m$.

Table 1. The features, that take place in the DDoS botnet detection process.

Feature	Description
p	transmission protocol
f_{IO}	a boolean feature that indicates whether the inbound traffic has an associated outbound traffic record
p_{OD}	a number of packages transmitted from origin to destination
b_{OD}	a number of bytes transmitted from origin to destination
d_C	a duration of the connection
d_{EL}	a duration of the connection, observed from the earliest of the associated inbound or outbound traffic until the end of the latter traffic
l_p	an average payload length per connection
b_{TC}	a total number of bytes transmitted per connection
b_{EH}	a total number of bytes per connection excluding the header
n_{PSF}	a number of a different size of packets transferred to a total number of frames per connection
p_s	total number of packets in the session
b_s	total size for the session in bytes
d_{PSB}	standard deviation of packet size within the session measured in bytes
v_{OBP}, v_{IBP}	velocity of outbound/inbound traffic measured in bytes per packet
v_{OBS}, v_{IBS}	velocity of outbound/inbound traffic measured in bits per second
v_{OPS}, v_{IPS}	velocity of outbound/inbound traffic measured in packets per second
o_{SS}, i_{SS}	self-similarity of the outbound/inbound packets in the session, determined by examining the variance in size of the outbound/inbound packets using the Hurst exponent
n_{DP}	an amount of denied packets
n_{NAT}	a number of records in the NAT/PAT-table
n_{ARP}	a number of the ARP-requests
f_{TCP}	invalid values of TCP flags seen in this session
f_{GEO}	the geolocation feature defined by IP-address
p_R	a value of the router’ s processor’ s time, %
m_R	a size of the router’ s memory used, megabytes
s_{RT}	server response time, milliseconds

4.2 Presentation of the Knowledge About the Cyberattacks As the Set of the Feature Vectors

All the above-mentioned features are the base of the set of feature vectors $X = \{x_k\}_{k=1}^{N_x}$, where each of feature vector x_k describes the botnet’ attack and the legitimate traffic, N_X – the number of the feature vectors. Employing the obtained from the network traffic features, which are presented as the feature vectors, the set of rule R is constructed. Each rule describes specified DDoS botnet’ attack. The set of feature vectors forms the training set, which is used for the semi-supervised learning.

For instance, the rule R describes the smurf DDoS botnet’ attack can be presented as follows:

$$\begin{gathered} R: if\left(\left((d_c > \delta) or (d_{EL} > \delta'')\right) and (d_{PSB} \in [\varphi, \varphi']) and \left((v_{OBP} < \sigma) and (v_{OPS} < o) and (v_{OBS} < \kappa)\right) and \right. \\ \left. and\left((v_{IBP} < \varepsilon) and (v_{IPS} < \beta) and (v_{IBS} < \gamma)\right) and \left((o_{SS} > \tau) or (o_{IS} > \tau)\right)\right) \Rightarrow a_{13} \qquad (1) \end{gathered}$$

4.3 Labeling the Obtained Feature Vectors of the DDoS Botnets Attacks for the Purpose of the Clusters' Formation

Let *c* denote the number of the predefined clusters of feature vectors. Each cluster corresponds to the specified DDoS botnets attacks and one cluster corresponds to the legitimate network traffic. The membership of the feature vector x*k* to the i-th cluster indicates the DDoS botnets attacks performance or its absence in the network.

In order to construct the centroid (the prototype) of the i-th clusters, v*i*, the labeled data are to be assumed. It is based on the knowledge about the features that may indicate the DDoS botnets’ attacks in the network and is presented as the set of feature vectors. Each feature vector x_k of labeled data belongs to one of the predefined clusters. The semi-supervised fuzzy c-means clustering is based on the minimization of the following objective function [13]:

$$J_k = \sum_{i=1}^{c}\sum_{k=1}^{N} u_{ik}^{p} d_{ik}^{2} + \alpha \sum_{i=1}^{c}\sum_{k=1}^{N} \left(u_{ik} - f_{ik} b_k\right)^{p} d_{ik}^{2}, \qquad (2)$$

where N – the total number of the feature vectors to be clustered (labeled and unlabeled feature vectors), u_{ik} – the membership value for the *k*-th feature vector in the i-th cluster, f_{ik} – the membership value of the *k*-th labelled feature vector in the *i*-th cluster, d_{ik} – the distance between the *k*-th feature vector and prototype of the *i*-th cluster, $b = [b_k]$ – a boolean indicator, which distinguishes the labeled and unlabeled feature vectors:

$$b_k = \begin{cases} 1, if \ \ feature\, vector\ x_k \ is\ labeled, \\ 0, otherwise. \end{cases} \qquad (3)$$

The centroid of the i-th cluster, v_i, and the partition matrix u_{ik} are calculated using the formulas (4) [28]:

$$v_i = \frac{\sum_{k=1}^{N} u_{ik}^2 x_k}{\sum_{k=1}^{N} u_{ik}^2}, \quad u_{ik} = \frac{1}{1+\alpha}\left\{ \frac{1+\alpha\left(1-b_k \sum_{l=1}^{c} f_{ik}\right)}{\sum_{l=1}^{c}\left(\frac{d_{ik}}{d_{lk}}\right)^2} + \alpha f_{ik} b_k \right\}, \tag{4}$$

where α denotes a scaling factor to maintain a balance between the supervised and unsupervised component within the optimization mechanism [13].

As a distance metric between the k-th feature vector and the centroid of cluster the Mahalanobis distance was used:

$$d_{ik} = \left\| x_k - v_i \right\|^T A \left\| x_k - v_i \right\|, \tag{5}$$

with A being a positive definite matrix in $R^n \times R^n$.

4.4 Gathering the Inbound and the Outbound Network Traffic

At this stage of the method for the purpose of the DDoS botnets' attacks detection, the monitoring of the network activity, that may indicate its appearance, is performed. The gathered information is sent to the classifier for the further analysis.

4.5 Construction of the Feature Vectors and the Implementation of the Semi-Supervised Fuzzy C-Means Clustering for the DDoS Botnets Attack Classification

The features that may indicate the presence of the DDoS botnets' in the network are extracted from data gathered at the previous stage, and are to be analyzed. The result of the analysis is conclusion about the presence or absence of DDoS botnet attack. As the means of the classification is the semi-supervised fuzzy c-means clustering was used. The objects of the clustering are the feature vectors x_k, obtained in the analysis of the payload of the inbound and outbound traffic about the possible network hosts' infection. The result of clustering are the membership values u_{ik} of the feature vector x_k to each cluster i. The membership of feature vector x_k to the *i*-th cluster assigns the type of the DDoS botnets' attack.

4.6 Localization of Hosts Infected with DDoS Botnets

Based on the membership of the vector of the to malicious traffic the localization of the network host or hosts is carying out. It is performed using the logs with MAC- and IP-addresses of the hosts that carried malicious network requests.

5 Experiments

In order to determine the efficiency of the proposed technique several experiments were held. For the experiments the DDoS dataset [14] of the malicious network traffic was used. For the experiments, a network of 80 hosts was employed, and each mentioned above types of the DDoS botnets' attacks were executed (simulated).

Each experiment lasted 24 hours. Network traffic was captured by means of tcpdump utility. As the training set 15% of feature vectors of the inbound and outbound network traffic were labeled. The experimental results are presented in Table 2 and in Figure 1. The results demonstrated that the efficiency of the DDoS botnets' detection is at about 95%, while the rate of false positives is about 6%.

Table 2. Experimental results: detection and false positives rates.

Type of the DDoS botnet's attack	Number of attacks	Detected attacks	False negatives
ping flooding	10	10	0
smurf	10	9	1
TCP SYN flood	10	10	0
fragmented UDP flood	10	9	1
DNS amplification	10	10	0
TCP reset	10	10	0
ICMP flood	10	10	0
SIP INVITE flood	10	10	0
encrypted SSL DDoS	10	9	1
ping sweep	10	9	1
DNS spoofing	10	10	0
ping of death	10	10	0
R.U.D.Y.	10	8	2
Total	130	124 (95,38%)	6

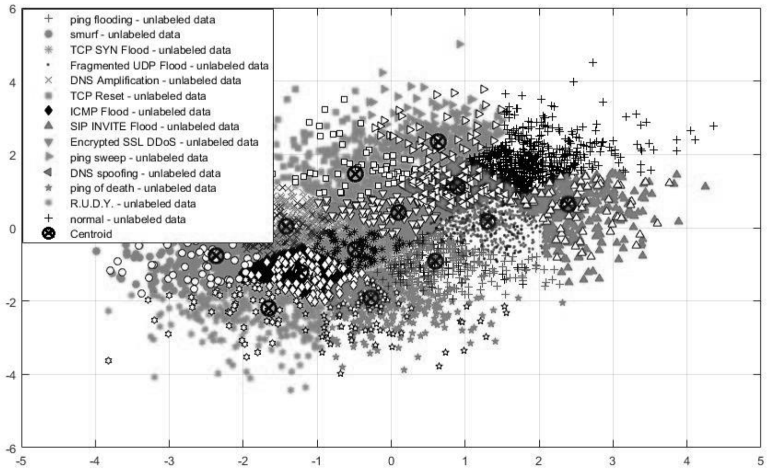

Fig. 1. Results of clustering.

6 Conclusions

A new technique for the DDoS botnet detection based on the botnets network features analysis is proposed. It uses the semi-supervised fuzzy c-means clustering. The proposed approach includes the learning and the detection stages. Analysis is based on the extracted from the network traffic features that may indicate the presence of the DDoS botnets' presence in the network. Experimental results demonstrated that the detection rate is at about 95% and false positives 6%.

References

1. Virus Bulletin, https://www.virusbulletin.com/, last accessed 2018/03/26.
2. Cisco. A Cisco Guide to Defending Against Distributed Denial of Service Attacks, https://www.cisco.com/c/en/us/about/security-center/guide-ddos-defense.html, last accessed 2018/03/26.
3. Gupta, B. B., Badve, O. P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. Neural Computing and Applications, vol. 28, No. 12, pp. 3655-3682 (2017).
4. Saied, A., Overill, R. E., Radzik, T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. Neurocomputing, vol. 172, pp. 385-393 (2016).
5. Somani, G., Gaur, M. S., Sanghi, D., Conti, M., Buyya, R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, vol. 107, pp. 30-48 (2017).
6. Matta, V., Di Mauro, M., Longo, M. DDoS attacks with randomized traffic innovation: botnet identification challenges and strategies. IEEE Transactions on Information Forensics and Security, vol. 12, No. 8, pp. 1844-1859 (2017).
7. Sieklik, B., Macfarlane, R., Buchanan, W. J. Evaluation of TFTP DDoS amplification attack. Computers & security, No. 57, pp. 67-92 (2016).
8. Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Kumar, D. Understanding the mirai botnet. In USENIX Security Symposium, pp. 1092-1110 (2017).
9. Lysenko, S., Savenko, O., Kryshchuk, A., Kljots, Y. Botnet detection technique for corporate area network. In: Proceedings of the 2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), pp. 363-368 (2013).
10. Savenko, O., Lysenko, S., Kryshchuk, A. Multi-agent Based Approach for Botnet Detection in a Corporate Area Network Using Fuzzy Logic. In: International Conference on Computer Networks: Springer, pp. 146-156 (2013).
11. Pomorova, O., Savenko, O., Lysenko, S., Kryshchuk, A., Bobrovnikova, K. Antievasion technique for the botnets detection based on the passive DNS monitoring and active DNS probing. In: International Conference on Computer Networks: Springer International Publishing, pp. 83-95 (2016).
12. Lysenko, S., Savenko, O., Bobrovnikova, K., Kryshchuk, A., Savenko, B. Information Technology for Botnets Detection Based on Their Behaviour in the Corporate Area Network. In: International Conference on Computer Networks: Springer, Cham, pp. 166-181 (2017).
13. Pedrycz, W., Waletzky, J. Fuzzy clustering with partial supervision. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 27, No. 5, pp. 787-795 (1997)
14. Canadian Institute for Cybersecurity. Botnet dataset, https://www.unb.ca/cic/datasets/botnet.html, last accessed 2018/03/26.