Primljen: 29.09.2017.
Prihvaćen: 27.10.2017.

Stručni rad
UDK: 004.738.2

Sprječavanje komunikacije BitTorrent protokolom u školskoj lokalnoj mreži

Preventing BitTorrent Protocol Comunication in the School Local Network

[1]Ivan Sekovanić, [2]Ante Javor, [3]Zoran Vrhovski
[1,3]Visoka tehnička škola u Bjelovaru, Trg Eugena Kvaternika 4, 43000 Bjelovar
[2]student Visoke tehničke škole u Bjelovaru
e-mail: [1]isekovanic@vtsbj.hr , [2]ajavor@vtsbj.hr, [3]zvrhovski@vtsbj.hr

Sažetak: *U ovom radu je opisana metoda sprječavanja komunikacije u BitTorrent mreži radi rješavanja problema nezakonitog preuzimanja sadržaja u školskoj lokalnoj mreži. Školske lokalne mreže pružaju pristup internetu velikom broju korisnika i zbog toga su podložne velikom broju prigovora zbog kršenja autorskih prava. Analiziran je način uspostavljanja i odvijanja komunikacije između sudionika u BitTorrent mreži kako bi se identificirale mogućnosti sprječavanja te komunikacije. Pokretanje preuzimanja zahtijeva kontaktiranje tracker poslužitelja ili DHT čvorova od strane sudionika preko određenih mrežnih portova. Osim toga, sudionici u BitTorrent mreži koriste određene mrežne portove za međusobnu komunikaciju. Identifikacija tih mrežnih portova omogućuje konfiguriranje vatrozida na način da se onemogući rad BitTorrent mreže. Navedena metoda pruža dovoljnu razinu zaštite za prosječnu školsku lokalnu mrežu.*

Ključne riječi: *p2p, BitTorrent, vatrozid, mrežni portovi*

Abstract: *This paper describes a method of preventing communication in the BitTorrent network to address the problem of illegal downloading in school LAN. School LANs provide Internet access for a large number of users. Therefore they are subject to a large number of copyright infringement claims. Establishing and maintaining communication between BitTorrent network peers is analyzed in order to identify the possibilities of preventing that communication. Starting a download requires contacting the tracker server or DHT nodes by the participants using certain network ports. In addition, BitTorrent network peers use certain network ports for mutual communication. Identifying these network ports allows*

configuration of the firewall with a intention of disabling BitTorrent networking. This method provides a sufficient level of protection for an average school LAN.

Keywords: *p2p, BitTorrent, firewall, network ports*

1. Uvod

BitTorrent protokol jedan je od najpoznatijih protokola za dijeljenje podatkovnih datoteka temeljen na P2P (engl. *peer to peer*) arhitekturi. P2P mrežna arhitektura pojavila se kao naprednije rješenje za dijeljenje velikih datoteka koje su postale preveliko opterećenje za dijeljenje u klasičnoj klijent-poslužitelj arhitekturi. Svako računalo sudionik u P2P mreži razmjenjuje podatke s ostalim sudionicima. Pri tom sudjeluje kao klijent koji preuzima podatke koji mu nedostaju te istovremeno kao poslužitelj podataka prema ostalim sudionicima koji te podatke potražuju. P2P arhitektura donijela je još jednu specifičnost. Podijeljenu odgovornost za distribuciju sadržaja. Dolaskom BitTorrent i ostalih srodnih protokola svi sudionici mreže, osim za preuzimanje, postaju odgovorni i za distribuciju sadržaja.

2. Razmjena nelegalnog sadržaja

U praksi postoji velik broj korisnika P2P sustava koji preuzimaju sadržaje zaštićene autorskim pravima, a koji nisu svjesni metoda zaštite identiteta u mreži. Takve korisnike povremeno detektiraju agencije koje unajmljuju ljudi iz industrije zabave. Prikuplja se trenutna IP adresa korisnika koji preuzima nezakonit sadržaj. Na temelju IP adrese agencija određuje koji se ISP (engl. *Internet Service Provider*) nalazi u posjedu te adrese. Agencija se obraća ISP-u s informacijom o povredi autorskih prava uz detalje o datoteci koja je preuzimana, vremenu kada je preuzimanje zabilježeno i IP adresi koja je preuzimala takav sadržaj. ISP iz svojih zapisa može identificirati korisnika koji je navedeni sadržaj preuzimao. Hrvatske ISP tvrtke do sada su uglavnom štitile svoje korisnike koji se bave povremenim preuzimanjem, odnosno tek na temelju sudskoga naloga dostavljaju podatke o svojim korisnicima. U tom slučaju može doći do pokretanje sudske tužbe protiv korisnika uključenog u preuzimanje takvoga sadržaja.

Za razliku od privatnih ISP-a, CARNet ima restriktivnija pravila korištenja svoje mreže (ftp://ftp.carnet.hr/pub/CARNet/docs/rules/CDA0035.pdf). U slučaju da učenici ili studenti

pristup internetu ostvaruju preko školske LAN mreže spojene na CARNet internet priključak, javlja se situacija da je školska IP adresa opterećena potencijalno velikim brojem pritužbi zbog preuzimanja sadržaja zaštićenih autorskim pravima.

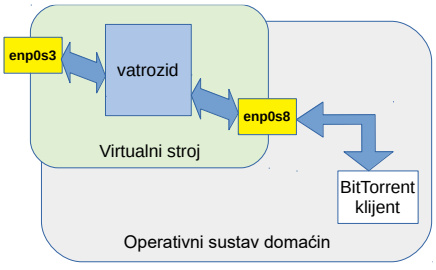
Škola može zaštiti svoj priključak tako da prati identitet korisnika koji se prijavljuju na školsku LAN mrežu. Druga mogućnost je ograničavanje brzine prijenosa podataka koju korisnik može ostvariti na LAN mreži. To rješenje, ovisno o veličini ograničenja brzine, može demotivirati određen broj korisnika od korištenja P2P sustava zbog niskih brzina preuzimanja. Loša strana ovog mehanizma je što su svi korisnici pogođeni ovim ograničenjem. Treći mehanizam, koji je tema ovog članka, je onemogućavanje komunikacije sudionika u P2P mreži. Taj oblik zaštite zahtijeva postojanje ispravno konfiguriranoga vatrozida.

3. Vatrozid

Vatrozid može biti implementiran kao samostojeći uređaj (engl. *hardware firewall*) ili kao programsko rješenje na postojećem računalu u mreži. On se mora nalaziti između LAN mreže i internet priključka (između LAN i WAN mreže). U primjeru opisanom u ovom članku korišten je programski vatrozid na postojećem računalu, zbog nižega inicijalnoga troška. Računalo je priključeno na lokalnu mrežu i ne služi kao prolaz između WAN i LAN mreže nego kao testno okruženje.

Korišteni vatrozid dio je *ClearOS* operativnog sustava, koji je temeljen na *CentOS* i *Red Hat* linux distribucijama. *ClearOS* je operativni sustav prikladan za instalaciju na mrežni poslužitelj jer osim vatrozida ima ugrađene i druge dodatke za obavljanje mrežnih zadaća (*Active Directory*, *Samba* poslužitelj, *DNS* poslužitelj, antivirus, itd.). Za potrebe ovog testiranja korištena je besplatna *Community* verzija navedenog operativnog sustava.

Slika 1 *Testno okruženje*



Izvor: Autor

Na testnom računalu instaliran je operativni sustav *Windows 10* na kojemu je instalirana aplikacija za virtualizaciju *VirtualBox*. *ClearOS* je instaliran u obliku virtualnog stroja koji je pokrenut u aplikaciji za virtualizaciju. Operativni sustav *Windows* pristupa LAN mreži i internetu preko mrežnog sučelja virtualnog stroja umjesto izravnoga pristupa mrežnoj kartici računala. *ClearOS* virtualni stroj je instaliran s dva virtualna mrežna sučelja. Prvo sučelje s oznakom „enp0s3“ ima izravan pristup lokalnoj mreži i internetu. Drugo sučelje s oznakom „enp0s8“ služi isključivo za komunikaciju između virtualnoga stroja i operativnoga sustava domaćina. Mrežni promet svih aplikacija iz *Windows* operativnog sustava usmjerava se na *ClearOS* operativni sustav preko njegovog „enp0s8“ sučelja, a zatim *ClearOS* taj promet dalje preusmjerava na svoje sučelje „enp0s3“. Između sučelja „enp0s3“ i „enp0s8“ postavljen je vatrozid koji filtrira nepoželjan mrežni promet. (slika 1)

4. Bittorrent protokol

4.1. Uspostavljanje komunikacije između sudionika

Za potrebe testiranja rada BitTorrent mreže u ovom članku, korištena je aplikacija/klijent *qBittorrent*. Svaka datoteka koja se dijeli pomoću BitTorrent mreže mora biti opisana pomoću torrent datoteke ili magnet poveznice. Nadalje će se razmatrati rad s magnet poveznicom kao rasprostranjenijom metodom, imajući u vidu da je funkcionalna razlika zanemariva. Sudionik mreže koji želi ostalim korisnicima pružiti novu datoteku za dijeljenje, mora je opisati pomoću magnet poveznice. Zatim se magnet poveznica objavljuje se na mjestu dostupnom ostalim korisnicima (npr. PirateBay) ili se ciljano šalje određenoj grupi korisnika konvencionalnim komunikacijskim kanalima. Zainteresirani korisnici preuzimaju pripadajuću magnet poveznicu i pokreću preuzimanje datoteke.

Nakon preuzimanja magnet poveznice, klijent dobiva osnovne podatke o datoteci koju preuzima i način na koji se može spojiti s rojem (engl. *swarm*) sudionika koji dijele istu datoteku. Klijentu su na raspolaganju 4 mehanizma za dohvaćanje informacija o roju.

4.1.1. Sustav trackera

Jedan je od dva važna mehanizma za uspostavljanje komunikacije s rojem u BitTorrent mreži. Tracker je poslužitelj koji održava popis sudionika u koji razmjenjuju određenu datoteku. On bilježi IP adresu i mrežni port svakog sudionika koji mu se obrati s

informacijom da sudjeluje u razmjeni određene podatkovne datoteke. (Raymond Lei Xia i Jogesh K. Muppala, 2010) Magnet poveznica u sebi sadrži adrese nekoliko tracker poslužitelja. Nakon što *qBittorrent* klijent preuzme magnet poveznicu, iz nje iščitava adrese tracker poslužitelja te ih kontaktira kako bi dobio podatke o ostalim sudionicima mreže koji dijele datoteku. *qBittorrent* od trackera dobiva IP adrese i mrežne portove ostalih sudionika, što je dovoljan podatak za uspostavljanje izravne komunikacije s ostalim sudionicima.

4.1.2. DHT sustav

DHT (engl. *Distributed Hash Table*) sustav drugi je važan mehanizam za uspostavljanje inicijalne komunikacije u BitTorrent mreži. Specifičnost tog sustava je da svaki sudionik održava dio globalne tablice sudionika, bez postojanja centraliziranog poslužitelja (Stefan Schindler, 2015.). Sudionici, osim što razmjenjuju podatkovne datoteke, razmjenjuju i dijelove tablice svih sudionika koji se nalaze u roju. Sudionici BitTorrent mreže koji sudjeluju u DHT sustavu nazivaju se DHT čvorovi. Magnet poveznica mora sadržavati adresu barem jednog DHT čvora kako bi se BitTorrent klijent povezao na DHT sustav i započeo preuzimanje podatkovne datoteke. Magnet poveznica može istovremeno sadržavati popis tracker poslužitelja i DHT čvorova i na taj način omogućiti BitTorrent klijentu da paralelno koristi oba mehanizma za uključivanje u BitTorrent mrežu. *qBittorrent* se može povezati s određenim poznatim DHT čvorovima čak i u slučaju da nisu navedeni u magnet poveznici i tako pokrenuti preuzimanje.

4.1.3. PEX mehanizam

PEX (engl. *Peer Exchange*) je još jedan raširen mehanizam koji se koristi u BitTorrent mreži. Funkcionira tako da se sudionici BitTorrent mreže međusobno obavještavaju s kojim, ostalim, sudionicima trenutačno razmjenjuju podatke. Ovaj mehanizam ne može samostalno pronaći prvog sudionika za razmjenu podataka.

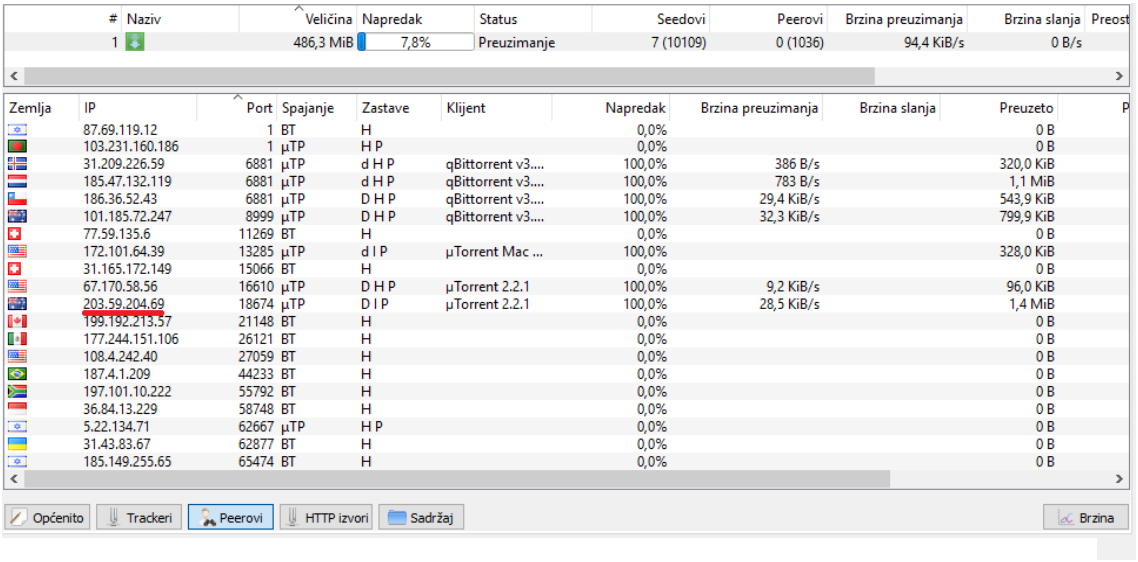
4.1.4. LSD mehanizam

LSD (engl. *Local Service Discovery*) mehanizam služi za otkrivanje sudionika BitTorrent mreže koji se nalaze na istoj lokalnoj mreži kao i klijent koji ih pretražuje. Nema velik značaj za preuzimanje datoteka.

4.2. Blokiranje komunikacije

CentOS vatrozid ima mogućnost blokiranja BitTorrent i drugih protokola. Rezultat aktivacije postavki za blokiranje BitTorrent protokola djelomično izostaje, što je vidljivo na slici 2. *qBittorrent* klijent je spojen na tracker poslužitelje, DHT čvorove i preuzima datoteke.

Slika 1 *Razmjena datoteka uz uključenu blokadu BT protokola*



#	Naziv	Veličina	Napredak	Status	Seedovi	Peerovi	Brzina preuzimanja	Brzina slanja	Preost
1		486,3 MiB	7,8%	Preuzimanje	7 (10109)	0 (1036)	94,4 KiB/s	0 B/s	

Zemlja	IP	Port	Spajanje	Zastave	Klijent	Napredak	Brzina preuzimanja	Brzina slanja	Preuzeto	P
	87.69.119.12	1	BT	H		0,0%			0 B	
	103.231.160.186	1	µTP	H P		0,0%			0 B	
	31.209.226.59	6881	µTP	d H P	qBittorrent v3....	100,0%	386 B/s		320,0 KiB	
	185.47.132.119	6881	µTP	d H P	qBittorrent v3....	100,0%	783 B/s		1,1 MiB	
	186.36.52.43	6881	µTP	D H P	qBittorrent v3....	100,0%	29,4 KiB/s		543,9 KiB	
	101.185.72.247	8999	µTP	D H P	qBittorrent v3....	100,0%	32,3 KiB/s		799,9 KiB	
	77.59.135.6	11269	BT	H		0,0%			0 B	
	172.101.64.39	13285	µTP	d I P	µTorrent Mac ...	100,0%			328,0 KiB	
	31.165.172.149	15066	BT	H		0,0%			0 B	
	67.170.58.56	16610	µTP	D H P	µTorrent 2.2.1	100,0%	9,2 KiB/s		96,0 KiB	
	203.59.204.69	18674	µTP	D I P	µTorrent 2.2.1	100,0%	28,5 KiB/s		1,4 MiB	
	199.192.213.57	21148	BT	H		0,0%			0 B	
	177.244.151.106	26121	BT	H		0,0%			0 B	
	108.4.242.40	27059	BT	H		0,0%			0 B	
	187.4.1.209	44233	BT	H		0,0%			0 B	
	197.101.10.222	55792	BT	H		0,0%			0 B	
	36.84.13.229	58748	BT	H		0,0%			0 B	
	5.22.134.71	62667	µTP	H P		0,0%			0 B	
	31.43.83.67	62877	BT	H		0,0%			0 B	
	185.149.255.65	65474	BT	H		0,0%			0 B	

Na slici 2 se nalazi prikaz IP adresa i mrežnih portova sudionika BitTorrent mreže za koje je *qBittorrent* saznao pomoću tracker i DHT sustava. Također je prikazano s kojim se sudionicima odvija razmjena datoteka. Vidi se da blokada BitTorrent protokola onemogućuje samo BT protokol koji je baziran na TCP protokolu, dok µTP protokol koji je baziran na UDP protokolu nesmetano radi. Ako se za primjer uzme sudionik s IP adresom 203.59.204.69 i napravi provjera komunikacije pomoću *Wireshark* aplikacije, dobit će se prikaz na slici 3. Na slici je vidljivo da se komunikacija odvija pomoću UDP protokola, gdje lokalni *qBittorrent* klijent svoje podatke šalje sa svog porta 6 na udaljeni port 18674, i obrnuto. Ukoliko je promet u BitTorrent mreži kriptiran, vatrozid nije sposoban zaustaviti niti BT protokol.

Slika 2 *Komunikacija sa sudionikom na IP adresi 203.59.204.69*

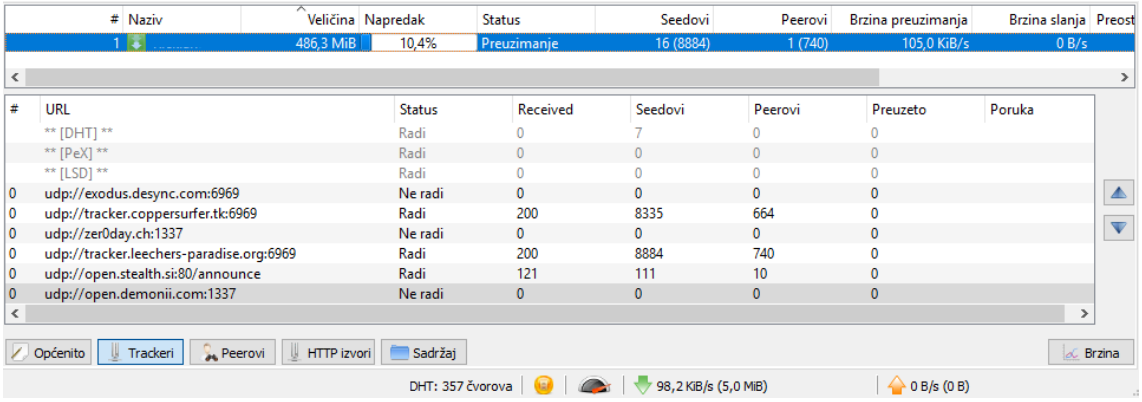
No.	Source	Destination	Protocol	Length	Info
16040	192.168.2.149	203.59.204.69	UDP	62	6 → 18674 Len=20
16042	203.59.204.69	192.168.5.21	UDP	1480	18674 → 6 Len=1438
16043	203.59.204.69	192.168.5.21	UDP	1480	18674 → 6 Len=1438
16193	192.168.2.149	203.59.204.69	UDP	62	6 → 18674 Len=20
16196	203.59.204.69	192.168.5.21	UDP	861	18674 → 6 Len=819
16199	192.168.2.149	203.59.204.69	UDP	79	6 → 18674 Len=37

Izvor: Autor

Kako bi se, ipak, zaustavio BitTorrent promet, iskorišten je mehanizam IPTABLES koji je uobičajen za vatrozide koji rade u linux okruženju. IPTABLES je mehanizam za konfiguriranje vatrozida pomoću definiranih pravila. Pravila se pohranjuju u tablice vatrozida (https://help.ubuntu.com/community/IptablesHowTo). Prilikom prosljeđivanja mrežnog prometa, vatrozid provjerava u tablicama IPTABLES mehanizma da li mrežni promet udovoljava pravilima i sukladno tome propušta ili blokira komunikaciju.

Kako bi se onemogućila komunikacija u BitTorrent mreži, određuju se odlazni mrežni portovi koje je potrebno blokirati pomoću IPTABLES mehanizma. Prvi korak je blokiranje sustava trackera. Na slici 4, u stupcu URL, vide se adrese tracker poslužitelja, mrežni port na kojem poslužitelji osluškuju dolazne veze i protokol komunikacije. Tracker poslužitelji uglavnom koriste UDP protokol te nekoliko uobičajenih mrežnih portova za komunikaciju. Najčešće su to portovi 6969 i 1337, dok se ponekad koristi port 80. Blokiranjem odlazne komunikacije prema tracker poslužiteljima na navedenim portovima onemogućuje se povratna informacija klijentu o sudionicima BitTorrent mreže.

Slika 3 *Status trackera i DHT čvorova*



Izvor: Autor

Drugi korak je blokada DHT sustava. Na slici 5 prikazana je mrežna komunikacija u kojoj *qBittorrent* klijent doznaje IP adrese poznatih DHT čvorova. Na slici 6. prikazana je komunikacija klijenta s DHT čvorovima na dohvaćenim IP adresama. Klijent koristi mrežni port 6, dok DHT čvorovi koriste mrežne portove 6881 i 25401.

Slika 4 *Inicijalno kontaktiranje DHT čvorova*

No.	Source	Destination	Protocol	Length	Info
25	192.168.5.5	192.168.5.21	DNS	171	Standard query response 0xa10a A dht.libtorrent.org A 104.168.32.188 NS
26	192.168.5.5	192.168.5.21	DNS	319	Standard query response 0x0cb8 A router.bittorrent.com A 67.215.246.10 N
27	192.168.5.5	192.168.5.21	DNS	356	Standard query response 0x9d87 A router.utorrent.com A 82.221.103.244 NS
28	192.168.2.149	192.168.2.1	DNS	82	Standard query 0xd7c0 A dht.transmissionbt.com
29	192.168.2.149	192.168.2.1	DNS	75	Standard query 0x169c A dht.aelitis.com
30	192.168.5.5	192.168.5.21	DNS	253	Standard query response 0x5f9d A dht.transmissionbt.com A 212.129.33.59

Izvor: Autor

Slika 5 *Razmjena informacija s DHT čvorovima*

No.	Source	Destination	Protocol	Length	Info
84	192.168.2.149	104.168.32.188	UDP	146	6 → 25401 Len=104
189	104.168.32.188	192.168.5.21	UDP	198	25401 → 6 Len=156
193	104.168.32.188	192.168.5.21	UDP	198	25401 → 6 Len=156
200	192.168.2.149	104.168.32.188	UDP	146	6 → 25401 Len=104

No.	Source	Destination	Protocol	Length	Info
43	192.168.2.149	82.221.103.244	UDP	146	6 → 6881 Len=104
72	192.168.2.149	82.221.103.244	UDP	146	6 → 6881 Len=104
80	192.168.2.149	82.221.103.244	UDP	146	6 → 6881 Len=104
128	82.221.103.244	192.168.5.21	UDP	528	6881 → 6 Len=486
153	82.221.103.244	192.168.5.21	UDP	528	6881 → 6 Len=486
154	82.221.103.244	192.168.5.21	UDP	528	6881 → 6 Len=486

No.	Source	Destination	Protocol	Length	Info
48	192.168.2.149	212.129.33.59	UDP	146	6 → 6881 Len=104
71	192.168.2.149	212.129.33.59	UDP	146	6 → 6881 Len=104
82	192.168.2.149	212.129.33.59	UDP	146	6 → 6881 Len=104
118	212.129.33.59	192.168.5.21	ICMP	174	Destination unreach
137	212.129.33.59	192.168.5.21	ICMP	174	Destination unreach
145	212.129.33.59	192.168.5.21	ICMP	174	Destination unreach

Izvor: Autor

Zadnji korak je blokada komunikacije između samih sudionika. Na slici 2 vidljivo je da većina sudionika za komunikaciju koristi mrežni port 6881 ili veći. Blokadom mrežnih portova u rasponu od 1024 do 65535[1], te porta 80 onemogućava se DHT i tracker sustav, kao i razmjena datoteka između sudionika mreže (iznimka je slučaj gdje je mrežni port sudionika manji od 1024, ali i tada je potreban funkcionalan tracker ili DHT kako bi se saznalo za tog sudionika).

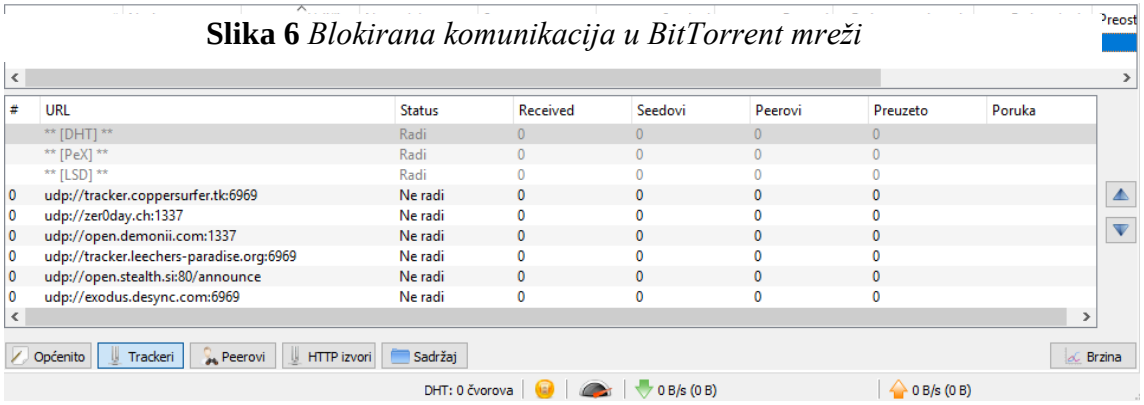
[1] Raspon mrežnih portova od 1024 do 65535 spada u neregistrirane portove pri organizaciji IANA, te stoga nisu službeno dodijeljeni niti jednom mrežnom servisu.

Naredbe koje će biti dodane u vatrozid su:

- iptables -I FORWARD -p tcp -m multiport --dports 1024:65535 -o enp0s3 -j DROP && iptables -I FORWARD -p udp -m multiport --dports 1024:65535 -o enp0s3 -j DROP
- iptables -I FORWARD -p udp --dport 80 -o enp0s3 -j DROP && iptables -I FORWARD -p tcp --dport 80 -o enp0s3 -j DROP

Ove naredbe onemogućuju komunikaciju pomoću TCP i UDP protokola, ako komunikacija ide prema enp0s3 sučelju vatrozida i ako je odlazni mrežni port između 1024 i 65535 u slučaju prve naredbe ili 80 u slučaju druge naredbe. Posljedica navedenih naredbi vidi se na slici 7. Nema komunikacije s tracker poslužiteljima niti s DHT čvorovima. Nema niti preuzimanja podataka od sudionika jer nema informacija o njima niti je moguća uspostava komunikacije između sudionika na portovima iznad 1023.

Slika 6 *Blokirana komunikacija u BitTorrent mreži*



Izvor: Autor

5. Zaključak

Postoji zanemariva mogućnost zaobilaženja blokade korištenjem mrežnih portova koji nisu obuhvaćeni vatrozidom, ali takve izolirane slučajeve moguće je rješavati po primanju možebitnih prigovora. Drugi način da korisnici zaobiđu blokadu je korištenje određenih VPN servisa, ali tada ih je gotovo nemoguće povezati s IP adresom školskoga internet priključka pa to ne predstavlja problem. Iako nije bez nedostataka, metoda blokiranja odlaznih mrežnih portova pruža zadovoljavajuću zaštitu školske mreže od preuzimanja nelegalnoga sadržaja.

Literatura

1. Iptables How To. https://help.ubuntu.com/community/IptablesHowTo (24.08.2017.).
2. Lei Xia, R.; Muppala, J. K., A Survey of BitTorrent Performance. http://www3.cs.stonybrook.edu/~cse300/A4/Xia-Muppala-BT-perf.pdf (12.08.2017.).
3. Odluka o prihvatljivom korištenju CARNet mreže. ftp://ftp.carnet.hr/pub/CARNet/docs/rules/CDA0035.pdf (13.09.2017.).
4. Schindler, S., Analysis of BitTorrent Trackers and Peers. https://www1.informatik.uni-erlangen.de/filepool/gruhn/btt.pdf (20.09.2017.).