UOT 004.056

Nəbiyev B.R.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
babek@iit.science.az

DDoS HÜCUMLARIN AŞKARLANMASI ÜÇÜN ŞƏBƏKƏ TRAFİKİNİN KLASTERİZASİYASI METODUNUN TƏTBİQİ

Şəbəkə təhlükəsizliyində əlçatanlığın təmin olunması vacib məsələlərdən biridir. Şəbəkənin əlçatanlığına isə ən çox təsir göstərən təhdidlərdən biri DdoS hücumlardır. Bu hücumların müəyyən olunması və qarşısının alınması bu məqalənin əsas məqsədidir. Bu məqsəd üçün KDD CUP 99 verilənləri və onların analizi üçün klasterizasiya metodları seçilmişdir. Əsas analiz metodları kimi K-ortalar və EM alqoritmləri seçilmişdir.

Açar sözlər: *DDoS, klasterizasiya, K-ortalar, EM alqoritmi, şəbəkə trafiki, KDD CUP 99.*

Giriş

İnformasiya təhlükəsizliyi konfidensiallıq, əlçatanlıq və tamlığın təmin edilməsini nəzərdə tutur. Bunların hər hansı birinə təhdid yaranması mühafisə edilən informasiyaya təhlükə yaradır. DDoS (*ing. Distributed Denial of Service*) və DoS (*ing. Denial of Service*) isə bu təhlükəsizlik üçbucağında əlçatanlığın pozulmasına yönəlmiş hücumdur. DoS/DDoS kiber cinayət alətidir. Bu hücum növü hər hansı bir xidməti və ya şəbəkəni əlçatmaz etmək, şəbəkənin buraxma qabiliyyətini zəiflətmək və ya hər hansı bir xidmətin emal imkanlarından daha çox müraciət etməklə realizasiya olunur. Beləliklə, əlçatanlıq mümkün olan bütün yollarla pozulur. Amma bu heç də həmişə hücum nəticəsində baş vermir, bəzi hallarda pis konfiqurasiya olunmuş sistem və şəbəkələrdə belə hallara rast gəlinə bilər. Buna misal olaraq, hər hansı bir xəbər saytına eyni anda çoxlu adam daxil olduğu və müraciətlərin optimallaşdırılması prosesi düzgün aparılmadığı halda xidmətdən imtinanın baş verdiyini göstərmək olar.

Müasir dövrdə DDoS hücumların realizasiyası informasiya texnologiyaları sahəsində xüsusi biliklərin olmasını tələb etmir. Belə ki, bu hücumun realizasiyasını ucuz qiymətə sifariş etmək və ya bədniyyətlilər tərəfindən hazırlanmış xüsusi alətlərdən istifadə etməklə həyata keçirmək olar. Ona görə də bu istiqamətdə təhlükəsizliyin təmin olunması üçün ən son trendlər, alətlər və təhdidlər haqqında daim məlumatlı olmaq vacibdir.

Neustar şirkətinin təqdim etdiyi "*Worldwide DDoS Attacks and Cyber Insights Research Report 2017*" adlı hesabat [1] baş verən hadisələrin miqyasını daha yaxından anlamağa imkan verir. Belə ki, hesabata əsasən, "volumetric" hücumların 45%-i 10 Qbit/san, 15%-i 50Qbit/san yükləmə gücünə malikdir. Bu isə 2016-cı ilin uyğun göstəricilərindən təxminən iki dəfə çoxdur. Korporativ şəbəkələrə olan hücumların sayında isə ötən ilə nisbətən 15% artım müşahidə olunur. Təşkilatların 43%-i DDoS hücumların nəticəsində bir saat ərzində orta hesabla 250000 ABŞ dolları itirirlər, hücumların qarşısının alınması isə 51% halda 3 saatdan az çəkmir. Ən maraqlısı da odur ki, təşkilatların 99%-ndə DDoS hücumların qarşısının alınması üçün alətlər mövcuddur.

Yuxarıda deyilənlərdən göründüyü kimi, DDoS hücumlarının qarşısının alınması üçün müxtəlif alətlərdən, proqramlardan, avadanlıqlardan istifadə olunmasına baxmayaraq, bu təhdidlə mübarizə aparmaq olduqca çətin və çox vaxt aparan prosesdir.

Bu problemin həll olunması üçün bir çox elmi təşkilatlar tətqiqatlar aparırlar. Bunlardan biri də ABŞ-ın Müdafiə Nazirliyinin nəzdində fəaliyyət göstərən DARPA-dır (*ing. Defense Advanced Research Projects Agency*). DARPA 1998 IDS (*ing. İntrusion Detection System*) qiymətləndirmə proqramı MIT Lincoln Laboratory tərəfindən hazırlanıb və idarə olunur. Məqsəd müdaxilələrin aşkarlanması sahəsində tədqiqatları qiymətləndirməkdir. Bu məqalədə təklif olunan metodun yoxlanılması üçün DARPA tərəfindən hazırlanmış KDD CUP 99 verilənlər toplusundan istifadə olunub.

Verilənlərin analizi üçün *K*-ortalar və EM-klasterizasiya alqoritmləri istifadə olunmuşdur. Verilənlər toplusunda iki cür trafik mövcuddur. Birincisi, DDoS trafiki, ikinci isə normal trafik. Məlum olduğu kimi, bir çox hallarda DDoS trafikin qarşısının alınması zamanı səhvən ya inzibatçı, ya da hər hansı bir alət normal trafikin də qarşısını alır. Yaxud, DDoS trafiki normal trafik kimi qəbul edib, onu şəbəkəyə buraxır. Buna görə də məqalənin əsas məqsədi daha dəqiq nəticələrin əldə olunması və ümumiyyətlə, DDoS hücumların qarşısının alınmasıdır.

Əlaqədar işlər

Verilənlərin intellektual analizi metodları normal və anomal trafiki effektiv şəkildə və yüksək dəqiqliklə bir-birindən ayırmağa imkan verir [2, 3]. Şəbəkə trafiki haqqında informasiya əsasən monitorinq qovşaqlarından (*ing. router və server*) toplanır və DDoS hücumlarının aşkarlanması üçün IDS sistemlərində analiz olunur.

Buna misal olaraq, [4]-də DDoS hücumların aşkarlanması və qarşısının alınması üçün *K*-ortalar metodu yanaşması təklif olunur. Təcrübə üçün "*CAIDA USCD, DDoS Attack 2007 dataset*" DDoS hücumlar bazası, normal trafikin tədqiqi üçün isə "*CAİDA Anonymized Internet Traces 2008*" götürülmuş və yuxarıda göstərilən verilənlərin intellektual analizi metodu tətbiq olunmuşdur.

DDoS hücumların proaktiv aşkarlanması, yəni hücumların aşkarlanması və səbəbinin müəyyən olunması üçün [5]-də klasterizasiyanın tətbiqi ilə metod təklif olunmuşdur. DDoS hücumların proaktiv aşkarlanması üçün emalçı və agent, əlaqə və kompromis, hücumlardan ibarət dəyişənləri olan özünəməxsus arxitektur təklif olunur. Burada DDoS hücumların proseduruna baxılır və bu funksiyalar əsasında dəyişənlər seçilir. Təklif olunan metodun yoxlanılması üçün "*2000 DARPA İntrusion Detection Scenario Spesific Data Set*" bazasından istifadə edilmişdir.

Son zamanlar bədniyyətlilər DDoS hücumların realizasiyası üçün daha çox OSI modelinin tətbiq səviyyəsinə müraciət edirlər. Belə olduğu halda, OSI modelinin şəbəkə və nəqliyyat səviyyələri üçün tətbiq olunan metodlar DDoS hücumların qarşısını almaq üçün öz effektivliyini itirir. Tətbiqi səviyyədə isə ən çox təhdidə məruz qalan veb-xidmətlər olur. [6]-da tətbiqi səviyyədə DDoS hücumlarının aşkarlanması üçün ikisəviyyəli təhlil prosesi aparılır. Yəni, veb-loqlar əsasında istifadəçilərin davranışı analiz olunur və tətbiqi səviyyədə DDoS hücumların aşkarlanması sistemi və aparılan analiz arasındakı fərq təhlil olunur. Klasterizasiya prosesinin realizasiyası üçün L-Kmeans metoduna əsaslanan seyrək vektor parçalanma və "ritm" uyğunluğu (*ing. Sparse vector decomposition and rhythm matching (SVD-RM*)) mexanizmi təklif olunur.

[7]-də isə DDoS hücumların aşkarlanması üçün ranqlaşdırma (reytinq) funksiyalı adaptiv klasterizasiya metodu təklif olunur. Birincisi, şəbəkə trafikinin analizi əsasında ilkin dəyişənlər seçilir. Hədəf verilənlərin klaster strukturunu identifikasiya etmək üçün artan (*ing. incremental*) klasterizasiya alqoritminin bazası olaraq modifikasiya olunmuş "Global K-means" alqoritmi tətbiq olunur. Sonra xüsusiyyətlərin ranqlaşdırılması üçün xətti korrelyasiya əmsalı istifadə olunur. Nəhayət, xüsusiyyətlərin ranqlaşdırılması nəticələri klasterlərin yenidən hesablanması üçün istifadə olunur.

Paylanmış DoS hücumlarından biri, HTTP protokoluna yönəlmiş HTTP-GET hücumlardır. Bu hücum vasitəsilə bədniyyətlilər veb-serverə çoxlu sayda sorğular yönləndirərək xidmətdən imtinaya nail olurlar. [8]-də bu növ hücumlarla mübarizə üçün yeni metod təklif olunur. Belə ki, normal və anomal trafik əsasında fərqi müyyən etmək üçün Bayes faktorlarının tətbiqi ilə entropiya əsasında klasterizasiya metodu təklif olunmuşdur.

DDoS hücumların aşkarlanması üçün bir çox metodlar olsa da, onların əsasən ortaq iki problemi vardır. Bunlar DDoS müdaxilələrinin aşkarlanması sisteminin öyrənmə qabiliyyəti və böyük həcmli strukturlaşdırılmamış verilənlərin emalı qabiliyyətidir. Bu problemlərin həlli üçün öyrənmə qabiliyyəti olan, yeni təhdidlər qarşısında adaptasiya oluna bilən və böyük həcmli strukturlaşdırılmamış verilənlərin saxlanılması-emalı qabiliyyəti olan DDoS müdaxilələrinin aşkarlanması sistemi olmalıdır. Bu problemin həllinə ən yaxın olan yanaşma [9]-da göstərilmişdir.

Burada HBase sistemində və Apache Hadoop klasterində realizasiya olunmuş və neyron şəbəkəsi əsasında DDoS hücumların aşkarlanması təklif olunmuşdur.

KDD CUP 99 verilənlər toplusu

DARPA 1998 MAS qiymətləndirmə proqramı MIT Lincoln Laboratory tərəfindən hazırlanıb və idarə olunur. Məqsəd müdaxilələrin aşkarlanması sahəsində tədqiqatları qiymətləndirməkdir. Bu verilənlər imitasiya olunmuş şəbəkədə 9 həftə ərzində toplanıb. İmitasiya üçün ABŞ Hərbi Hava Qüvvələrinin kompüter şəbəkəsi əsas götürülüb. Verilənlər toplusu, [10]-da göstərildiyi kimi, 4 hissədən ibarətdir və 41 əlamət daxildir (cədvəl 1.), bu isə 5 milyona yaxın trafik paketi və 4Gb həcm deməkdir.

Cədvəl 1

KDD verilənlər toplusunun əlamətləri

Say	Əlamətin adı	İzahatı
1	Duration	length (number of seconds) of the connection
2	Protocol_type	type of the protocol, e.g. tcp, udp, etc.
3	Service	network service on the destination e.g. http, telnet, etc.
4	Src_bytes	number of data bytes from source to destination
5	Dst_bytes	number of data bytes from destination to source
6	Flag	normal or error status of the connection
7	Land	1 if connection is from/to the same host/port; 0 otherwise
8	Wrong_fragment	number of ``wrong'' fragments
9	Urgent	number of urgent packets
10	Hot	number of ``hot'' indicators
11	#_failed_logins	number of failed login attempts
12	Logged_in	1 if successfully logged in; 0 otherwise
13	#_compromised	number of ``compromised'' conditions
14	Root_shell	1 if root shell is obtained; 0 otherwise
15	Su_attempted	1 if ``su root'' command attempted; 0 otherwise
16	#_root	number of ``root'' accesses
17	#_file_creations	number of file creation operations
18	#_shells	number of shell prompts
19	#_access_files	number of operations on access control files
20	#_outbound_cmds	number of outbound commands in an ftp session
21	Is_host_login	1 if the login belongs to the ``host'' list; 0 otherwise
22	Is_guest_login	1 if the login is a ``guest''login; 0 otherwise
23	Count	number of connections to the same host as the current connection in the past two seconds
24	Srv_count	number of connections to the same service as the current connection in the past two seconds
25	serror_rate	% of connections that have ``SYN'' errors
26	srv_serror_rate	% of connections that have ``SYN'' errors
27	rerror_rate	% of connections that have ``REJ'' errors

28	Srv_rerror_rate	% of connections that have ``REJ'' errors
29	Diff_srv_rate	% of connections to different services
30	Srv_rerror_rate	% of connections that have ``REJ'' errors
31	Srv_diff_host_rate	% of connections to different hosts
32	Dst_host_count	count of connections having the same destination host
33	Dst_host_srv_count	count of connections having the same destination host and using the same service
34	Dst_host_same_srv_rate	% of connections having the same destination host and using the same service
35	Dst_host_diff_srv_rate	% of different services on the current host
36	Dst_host_same_src_ port_rate	% of connections to the current host having the same src_port
37	Dst_host_srv_diff_host _rate	% of connections to the same service coming from different hosts
38	Dst_host_serror_rate	% of connections to the current host that have an S0 error
39	Dst_host_srv_serror_ rate	% of connections to the current host and specified service that have an S0error
40	Dst_host_rerror_rate	% of connections to the current host that have an RST error
41	Dst_host_srv_rerror_ rate	% of connections to the current host and specified service that have an RST error

Fundamental əlamətlər: əsas əlamətlər ötürmə üçün faydalı yüklənmə nəzərə alınmadan diferensial paketlərdən əldə edilir.

Kontent: Bu halda əlamətlər TCP paketlərdə ötürmə üçün faydalı yüklənmə və uğursuz giriş cəhdlərinin qiymətləndirilməsi üçün istifadə olunur.

Trafikin zaman əsaslı əlamətləri: bu funksiyalar davamlı olaraq iki saniyədən artıq zaman ərzində baş verən hadisələr haqqında əlamətlərin əldə olunması üçün istifadə olunurlar. Bu funksiyalara hosta qoşulmaların sayının müyyən olunmasını misal göstərmək olar.

Trafikin host əsaslı əlamətləri: bu əlamət qoşulma sayını müəyyən etmək üçün zaman yerinə əvvəlki qeydlərə (*ing. historical window*) müraciət edir. Bundan əlavə, iki saniyədən çox zaman ərzində baş verən hücumların miqyasının müəyyən olunması üçün də istifadə edilir.

[11]-də KDD CUP 99 verilənlər toplusunda göstərilən hücum sinifləri aşağıdakı kimidir (cədvəl 2):

1. DoS: xidmətdən imtina.
2. Probing: müşahidə və digər skanlama növləri. Məsələn, port skanlaması.
3. U2R: lokal səlahiyyətlərə icazəsiz giriş. Məsələn, buferin yüklənməsi hücumu.
4. R2L: icazəsiz girişin əldə olunması üçün kənar kompüterlərdən müdaxilə. Məsələn, parolun seçilməsi.

KDD CUP 99 verilənlər toplusunda aşağıdaki DoS hücumlar qeydə alınmışdır:

1) **backDoS:** bu Apache serverinə yönləndirilmiş hücumdur. Bədniyyətli URL-ə müraciət edərkən çoxlu sayda əks-çarpazlardan (\) istifadə edir. Server bu cür müraciəti emal etməyə calışarkən iş qabiliyyəti aşağı düşür və digər müraciətləri emaletmə vaxtı uzanır və ya ümumiyyətlə emal edə bilmir. Bunun əsasında xidmətdən imtina baş verir.

Cədvəl 2

KDD verilənlər toplusunda qeydlərin növü, sayı, sinifləri və əlamətləri

Qeydlərin növləri	**Qeydlərin sayı**	**Qeydlərin sinifləri**	**Uyğun əlamətlər**
back	2,203	DoS	5,6
land	21	DoS	7
neptune	107,201	DoS	3.4,5,23,26.29,30,31,32,34,36,37,38,39
pod	264	DoS	8
smurf	280,790	DoS	2,3,5,6,12,25,29,30,32,36,37,39
teardrop	979	DoS	8
satan	1,589	PROBE	27
ipsweep	1,247	PROBE	36
nmap	231	PROBE	5
portsweep	1,040	PROBE	28
normal	97,277	NORMAL	3,6,12,23,25,26,29,30,33,34,35,36,37,38,39
Guess_passwd	53	R2L	11,6,3,4
ftp_write	8	R2L	9,23
imap	12	R2L	3,39
phf	4	R2L	6,10,14,5
multihop	7	R2L	23
warezmaster	20	R2L	6,1
warezclient	1,020	R2L	3,24,26
spy	2	R2L	39,1
Buffer_overflow	30	U2R	3,24,14,6
loadmodule	9	U2R	36,24,3
perl	3	U2R	14,16,18,5
rootkit	10	U2R	24,23,3

2) **landDoS:** bədniyyətli kənarda yerləşən serverin iş prosesinə xələl gətirmək üçün xüsusi formatlanmiş paket göndərə bilər və bu, nəticədə xidmətdən imtinaya gətirib çıxarır. Bu hücum TCP/IP protokolunun boşluğundan istifadə edir. Məsələn, serverə yönləndirilmiş paketin mənbə IP ünvanı və portu, təyinat IP ünvanı və portu ilə identikdirsə, deməli, bu saxta paketdir. Belə olduğu halda bu hücum serveri özü-özünə müraciət etməyə məcbur edir və nəticədə xidmətdən imtina baş verir.
3) **neptuneDoS:** emal oluna biləcəkdən daha çox sayda yarımçıq TCP/IP sessiyası yaradaraq şəbəkə və ya server avadanlığını xidmətdən imtinaya gətirib çıxarır.
4) **Ping of death (PoD) DoS:** adından göründüyü kimi, hücum ping paketlərin göndərilməsi ilə həyata keçirilir. Amma bu normal ping paketi deyil, 64000 bayt həcmli anormal ping paketidir. Server və ya şəbəkə avadanlığı belə böyük anormal ping paketi aldıqda, iş fəaliyyəti dayana və ya yenidən yüklənmə prosesinə keçə bilər.
5) **smurfDoS:** Ping göndərilən zaman paketin mənbə IP ünvanı dəyişdirilərək hücum üçün hədəf kompüterin IP ünvanı yazılır və bu paketdən eyni vaxtda müxtəlif yerlərə göndərilir. Bu paketi alan kompüterlər Ping paketinə cavab verməyə məcbur olduqları üçün hamısı bu paketə cavab verir və trafik axını yetərli qədər güclü generasiya olunsa, mənbə IP ünvanı göstərilən hədəf kompüter xidmətdən imtina hücumuna məruz qalmış olur.
6) **teardropDoS:** Göndərilən paket böyük olduğu halda qaydaya uyğun olaraq xırda hissələrə bölünür, işarələnir və qəbul edən tərəfdə yenidən toplanır. Hücum edən paketin

işarələnməsində dəyişikliklər etdiyi halda qəbul edən kompüterin bu vəziyyətə qarşı tədbiri yoxdursa, təhdid altına düşmüş olur.

Bundan başqa, KDD CUP 99 verilənlər toplusunda trafik haqqında 494020 sətir loq vardır. Bu loqların tərkibində 22 adda hücum növü və 1 adda normal trafik haqqında qeydlər vardır (cədvəl 2). Bunların 6-sı DoS hücumlar haqqında qeydlərdir. Bu məqalədə biz DoS hücumların aşkarlanmasına baxdığımız üçün KDD verilənlər toplusunun loqlarında seçmə işləri apararaq, 6 adda DoS hücumla əlaqəli olan loq sətirlərini, yəni 391458 sətri və normal trafiklə bağlı olan 97277 sətri saxlayaraq (cədvəl 2) qalanlarını KDD verilənlər toplusundan çıxarırıq (cədvəl 3). Bu redaktə prosesinin nəticəsi bizə həm sürətli, həm də dəqiq analiz aparmağa imkan verəcək.

Cədvəl 3

KDD verilənlər toplusu seçilmədən sonra

Qeydlərin adı	**Sayı**
back	2203
teardrop	979
neptune	107201
land	21
smurf	280790
pod	264
normal	97277

Daha sonra 6 adda olan DoS hücum siniflərini birləşdirərək bir DoS sinfi yaratdıq. Belə olduğu halda klasterizasiya prosesində 2 sinif iştirak etmiş olur (cədvəl 4). Bunlar özündə DoS hücumları birləşdirən DoS sinfi və normal trafiki təcəssüm edən NORMAL sinfi olur.

Cədvəl 4

DoS hücum sinifləri birləşdirildikdən sonra

Qeydlərin adı	**Sayı**
DoS	391458
Normal	97277

Analiz prosesi

Analiz prosesi *K*-ortalar və EM alqoritmi əsasında aparılır. Analiz cədvəl 4-də göstərilmiş verilənlər üzrə hər iki alqoritm əsasında aparılımışdır.

DoS hücumların aşkarlanması üçün ilkin olaraq k-ortalar klasterizasiya alqoritmi tətbiq olunur [12]. Tutaq ki, $X = \{x_1, \dots, x_n\}$ verilənlər toplusu n trafik sessiyalarından ibarətdir. Tutaq ki, hər bir trafik-sessiyası x_i Evklid fəzasında m-ölçülü nöqtə kimi təsvir edilmişdir: $x_i = (x_{i1}, \dots, x_{im})$, burada x_{ij} i-ci trafik-sessiyanın j-cu attributunun çəkisidir, $(i = 1, \dots, n;\ j = 1, \dots, m)$. Məqsəd trafik-sessiyaları, başqa sözlə $X = \{x_1, \dots, x_n\}$ verilənlər toplusunu K sayda klasterlərə bölməkdir: $C = (C_1, \dots, C_K)$. Burada fərz edirik ki, aşağıdakı şərtlər ödənilir:

1) İxtiyari p $C_p \neq \varnothing$, başqa sözlə hər bir klasterdə heç olmasa bir nöqtə olmalıdır, $p = 1,2,..., K$

2) İxtiyari $p1 \neq p2$ üçün $C_{p1} \bigcap C_{p2} = \varnothing$, yəni iki müxtəlif klaster ortaq elementləri olamamalıdır, $p1, p2 = 1,..., K$;

3) $\bigcup_{p=1}^{K} C_p = X$, yəni hər bir nöqtə hər hansı bir klasterə mütləq aid edilməlidir;

4) Klasterlər üzərinə heç bir şərt qoyulmur C_p, $p = 1,..., K$.

k-ortalar alqoritm aşağıdakı mərhələlərdən ibarətdir:

1. İlk olaraq $X = \{x_1, \dots, x_n\}$ nöqtələr toplusundan K sayda nöqtə klasterlərin mərkəzi kimi seçilir. Bu mərkəzləri $O = \{o_1, \dots, o_K\}$ ilə işarə edək və $s = 0$ qəbul edək (s iterasiyaların sayını göstərir).
2. Hər bir verilən $x_i = (x_{i1}, \dots, x_{im})$ ilə p-ci klasterin mərkəzi, $o_p = (o_{p1}, \dots, o_{pm})$, arasındakı məsafə hesablanır. Bu məsafəni hesablamaq üçün Evklid metrikasından istifadə olunur:

$$\mathrm{d}(x_i, o_p) = \left(\sum_{j=1}^{m}(x_{ij} - o_{pj})^2\right)^{\frac{1}{2}}, \; i = 1, \dots, n; \; p = 1, \dots, K, \qquad (1)$$

burada $o_{pj} - p$-ci klasterin mərkəzinin j-cu koordinatıdır.

3. x_i nöqtəsi o klasterə aid edilir ki, $\mathrm{d}(x_i, o_p)$-nin qiyməti minimum olsun, yəni $x_i \in C_p$, əgər $d(x_i, o_p) = \min_q d(x_i, o_q)$.
4. Bütün nöqtələr klasterlərə aid edildikdən sonra, aşağıdakı məqsəd funksiyasının qiyməti hesablanır:

$$f^{(s)}(x) = \sum_{p=1}^{\mathrm{K}} \sum_{\mathrm{x} \in C_p} \left\| x - o_p \right\|^2 \qquad (2)$$

Bu funksiyanın qiyməti nə qədər kiçik olarsa, klasterləşmə o qədər yaxşı hesab olunur.

5. Sonra hər bir klasterin mərkəzi aşağıdakı düsturun köməyi ilə yenidən hesablanır:

$$o_p = \frac{1}{|C_p|} \sum_{x_i \in C_p} x_i, \;, \; p = 1, \dots, K, \qquad (3)$$

burada $|C_p| - p$-ci klasterdəki nöqtələrin sayıdır.

6. $s = s + 1$
7. 3-5 addımları o vaxta qədər təkrarlanır ki, aşağıdakı yığılma şərti ödənilisin:

$$\left| \frac{f^{(s+1)}(x) - f^{(s)}(x)}{f^{(s)}(x)} \right| \le \varepsilon, \qquad (4)$$

burada ε əvvəlcədən verilmiş parametrdir.

Klasterləşmənin keyfiyyətini qiymətləndirmək üçün aşağıdakı indeksdən istifadə olunur [13]:

$$\text{Validity} = \frac{\sum_{p=1}^{K} \left\{ \frac{1}{|C_p|} \max_{x_i \in C_p} \mathrm{d}(x_i, o_p) \right\}}{\sum_{p=1}^{K} \left\{ \min_{\substack{q \neq p \\ q=1,\dots,K}} \mathrm{d}(o_p, o_q) \right\}} \qquad (5)$$

Bu indeksin qiyməti nə qədər kiçik olarsa, klasterləşmənin keyfiyyəti o qədər yüksək hesab olunur.

İkinci tətbiq olunacaq metod isə EM alqoritmidir. Cünki, EM alqoritmi müşahidə edilən məlumatların ehtimalını maksimum dərəcədə artırmaq üçün parametrləri qiymətləndirir. Bu məqsədlə aşağıda iki addım arasında təkrarlanan ehtimal loqu $L_c(\Psi)$ haqqında məlumat veriləcək.

EM alqoritminin E addımı aşağıdakı hesablamadan (*ing. computing*) ibarətdir:

$$Q(\Psi, \Psi^{(q)}) = E_{\Psi(q)}[\log L_c(\Psi) | y, z];$$

Burada Ψ-nin q iterasiyasına uyğunluğu $\Psi^{(q)}$ olur. $E_{\Psi(q)}$ isə $\Psi_{(q)}$ parametrlərindən istifadə etməyə hesablanmış riyazi gözləməni təmsil edir, yəni

$$t_{ik} = E_{\Psi(q)}[Z_{ik}|x_i, \Psi_k] = P_{\Psi(q)}[Z_{ik} = 1|x_i] = \frac{\pi_k g_k(x_i;\Psi_k)}{\sum_{k=1}^{g} \pi_k g_k(x_i;\Psi_k)}; \quad (6)$$

sonra

$$Q(\Psi, \Psi^{(q)}) = \sum_{k=1}^{g} log\pi_k \sum_{i=1}^{n} t_{ik} - \frac{np}{2} log(2\pi) - \sum_{k=1}^{g}\sum_{i=1}^{n} t_{ik} \sum_{j=1}^{p} \log(\sigma_{jk}) - \frac{1}{2}\sum_{i=1}^{n}\sum_{k=1}^{g}\sum_{j=1}^{p} \frac{t_{ik}}{\sigma_{jk}^2}(x_{ij} - m_{jk})^2$$

EM alqoritminin *M* addımı $Q(\Psi,\Psi^{(q)})$ ilə əlaqədar $\Psi^{(q)}$ gözləmənin maksimallaşdırılmasını nəzərdə tutur, yəni Ψ_{q+1} hesablanması zamanı $Q(\Psi_{q+1},\Psi^{(q)}) \geq Q(\Psi,\Psi^{(q)})$ belə müəyyən olunur və hamısı üçün $\Psi \in \Omega$ qəbul edilir. Praktikada yeniləmə tənlikləri $Q(\Psi, \Psi^{(q)})$ törəmələrinin hər bir komponentinə görə Ψ sıfra bərabər olur. Kovarians matrisini diaqonal qəbul etsək, onda

$$\pi_k^{(q+1)} = \frac{1}{n}\sum_{i=1}^{n} t_{ik}$$

$$m_{jk}^{(q+1)} = \frac{\sum_{i=1}^{n} t_{ik} x_{ij}}{\sum_{i=1}^{n} t_{ik}}$$

$$\sigma_{jk}^{(q+1)} = \sqrt{\frac{\sum_{i=1}^{n} t_{ik}\left(x_{ij} - m_{jk}^{(q+1)}\right)^2}{\sum_{i=1}^{n} t_{ik}}}$$

Klasterizasiya prosesi yuxarıda göstərilən və redaktə olunmuş KDD verilən toplusunun üzərində, WEKA aləti üzərində yerləşən Expectation-maximization (EM) klasterizasiya alqoritmi əsasında aparılır [14, 15]. EM klasterizasiya alqoritmi *K*-ortalar metoduna bənzərdir. *K*-ortalar klasterizasiyasının əsas əməliyyatları nisbətən sadədir. *K* klasterlərin müəyyən olunmuş sayını nəzərə alaraq, bu klasterlər müşahidəyə alınır ki, bütün dəyişənlər üzrə klasterlər bir-birindən mümkün qədər aralı olsunlar. EM alqoritmi bu baza yanaşmanı iki vacib yolla genişləndirir:

- Klasterlərə nümunələr təyin edilməsi və davamlı dəyişənlər arasında fərqin maksimallaşdırması əvəzinə EM klasterizasiya alqoritmi klasterin üzvlük ehtimalını bir və ya bir neçə ehtimal paylanması ilə hesablayır. Klasterizasiya alqoritminin əsas məqsədi ümumi ehtimalı və ya klasterləri nəzərə almaqla verilənlərin ehtimalının maksimallaşdırılmasıdır.
- Klassik *k*-means klasterizasiya realizasiyasından fərqli olaraq, EM alqoritmi həm kəsilməz, həm də kateqoriya dəyişənlərinə tətbiq edilə bilər.

WEKA aləti VMware virtual maşını üzərində yerləşən İntel Xeon x5670 2 nüvəli 2.93Ghz prosessor və 12Gb əməli yaddaşı olan kompüterin üzərində quraşdırılmışdır. Təhlil zamanı 10 pilləli kross yoxlama intervalı seçilmişdir. Bu hal üçün klasterizasiyanın nəticələri aşağıdakı kimidir (cədvəl 5):

Cədvəl 5

İki klaster üzrə *K*-ortalar metodunun nəticələri

0 (DoS)	1(Normal)	< - -Təyin olunmuş klasterlər
280947	110511	DoS
1107	96170	Normal

Nəticənin xəta faizi 22.8381%-dir. Göründüyü kimi, bu nəticə məqsədəuyğun deyil və reallığı əks etdirmir. Daha sonra eyni verilənlər və eyni şərtlər əsasında EM alqoritmi tətbiq edildi. Bu halda isə klasterizasiyanın nəticələri aşağıdakı kimidir (cədvəl 6):

Cədvəl 6

İki klaster üzrə EM alqoritminin nəticələri

0 (DoS)	1 (Normal)	< - -Təyin olunmuş klaster
107359	284099	DoS
683	96594	Normal

Nəticənin xəta faizi 41.7308%-dir. Göründüyü kimi, bu nəticələr də məqsədəuyğun deyil və reallığı əks etdirmir.

Bu qədər xətanın səbəbi smurf DoS hücumun trafikinin xüsusiyyətlərinin normal trafikin xüsusiyyətlərinə yaxın olmasıdır. Buna görə də biz klasterizasiyanın nəticələrinin daha dəqiq və dolğun olması üçün DoS sinfini 2 yerə böldük. DoS1 (*ing. back, teardrop, neptune, land, pod*), DoS2 (*ing.smurf*). Belə olduğu halda artıq bizdə 3 sinif olur. Bunlar DoS1, DoS2 və NORMAL siniflərdir. Buna uyğun olaraq, 1-ci eksperimentdə göstərilən parametrlər yenidən 3 sinif üçün tətbiq olundu. Alınan nəticələr *K*-ortalar metodu üçün aşağıdakı kimidir (Cədvəl 7):

Cədvəl 7

Üç klaster üzrə *K*-ortalar metodunun nəticələri

0 (DoS2)	1 (Normal)	2 (DoS1)	< - -Təyin olunmuş klasterlər
159	3200	107309	DoS 1
280788	2	0	DoS 2
736	96518	23	Normal

Bu halda isə nəticənin xəta faizi 0.843-dür.

İkinci növbədə 3 sinif üçün EM alqoritmi tətbiq olunur və nəticənin xəta faizi 0.8162-dir. Alınan nəticələrin klasterlər üzrə paylanması isə aşağıdakı kimidir (cədvəl 8).

Cədvəl 8

Üç klaster üzrə EM alqoritminin nəticələri

0 (DoS1)	1 (DoS2)	2 (Normal)	< - -Təyin olunmuş klasterlər
107175	0	3493	DoS1
0	280327	463	DoS2
33	0	97244	Normal

Klasterizasiya nəticələrinin keyfiyyətinin ölçülməsi üçün TP, TN, FP, FN metrikalarından istifadə olunur. Bunun üçün "*The Stanford Natural Language Processing Group*"-un

"*Introduction to Information Retrieval*" kitabında üç klasterli klasterizasiya ölçmə məsələsinin həlli üçün [16]-da yaradılmış proqram istifadə olunmuşdur. Nəticələr aşağıdakı kimidir (cədvəl 9):

Cədvəl 9

Klasterizasiyanın keyfiyyət göstəriciləri

Klasterizasiya metrikaları / Keyfiyyət metrikaları	*K*-ortalar	EM alqoritmi
TP	49841582762	49769015431
FP	562947427	389851298
TN	68591380159	68764476288
FN	434795397	507362728
Rand index	0.991646	0.992488
Precision	0.988831	0.992228
Recall	0.991352	0.989909
F1	0.990090	0.991067

Nəticə

Bu məqalədə klasterizasiya metodu əsasında anomal trafikin aşkarlanması və normal trafikdən seçilməsi prosesi realizasiya olunmuşdur. DARPA KDD CUP 99 verilənlər toplusundan DDoS hücumlar və normal trafik seçilərək ayrılmışdır. Aparılan eksperimentlər seçilmiş verilənlər toplusunun üzərində aparılmışdır. Verilənlər toplusunun analizi üçün EM klasterizasiya alqoritmi tətbiq olunmuşdur. İlkin mərhələdə 6 adda DoS hücum və normal trafik iki sinfə ayrılmış və EM alqoritmi tətbiq olunmuşdur. Amma alınan nəticələr məqsədəuyğun olmamışdır. Tədqiqatın nəticəsində müəyyən olunmuşdur ki, bunun səbəbi smurf DoS hücum trafikinin xüsusiyyətlərinin normal trafikin xüsusiyyətlərinə yaxın olmasıdır. DoS sinfini iki hissəyə böldükdən sonra klasterizasiya nəticələrinin daha dəqiq olduğunu görə bilərik.

Bu iş Azərbaycan Respublikasının Prezidenti yanında Elmin İnkişafı Fondunun maliyyə yardımı ilə yerinə yetirilmişdir— Qrant № EİF-KETPL-2-2015-1(25)-56/05/1

Ədəbiyyat

1. https://www.neustar.biz/about-us/news-room/press-releases/2017/dDoS2017
2. Bhaya W., Manaa M.E. Review clustering mechanisms of distributed denial of service attacks // Journal of Computer Science, 2014, vol.10, no.10, pp.2037–2046.
3. Bhuyan M.H., Kashyap H.J., Bhattacharyya D.K., Kalita J.K. Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions // The Computer Journal, 2013, vol.57, no.4, pp.537–556.
4. Bhaya W., Manaa M.E. A Proactive DDoS Attack Detection Approach Using Data Mining Cluster Analysis // Journal of Next Generation Information Technology, 2014, vol.5, no.4, pp.36–47.
5. Lee K., Kim J., Kwon K. H., Han Y., Kim S. DDoS attack detection method using cluster analysis // Expert Systems with Applications, 2008, vol.34, no.3, pp.1659–1665.
6. Liao Q., Li H., Kang S., Liu C. Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching // Security and Communication Networks, 2015, vol.8 , no.17, pp.3111–3120.
7. Zi L., Yearwood J., Wu X.W. Adaptive Clustering with Feature Ranking for DDoS Attacks Detection / International Conference on Network and System Security (NSS), 2010, pp.281–286.

8. Chwalinski P., Belavkin R., Cheng X. Detection of Application Layer DDoS Attacks with Clustering and Bayes Factors / International Conference on Systems, Man, and Cybernetics, 2013, pp.156–161.
9. Zhao T., Lo D.C., Qian K. A Neural-Network Based DDoS Detection System Using Hadoop and HBase / 17th International Conference on High Performance Computing and Communications (HPCC), 2015, pp.1326–1331.
10. Kayacık H. G., Zincir-Heywood A. N., Heywood M.I. Selecting Features for Intrusion Detection: A Feature Relevance Analysis on KDD 99 Intrusion Detection Datasets / Third Annual Conference on Privacy, Security and Trust, 2005, pp.1–6.
11. Olusola A. A., Oladele A. S., Abosede D. O., Analysis of KDD'99 Intrusion Detection Dataset for Selection of Relevance Features / Proceedings of The World Congress on Engineering and Computer Science, 2010, pp.162–168.
12. Kumari R., Sheetanshu, Singh M.K., Jha R., Singh N.K. Anomaly detection in network traffic using K-mean clustering // International Conference on Recent Advances in Information Technology (RAIT), 2016, pp.387–393.
13. Aliguliyev R.M. Performance evaluation of density-based clustering methods // Information Sciences, 2009, vol.179, no.20, pp.3583–3602.
14. Tavallaee M., Bagheri E., Lu W., Ghorbani A.A. A detailed analysis of the KDD CUP 99 data set // IEEE Symposium on Computational Intelligencein Security and Defense Applications, 2009, pp.53–58.
15. Quost B., Denœux T. Clustering fuzzy data using the fuzzy EM algorithm // Fuzzy Sets and Systems, 2016, vol.286, pp.134–156.
16. http://stats.stackexchange.com/questions/89030/rand-index-calculation

Набиев Бабек Р.
Институт Информационных Технологий НАНА, Баку, Азербайджан
babek@iit.ab.az

Применение методов кластеризации сетевого трафика для обнаружения DDoS-атак

Одной из важных проблем в сетевой безопасности является обеспечение доступности. Идентификация и предотвращение этих атак являются основной целью этой статьи. С этой целью для их анализа были выбраны данные и методы кластера KDD CUP 99. В качестве основных методов анализа были выбраны алгоритмы к-средних и EM.

Ключевые слова: *DDoS, кластеризация, к-средних, EM-алгоритм, сетевой трафик, kdd cup 99.*

Babek R. Nabiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
babek@iit.ab.az

Application of clustering methods network traffic for detecting DDoS attacks

One of the important problems of network security is availability. Identifying and preventing these attacks is the main purpose of this article. For this purpose, the data and methods of the KDD CUP 99 cluster were selected for their analysis. As the main methods of analysis, algorithms were chosen k-means and EM.

Keywords: *DDoS, clustering, k-means, EM-algorithm, network traffic, kdd cup 99.*