JURNAL REKAYASA SISTEM DAN INDUSTRI
e-ISSN: 2579-9142 p-ISSN: 2356-0843
http://jrsi.sie.telkomuniversity.ac.id

ARP Cache Poisoning sebagai Teknik Alternatif untuk Membatasi Penggunaan *Bandwidth* berbasis Waktu

ARP Cache Poisoning as an Alternative Technique to Limit Bandwidth Usage based on Time

Ahmad Almaarif[1], Setiadi Yazid[2]

[1]Program Studi Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom
[2]Program Studi Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Indonesia

ARTICLE INFO

Article history:
Diterima 12-09-2018
Diperbaiki 20-10-2018
Disetujui 21-12-2018

Kata Kunci:
ARP Cache Poisoning, Bandwith, ARP, Manajemen Bandwidth

ABSTRAK

Kepadatan trafik data pada jaringan menyebabkan timbulnya kemacetan atau *congestion* pada lalu lintas data. Jika terjadi di jaringan hotspot publik, kondisi ini akan mengganggu kenyamanan pengguna. Seringkali kepadatan ini disebabkan oleh pengguna yang melakukan *download* data dalam jumlah besar. Solusi yang sering digunakan untuk mengurangi kepadatan trafik ini adalah dengan memperbesar kapasitas *bandwidth* atau menggunakan metode seperti *traffic policing* serta *queue management*. Permasalahannya, solusi ini sulit diterapkan untuk organisasi skala kecil seperti sekolah atau pemerintahan desa yang tidak memiliki sumber dana yang besar untuk teknologi ini. Penelitian ini bertujuan untuk memodifikasi perangkat lunak sumber terbuka bernama Tuxcut untuk dimanfaatkan sebagai perangkat pembatasan *bandwidth* dengan biaya murah. Pembatasan penggunaan bandwidth dilakukan dengan memanfaatkan teknik ARP Cache Poisoning yang umumnya digunakan untuk merusak. Dari hasil penelitian, didapatkan bahwa penerapan modifikasi perangkat lunak ini dapat digunakan untuk membatasi penggunaan *bandwidth* tanpa harus memutus koneksi pengguna secara total.

Keywords:
ARP Cache Poisoning, Bandwith, ARP, Bandwidth Management

ABSTRACT

Traffic overloading in computer network can cause congestion in data traffic. If it occurs on the public hotspot, this condition will disturb user's comfort. Often this traffic overloading is caused by users downloading large amounts of data. The solution that is often used to reduce traffic density is to increase bandwidth capacity or use methods such as traffic policing and queue management. The problem is that this solution is difficult to apply to small scale organizations such as schools or village governments that do not have a large source of funding for this technology. This study aims to modify open source software called Tuxcut to be used as a tool to limit bandwidth at a low cost. Limitation of bandwidth usage is done by utilizing the ARP Cache Poisoning technique which is generally used to damage. From the results of the study, it was found that the application of this software modification can be used to limit bandwidth usage without having to completely disconnect the user connection.

1. Pendahuluan

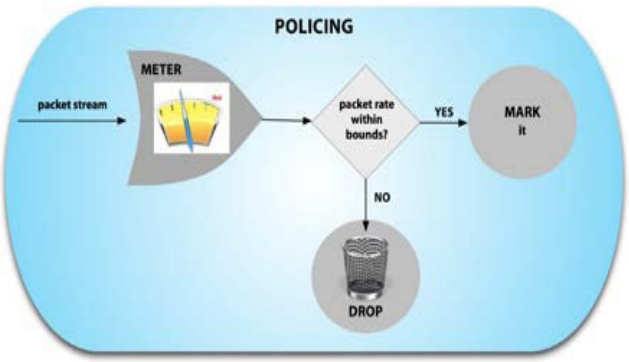
Pada 2018, penelitian yang dilakukan oleh Polling Indonesia bekerjasama dengan Asosiasi Penyelenggara Jasa Internet (APJII) mencatat ada 171 juta pengguna atau 64.8 persen dari total populasi Indonesia yang sudah terkoneksi dengan Internet [1]. Peningkatan jumlah pengguna ini berdampak pada penggunaan bandwidth yang terpakai. Dengan kata lain, semakin banyak jumlah pengguna maka semakin banyak bandwidth yang digunakan. Jika infrastruktur jaringan tidak mampu menampung jumlah pengguna yang sebanyak ini, makan akan berakibat pada terjadinya kemacetan atau *congestion* pada trafik jaringan. *Congestion* pada jaringan berdampak pada peningkatan jumlah *packet loss* sehingga waktu penyampaian paket data menjadi semakin lama. Pada pengguna internet rumahan, dampak dari *packet loss* ini mungkin tidak terlalu besar. Namun pada area internet publik seperti kafe, bandara, perpustakaan, dan area publik

*Penulis korespondensi : +6281363248150 (no telp.)
Email: ahmadalmaarif@telkomuniversity.ac.id (Almaarif, A.)

doi: https://doi.org/10.25124/jrsi.v5i02.367

lain, *congestion* ini akan sangat mengganggu. Masalah seringkali terjadi ketika ada pengguna yang melakukan *download* data yang besar sehingga mengganggu koneksi pengguna yang lain. Terkadang pengguna yang melakukan *download* ini juga menggunakan aplikasi *download* manager untuk mempercepat proses *download*.

Menambah kapasitas bandwidth memang merupakan sebuah solusi, tapi tentu saja tidak murah dan hanya bersifat sementara. Beberapa organisasi atau perusahaan besar biasanya menggunakan teknik dan perangkat tertentu untuk membuat trafik data yang melalui jaringannya stabil. Beberapa metode yang sering digunakan adalah *queue management* [2][3], *load balancing* [4][5], *traffic control, traffic policing* [6] atau *traffic shaping* [7].



Gambar 1. Ilustrasi *Traffic Policing* [8]

Metode-metode yang sering digunakan biasanya menerapkan pembatasan pada trafik yang lewat di jaringan atau menerapkan pembagian kerja untuk mengurangi beban pada jalur tertentu. Pembatasan tesebut dapat berupa pembatasan dengan menggunakan manajemen antrian seperti pada *queue management*, pembatasan berdasarkan jenis protokol seperti pada *traffic policing*, atau dengan menerapkan pembagian kerja merata seperti pada *load balancing*.

Metode-metode tersebut biasanya efektif digunakan untuk mengatasi *congestion* pada jaringan. Namun, biaya yang dikeluarkan tidak sedikit. Untuk organsisasi kecil seperti sekolah atau lingkup pemerintahan desa, biaya menjadi pertimbangan utama dalam penerapan teknologi. Untuk mengatasi permasalahan tersebut, penelitian ini mengusulkan teknologi pembatasan bandwidth dengan biaya terjangkau yang dapat digunakan secara bebas oleh publik.

2. Studi Literatur

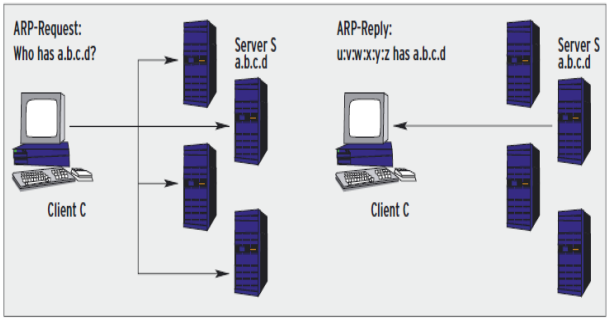
Teknik yang digunakan dalam usulan ini adalah ARP Cache Poisoning. ARP Cache Poisoning merupakan teknik yang biasanya digunakan untuk menyerang sebuah jaringan. Teknik ini memanipulasi Tabel ARP dengan cara mengirimkan paket ARP palsu ke jaringan sehingga isi tabel ARP tertimpa dengan ARP palsu yang dikirimkan oleh penyerang. Penelitian ini memanfaatkan teknik serangan ARP Cache Poisoning sehingga dapat digunakan oleh administrator jaringan sebagai teknik alternatif untuk membatasi penggunaan bandwidth oleh pengguna. Contoh tampilan Tabel ARP pada Sistem Operasi Windows dapat dilihat pada Gambar 2.

```
Interface: 192.168.67.1 --- 0x16
  Internet Address      Physical Address      Type
  192.168.67.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static

Interface: 192.168.73.1 --- 0x18
  Internet Address      Physical Address      Type
  192.168.73.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
```

Gambar 2 Tampilan ARP Tables pada Sistem Operasi Windows

ARP atau Address Resolution Protocol merupakan Protokol yang digunakan untuk memetakan alamat jaringan atau yang lebih dikenal dengan nama IP address ke alamat fisik atau MAC Address [9]. IP address atau alamat IP adalah alamat virtual yang ditetapkan pada setiap perangkat yang terhubung ke jaringan yang menggunakan IP. Alamat IP ini dapat berubah dan biasanya diatur oleh Dynamic Host Control Protocol (DHCP). Sedangkan MAC address atau alamat MAC ini pada dasarnya adalah alamat unik untuk setiap perangkat, bersifat tetap dan terdiri dari bilangan 48 bit yang direpresentasikan dengan bilangan heksadesimal. Tabel ARP merupakan pemetaan IP address ke MAC address perangkat terkait. Pemetaan ini disimpan di Tabel ARP dalam waktu tertentu sehingga disebut juga dengan istilah ARP Cache. ARP Cache ditentukan secara dinamis dengan du acara; traffic monitoring dan paket ARP Request/Reply [10]. Ketika sebuah node atau perangkat menerima paket dari node lain, secara otomatis ARP Cache akan ditulis di Tabel ARP jika pada paket data tersebut terdapat IP address dan MAC address node terkait. Metode ini disebut dengan traffic monitoring. Namun jika paket atau frame data tersebut tidak terdapat IP Address dan MAC Address terkait, maka digunakan metode ARP Request/Reply.



Gambar 3. Ilustrasi Proses ARP Request dan ARP Reply [5]

Pada ARP Request, ARP meminta alamat hardware tujuan dengan mengirimkan *request* ke semua *host*. Sebagai respon, *host* mengirimkan alamat *hardware* yang diminta melalu paket ARP Reply. Ilustrasi Proses ARP Request dan ARP Reply ini dapat dilihat pada Gambar 3.

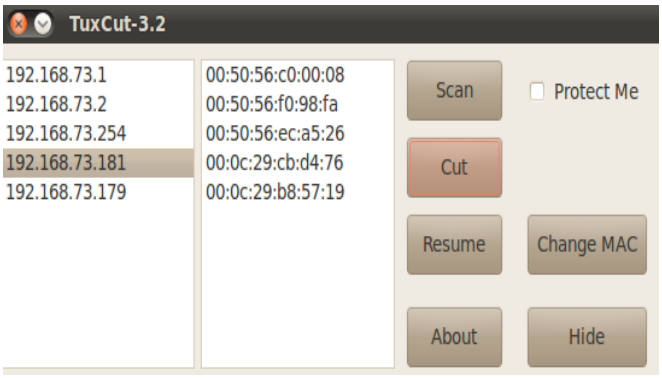
3. Metode Penelitian

Metode penelitian yang diterapkan pada penelitian ini adalah melalui implementasi dan simulasi pengujian pada *virtual machine*. Penelitian ini dilakukan dengan melakukan modifikasi pada aplikasi Tuxcut. Aplikasi Tuxcut merupakan aplikasi desktop berbasis Linux dan digunakan untuk melindungi computer pengguna dari serangan ARP Spoofing. Meskipun begitu, Tuxcut juga memiliki fitur memotong koneksi pengguna lain dan menyembunyikan identitas alamat

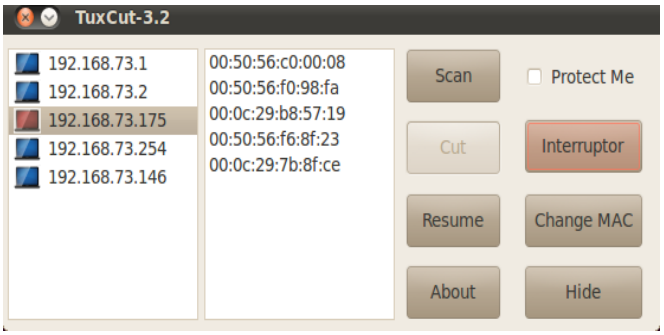
pengguna di dalam jaringan. Pada penelitian ini, fitur memutus koneksi dimodifikasi sedemikian rupa sehingga dapat digunakan untuk membatasi koneksi pengguna lain yang tidak diinginkan. Teknik ARP Cache Poisoning digunakan untuk membatasi koneksi pengguna yang pada penelitian ini kita sebut sebagai *target.* Sedangkan untuk komputer pengelola jaringan kita sebut sebagai komputer *admin.* Admin juga dapat disebut sebagai penyerang karena pada dasarnya komputer admin melakukan serangan terhadap tabel ARP Switch atau Router yang ada pada jaringan yang bertujuan untuk mengubah rute paket data yang ditujukan ke alamat target. Akibatnya target akan kehilangan paket data selama admin melakukan serangan terhadap switch di jaringan.

3.1 Skenario Implementasi

Penerapan ARP Cache Posioning sebagai teknik untuk membatasi penggunaan bandwidth dilakukan dengan memodifikasi perangkat lunak yang bernama Tuxcut. Tampilan Tuxcut dapat dilihat pada Gambar 4. Pembatasan penggunaan bandwidth dilakukan dengan memodifikasi fungsi Cut yang terdapat pada Tuxcut. Fungsi Cut pada awalnya digunakan untuk memutus koneksi komputer berdasarkan alamat IP atau alamat MAC yang dipilih. Ketika fungsi Cut dijalankan, komputer Admin mengirimkan paket ARP palsu dengan menggunakan perintah *arpspoof.* Perintah *arpspoof* ini mengirimkan paket ARP Reply secara terus menerus ke *gateway* dengan memasangkan alamat IP komputer target ke alamat MAC komputer admin. Dampaknya, *gateway* akan mengira alamat komputer target adalah alamat komputer admin sehingga paket yang ditujukan ke komputer target tidak akan sampai ke tujuan. Jika ini terjadi, maka komputer target tidak akan dapat melakukan koneksi ke Internet karena *gateway* tidak mengenali alamat komputer target sebagai alamat valid yang terdapat di Tabel ARP. Implementasi pembatasan bandwidth ini diterapkan pada fitur khusus yang dinamakan *Interruptor*. Fitur ini merupakan pengembangan dari fitur Cut yang terdapat pada Tuxcut. Jika pada fitur Cut paket ARP Reply dikirimkan secara terus menerus ke *gateway,* maka pada fitur Interruptor paket ARP Reply dikirimkan secara berkala dengan rentang waktu tertentu tanpa memutus koneksi komputer target. Tampilan aplikasi Tuxcut Modifikasi setelah diterapkan fungsi Interruptor dapat dilihat pada Gambar 5.

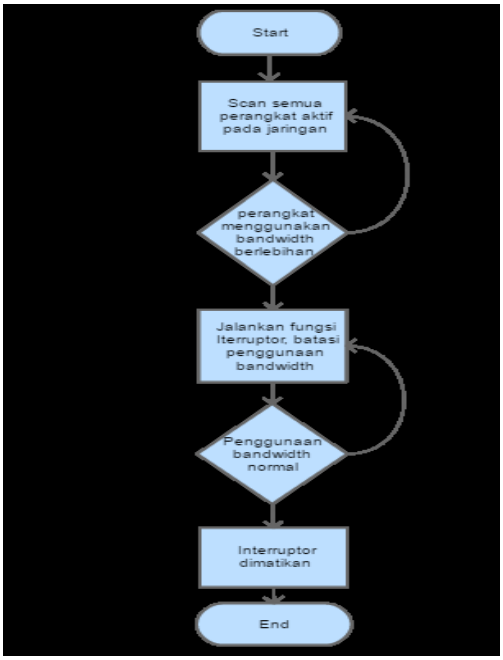


Gambar 4. Tampilan Tuxcut



Gambar 5. Tampilan Tuxcut Modifikasi

Pada Tuxcut Modifikasi, admin akan melakukan pemindaian perangkat yang terhubung ke jaringan. Dengan menggunakan perangkat network monitoring, admin memeriksa perangkat yang menggunakan bandwidth secara berlebihan. Jika ditemukan, maka admin akan menjalankan fungsi interruptor dan membatasi koneksi target. Jika penggunaan bandwidth sudah kembali normal, admin akan mematikan fungsi interruptor dan target dapat kembali terkoneksi ke internet secara normal. Alur skenario pembatasan bandwidh dengan Tuxcut Modifikasi dapat dilihat pada Gambar 6.

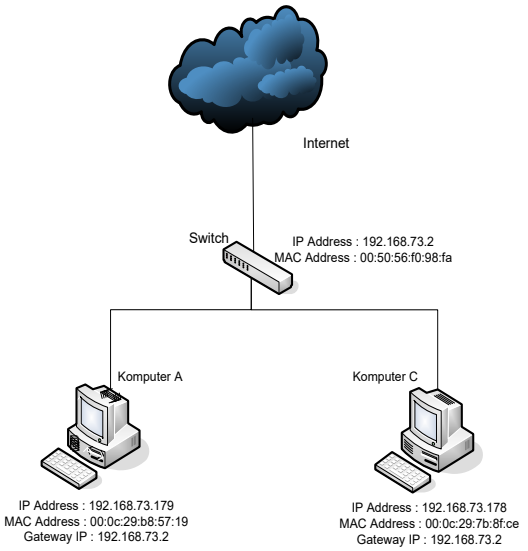


Gambar 6. Proses Pembatasan Bandwidth

3.2 Skenario Pengujian

Pengujian dilakukan dengan melakukan simulasi menggunakan tiga mesin; satu mesin sebagai admin, satu mesin sebagai target, dan satu mesin lagi bertindak sebagai gateway. Ilustrasi skenario pengujian dapat dilihat pada Gambar 7. Pengujian dilakukan dengan dua metode; Ping Test dan TCP Packet Transfer. Ping test digunakan untuk menguji konektivitas target ke jaringan, sedangkan TCP Packet Transfer digunakan untuk melihat berapa lama paket sampai ke komputer target. Tujuan dari penelitian ini adalah melihat tingkat keberhasilan Tuxcut Modifikasi dalam membatasi penggunaan bandwidth komputer target. Oleh karena itu, pada

pengujian terakhir ditambahkan satu mesin sebagai user biasa untuk melihat apakah penggunaan Tuxcut Modifikasi dapat membatasi komputer target tanpa memengaruhi koneksi komputer biasa atau normal. Pengujian terakhir ini dapat terlihat pada Tabel 1.



Gambar 7. Skenario pengujian

4. Hasil dan Pembahasan

Pengujian dilakukan dengan menggunakan Ping Test dan transfer paket TCP yang dilakukan di komputer admin dan komputer target. Hasil pengujian dapat terlihat pada Tabel 1 dan Tabel 2.

4.1.1 Ping Test

Ping Test digunakan untuk menguji ketersediaan koneksi dan menghitung *round-trip time* (RTT) pesan pada komputer target pada saat fungsi Interrupt dijalankan. Pada saat Interrupt dijalankan, fungsi ini memutus sementara koneksi target dengan cara mengirim paket ARP palsu selama interval waktu tertentu. Pengujian dilakukan dengan menggunakan dua komputer; komputer admin dan komputer target. Tujuan dari pengujian ini adalah untuk menentukan waktu interval pengiriman paket ARP yang efektif agar koneksi target tidak benar-benar terputus. Dari Tabel 1 dapat terlihat bahwa mulai dari interval 10ms dan seterusnya, *packet loss* yang dialami komputer target semakin besar dan waktu yang dibutuhkan semakin lama. Sebaliknya, untuk waktu interval yang kecil, *packet loss* yang terjadi hanya sedikit. Paket yang digunakan untuk transmisi data bervariasi. Hal ini dilakukan untuk melihat perbandingan paket loss berdasarkan jumlah paket yang ditransmisikan. Hasilnya, untuk setiap interval perbandingan persentase *packet loss* tidak terlalu berbeda satu sama lain. Dari data ini dapat disimpulkan bahwa interval efektif yang digunakan untuk pengiriman paket ARP sebaiknya lebih besar dari 10ms.

4.2 TCP Packet Transfer

Pengujian ini dilakukan dengan melakukan pengunduhan paket dari internet. Paket yang digunakan pada pengujian ini berukuran 9.8 MB. Ada tiga skenario yang diujikan:

a. Menggunakan satu mesin pada kondisi normal
b. Menggunakan dua mesin secara bersamaan; pada pengujian ini kedua mesin diuji dengan mengunduh paket secara bersamaan pada kondisi normal dan kondisi ketika salah satunya berperan sebagai target.
c. Menggunakan tiga mesin secara bersamaan; pengujian dilakukan pada kondisi normal dan kondisi ketika salah satunya berperan sebagai target.

Tabel 1 Ping Test

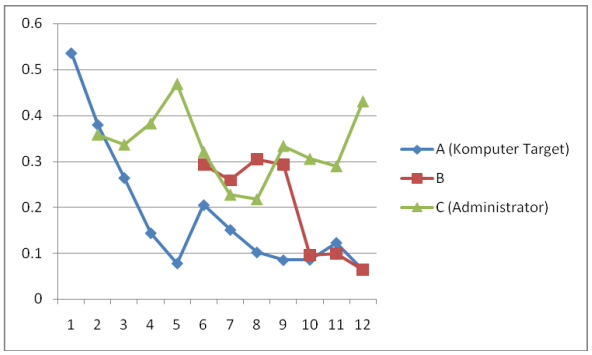
No	ARP Fake Interval (s)	Packet Transmitted (pkts)	Packet Loss (%)	RTT Avg (ms)
1	1	25	4%	221.321
		50	6%	177.858
		100	4%	254.468
2	10	21	66%	187.466
		50	68%	201.554
		100	71%	213.972
3	15	30	76%	145.261
		46	76%	195.298
		442	79%	178.103
4	20	39	82%	3675.18
		81	85%	240.086
		155	84%	192.861
5	25	75	90%	342.463
		97	87%	215.37
		175	89%	314.327
6	30	31	83%	165.883
		93	90%	162.071
		161	86%	216.829
		221	86%	1595.33
7	35	46	86%	1219.05
		110	86%	136.525
		734	90%	207.683
8	40	66	92%	323.846
		149	85%	122.801
9	50	52	92%	200.631
		118	94%	140.247
10	60	81	88%	303.02
		106	92%	116.813
		413	92%	124.203
11	120	123	95%	154.79
		295	94%	155.24

Pengujian dilakukan dengan membandingkan waktu pengunduhan ketika kondisi normal tanpa Interrupt dan ketika Interrupt dijalankan. Dari perbandingan ini didapatkan kesimpulan bahwa pada saat terjadi interrupt, proses pengunduhan data di komputer lain menjadi semakin cepat. Hasil lengkap pengujian dapat dilihat pada Tabel 2.

Tabel 2 Uji Transfer Paket

No	Eksperimen	Host	Avg. MBit/s	Waktu (s)
1	Satu Mesin Normal	A	0.536	155.494
2	Dua Mesin Normal	A	0.38	212.371
		C	0.359	198.413
3	Dua Mesin dengan ARP Spoofing (interval 10 s)	A (Target)	0.264	269.776
		C (Admin)	0.337	200.303
4	Dua Mesin dengan ARP Spoofing (interval 20 s)	A (Target)	0.144	333.813
		C (Admin)	0.383	171.295
5	Dua Mesin dengan ARP Spoofing (interval 30 s)	A (Target)	0.078	359.296
		C (Admin)	0.469	150.967
6	Tiga Mesin Normal	A	0.205	242.444
		B	0.293	270.750
		C	0.321	231.962
7	Tiga Mesin dengan ARP Spoofing (interval 10 s)	A (Target)	0.151	337.747
		B (Normal)	0.259	250.615
		C (Admin)	0.228	231.070
8	Tiga Mesin dengan ARP Spoofing (interval 20 s)	A (Target)	0.102	490.803
		B (Normal)	0.305	197.390
		C (Admin)	0.218	198.027
9	Tiga Mesin dengan ARP Spoofing (interval 30 s)	A (Target)	0.085	453.277
		B (Normal)	0.293	162.405
		C (Admin)	0.334	175.849
10	Tiga Mesin dengan ARP Spoofing (interval 20 s)	A (Target)	0.086	542.415
		B (Target)	0.096	481.135
		C (Admin)	0.306	179.379
11	Tiga Mesin dengan ARP Spoofing (interval 20 s)	A (Target)	0.123	418.000
		B (Target)	0.099	430.619
		C (Admin)	0.290	174.108
12	Tiga Mesin dengan ARP Spoofing (interval 30 s)	A (Target)	0.064	684.801
		B (Target)	0.064	750.644
		C (Admin)	0.431	153.612

Dari Tabel 2 terlihat bahwa pengujian pada interval waktu 10 detik tidak terlalu memberikan dampak bagi waktu pengunduhan, baik bagi komputer target maupun komputer admin dan komputer normal. Perbedaan waktu pengunduhan baru terlihat signifikan pada saat nilai interrupt 20 detik dan 30 detik. Pada interval ini, terlihat ketika interrupt dilakukan pada komputer target, waktu pengunduhan untuk komputer normal berkurang secara signifikan. Sedangkan untuk komputer target, waktu pengunduhan meningkat dengan perbedaan hingga 500 milidetik.



Gambar 8 *Average Transfer Rate* Setiap Percobaan

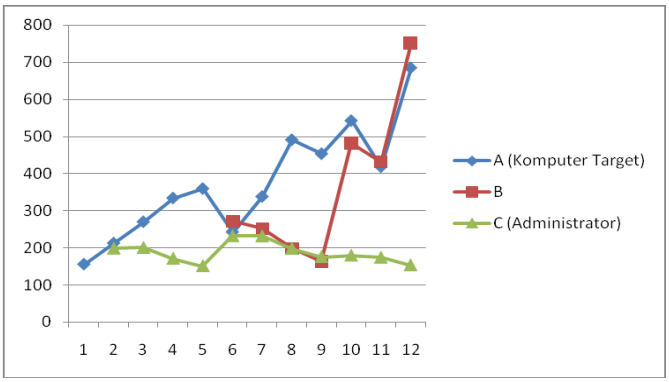
Kinerja Tuxcut Modifikasi dapat diamati pada Gambar 8 dengan mengukur waktu transfer rata-rata atau Average Transfer Rate untuk setiap jenis pengujian. Pada Gambar 8 terlihat rentang antara 1 hingga 12 yang merupakan nomor eksperimen pengujian pada Tabel 2. Gambar tersebut merupakan hasil beberapa jenis pengujian; percobaan dengan kondisi normal pada satu komputer (nomor 1), dua komputer (nomor 2) dan tiga komputer (nomor 6). Pada kondisi nomor 3, 4, dan 5 adalah kondisi dua komputer dengan Interrupt pada interval ke 10, 20 dan 30 detik. Nomor 7, 8 dan 9 pada sumbu horizontal menunjukkan skenario dengan satu komputer sebagai Admin (C), satu komputer dengan kondisi normal tanpa Interrupt (B) dan satu Komputer Target (A) dengan interval 10, 20, dan 30 detik. Serta kondisi nomor 10, 11 dan 12 menunjukkan skenario dengan satu Admin dan dua Komputer Target dengan interval interrupt 20, 20 dan 30.

Dari grafik dapat kita lihat pada kondisi normal (1, 2 dan 6) transfer rate antara ketiga komputer tidak terlalu jauh berbeda. Transfer rate tertinggi didapatkan ketika hanya ada satu komputer yang melakukan proses *download*. Sedangkan kondisi tertinggi pada Admin yaitu pada nomor 5, pada saat interrupt 30 detik dengan dua komputer. Transfer rate yang tinggi juga didapatkan ketika tiga komputer dengan satu komputer sebagai Admin melakukan *download* secara bersamaan dengan interrupt interval 30 detik.

Sedangkan jika ditinjau dari waktu transfer (detik) dapat dilihat pada Gambar 9. Dari grafik dapat terlihat bahwa ketika kondisi normal (1,2, dan 6) dan skenario satu komputer sebagai Admin, satu normal dan satu Komputer Target (7,8, dan 9), proses *download* dapat diseleseikan dalam waktu yang hampir bersamaan. Sedangkan waktu transfer yang lama dari Komputer Target didapatkan ketika dua Komputer Target dan satu Administrator melakukan proses *download* secara bersamaan dengan interval interrupt 30 detik.

Dari grafik juga terlihat bahwa kondisi ideal terdapat pada skenario 9, yaitu ketika terdapat tiga komputer dengan interval interrupt 30 detik. Pada skenario 9, proses pengunduhan di komputer target (A) membutuhkan waktu sekitar 453 detik, sedangkan pada komputer admin (C) dan komputer kondisi normal (B) waktu yang dibutuhkan berkisar antara 160 – 170 detik. Jika dibandingkan dengan kondisi normal tanpa Interrupt pada skenario 6, yaitu ketika proses pengunduhan membutuhkan waktu antara 230 detik hingga 270 detik, dapat terlihat bahwa Tuxcut Modifikasi berperan dalam membatasi bandwidth yang dipakai komputer target. Dari hasil uji ini

dapat terlihat bahwa setelah penerapan Tuxcut Modifikasi terjadi pengurangan waktu pengunduhan hingga 60 detik.



Gambar 9. Waktu Transfer Setiap Percobaan

5. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa teknik ARP Cache Poisoning dapat digunakan untuk membatasi penggunaan bandwidth. Pada pengujian dapat terlihat bahwa interval waktu interrupt berpengaruh pada efektifitas hasil pembatasan bandwidth. Pengiriman paket ARP palsu setiap interval waktu tertentu dapat membatasi penggunaan bandwidth komputer target tanpa memutus koneksi target secara total. Dampak lain dari pembatasan ini adalah peningkatan kecepatan transfer data bagi pengguna biasa karena penggunaan bandwidth komputer target dapat dibatasi. Teknik ini merupakan solusi alternatif berbiaya rendah sehingga tidak diharapkan sebagai solusi permanen. Penambahan kapasitas bandwidth tetap merupakan solusi yang paling jitu untuk mengurangi kemacetan pada trafik jaringan.

Referensi

[1] https://www.thejakartapost.com/life/2019/05/18/indonesia-has-171-million-internet-users-study.html, diakses Juni 2019.

[2] Xu, Q., Sun, J., New Active Queue Management Scheme Based on Statistical Analysis, Proceedings of the 10th World Congress on Intelligent Control and Automation, Beijing, China, 2012, pp. 2562-2565.

[3] Nakashima, T., Queue Management for the Heavy-tailed Traffics, 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, 2010, pp 222-228.

[4] Patni, Jagdish C., dan Aswal, Mahendra S.,Distributed Load Balancing Model for Grid Computing Environment, 2015 International Conference on Next Generation Computing Technologies, Dehradun, India, September 2015, pp. 123-126.

[5] Dasoriya, R., Kotadiya,P., Arya, G., dan Nayak, P.,Dynamic Load Balancing in Cloud: A Data-centric Approach, 2017 International Conference on Networks & Advances in Computational Technologies, India, 2017, pp. 162-166

[6] Traffic Policing in Distributed Infocommunication Systems with Service Oriented Architecture

[7] Lekchaeron, S. dan Fung, C., An Adaptive Fuzzy Control Traffic Shaping Scheme over Wireless Networks, Proceedings of Asia-Pacific Conference on Communications, 2007, pp. 177-182

[8] BTI Systems White Paper, Understanding Traffic Policing, http://www.btisystems.com/Documents/White%20Papers/Understanding-Traffic-Policing-WP0102.pdf., diakses Desember 2018.

[9] Bhirud, S.G., Katkar, V., Light Weight Approach for IP-ARP Spoofing Detection and Prevention, 2011 Second Asian Himalayas International Conference on Internet, Kathmandu, Nepal, 2011.

[10] Meghana, J., Subashri, T., Vimal, K., A Survey on ARP Cache Poisoning and Techniques for Detection and Mitigation, 2017 International Conference on Signal Processing, Communications and Networking, Chennai, India, Maret 2017.