

Analisis Performansi BGP *Resource Public Key Infrastructure* Studi Kasus PT. Time Excelindo

Nanda Iryani[#], Jafaruddin Gusti Amri Ginting, Dyas Dendi Andika

Jurusan Teknik Telekomunikasi, Fakultas Teknik Telekomunikasi dan Elektro, Institut Teknologi Telkom Purwokerto
Jl. DI Panjaitan No. 128, Karang Reja, Purwokerto Kidul, Kec. Purwokerto Sel., Jawa Tengah, Indonesia

[#]nanda@ittelkom-pwt.ac.id

Abstrak

Routing Border Gateway Protocol (BGP) yang berfungsi sebagai *backbone* jaringan internet secara bawaan tidak memiliki mekanisme keamanan yang kuat. Sering terjadi kasus dimana *routing* BGP yang berjalan di internet mengalami pembajakan pada rute jaringannya atau kesalahan konfigurasi baik secara sengaja maupun tidak sengaja terhadap informasi rute BGP yang mengakibatkan jaringan internet mengalami kegagalan atau tidak bisa diakses. Implementasi BGP dengan *Resource Public Key Infrastructure (RPKI)* akan membuat suatu jaringan melakukan *filtering* terhadap rute-rute yang ada sehingga keberadaannya bisa membuat jaringan internet yang memanfaatkan BGP diarahkan ke rute-rute yang valid saja dan menghindari pembajakan informasi rute yang tidak valid. Penelitian ini berupaya mengukur performansi terhadap BGP RPKI di PT Time Excelindo. Implementasi BGP RPKI untuk meningkatkan pemakaian CPU dan *memory* perangkat sebesar 3,6% dan 0,75% serta mengurangi daya *input router* dalam menerima informasi *prefix* masuk sebesar 1,15%. Selain itu, di sisi kualitas jaringan setelah menerapkan BGP RPKI menghasilkan nilai *download* dan *upload* yang turun sebesar 0,11 Mbps dan 0,02 Mbps ditambah dengan kenaikan nilai latensi selama 0,13 ms.

Kata kunci: BGP, internet, *network security*, BGP, RPKI

Abstract

Routing Border Gateway Protocol (BGP) which functions as the backbone of the internet network by default does not have a strong security mechanism. There are often cases where BGP routing running on the internet experiences hijacking of its network route or misconfiguration either intentionally or unintentionally on BGP route information which causes the internet network to fail or be inaccessible. The implementation of BGP with Resource Public Key Infrastructure (RPKI) will allow a network to filter existing routes so that its existence can make internet networks that use BGP directed to only valid routes and avoid piracy of invalid route information. This study seeks to measure the performance of the BGP RPKI at PT Time Excelindo. Implementation of BGP RPKI to increase CPU and device memory usage by 3.6% and 0.75% and reduce router input power in receiving incoming prefix information by 1.15%. In addition, in terms of network quality, after implementing BGP RPKI, the download and upload values decreased by 0.11 Mbps and 0.02 Mbps plus an increase in the latency value of 0.13 ms.

Keywords: BGP, internet, *network security*, BGP, RPKI

I. PENDAHULUAN

BGP berperan besar dalam menetapkan rute di dalam jaringan internet skala global. Namun, BGP tidak memiliki mekanisme untuk melakukan pengecekan apakah setiap rute yang masuk dalam perutean tersebut berasal dari sumber yang sah atau tidak. Keberadaan sebuah *Autonomous System (AS)* dalam jaringan dapat melakukan pembajakan terhadap informasi tujuan jaringan ke alamat yang membahayakan. Pembajakan AS tersebut

disebabkan karena pada dasarnya jaringan internet yang berdiri di atas protokol BGP yang terdiri dari 700.000 *prefix* IPv4 yang diatur oleh 5 *Regional Internet Registries*. Banyaknya informasi *prefix* tersebut menyebabkan sulitnya mengetahui pemilik dari IP *address* yang akhirnya dimanfaatkan oleh penyusup untuk melakukan pembajakan IP *address* atau *prefix* di protokol BGP. Contoh pembajakan rute tersebut dialami oleh perusahaan *Internet Service Provider (ISP)* di Pakistan pada tahun 2008 dimana kasus yang ada adalah terjadi proses

pembajakan BGP yang berusaha memblokir Youtube yang akibatnya hampir tidak bisa diakses di seluruh dunia. Kasus pembajakan serupa juga terjadi ditahun 2017 dan 2018 dimana terjadi pembajakan alamat *prefix* Visa dan Mastercard yang menyebabkan perbankan terganggu dan pembajakan untuk pencurian mata uang Crypto [1].

Sebuah metode mengamankan proses komunikasi data di lapisan internet bernama *Resource Public Key Infrastructure* (RPKI). RPKI merupakan suatu cara mengamankan jaringan internet yang didalamnya menggunakan *routing protocol* BGP dengan mengelompokkan *routing table* jaringan dengan suatu administrasi penomoran dalam jaringan internet atau biasanya yang dikenal dengan AS origin yang sah dan valid dimana sudah melewati proses sertifikasi. Metode RPKI akan memfilter alamat *network* dalam jaringan internet atau biasa dikenal sebagai *prefix* sesuai dengan pemiliknya apakah sah dan tervalidasi atau tidak sehingga bisa memastikan bahwa *route* jaringan yang ditambahkan ke BGP hanya dari AS yang diperbolehkan.

Penelitian [2] berupaya untuk meninjau terkait *deployment* RPKI dalam beberapa tahun terakhir dan juga meninjau dampak serta manfaat yang nyata dari RPKI. Peneliti mengkaji registrasi *prefix* dalam RPKI yang bisa meminimalisir adanya konflik ataupun rute yang invalid di dalam tabel *routing* global. Penelitian lain [3] sendiri sudah menyatakan apabila terdapat peningkatan dalam pendaftaran informasi *prefix* dan AS dalam RPKI dimana dari data yang dipaparkan dalam penelitian tersebut menunjukkan jumlah total *prefix* yang ada meningkat dari 19,2% menjadi 30,6% dari tahun 2017 ke 2019. Hal tersebut tentu menyebabkan jumlah *prefix* yang tidak valid yang disebabkan oleh kesalahan konfigurasi kedepannya akan jauh lebih kecil apabila sudah mengimplementasikan RPKI.

Peneliti [4] memaparkan mengenai evaluasi *origin validation* yaitu salah satu aspek di dalam sistem BGP RPKI yang menangani kesalahan memasukan informasi *prefix* jaringan dan AS-nya. Penelitian tersebut berupaya mengevaluasi efektifitas *origin validation* terhadap *mis-origination* atau akibat salah memasukan informasi *prefix* dan AS yang tepat. Peneliti tersebut menguji saat terjadi kesalahan secara acak dan berdasarkan kejadian yang nyata dengan hasil yang didapatkan penggunaan *origin validation* untuk memvalidasi informasi *prefix* dan AS mengurangi adanya dampak dari *mis-origination* terutama saat proses penerapan *origin validation* yang memiliki sejumlah link koneksi yang besar memiliki efektifitas yang kuat dalam mengurangi *mis-origination*.

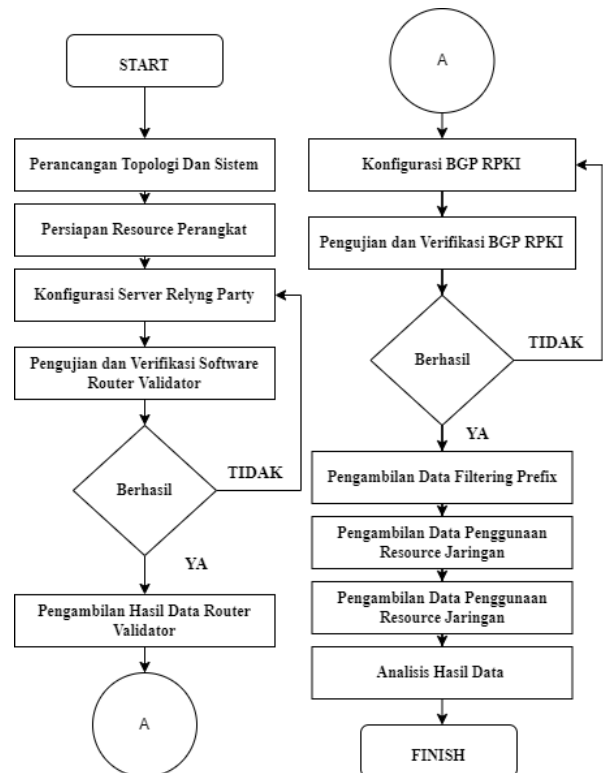
Penelitian ini berupaya mengimplemenetasikan secara langsung jaringan BGP berbasis RPKI pada perusahaan penyedia jasa layananan internet PT. Time Excelindo. Hasil implementasi dalam penelitian ini akan dikaji dari segi performansi serta segi *resource* jaringan yang dibutuhkan serta kualitas jaringan yang berjalan pada jaringan BGP RPKI. Kemudian akan dibandingkan hasil yang didapatkan pada jaringan sebelum menerapkan RPKI apakah terdapat perbedaan yang cukup jauh dan signifikan diantara keduanya.

II. METODE PENELITIAN

Penelitian ini menerapkan konsep penelitian studi kasus dengan metode penelitian yang digunakan yaitu secara langsung akan melakukan analisis terhadap implementasi dari sistem BGP RPKI di atas perangkat berbasis *open source* BIRD di PT. Time Excelindo. Analisis yang dilakukan akan berfokus terhadap hasil pengukuran performansi yang dijalankan pada jaringan sebelum dan sesudah menerapkan BGP RPKI.

A. Alur Penelitian

Gambar 1 merupakan alur kerja dari penelitian yang menggambarkan langkah-langkah untuk mengimplementasikan BGP RPKI menggunakan *open source router* di PT. Time Excelindo.



Gambar 1. Alur pengerjaan BGP RPKI

Alur kerja dimulai dengan melakukan perancangan terhadap topologi dan sistem dari jaringan BGP RPKI yang akan diimplementasikan yang tentunya perancangan tersebut harus menyesuaikan dengan topologi jaringan PT. Time Excelindo yang sudah ada. Proses setelah topologi sudah terancang terdiri dari mempersiapkan perangkat *server* yang digunakan sebagai *relying party*, yang berisi *software router validator* untuk melakukan validasi terhadap IP atau *prefix*, dan perangkat *router* yang akan menjalankan RPKI, serta bertindak sebagai *client* di dalam jaringan BGP RPKI yang nantinya akan dibentuk yang kemudian dilanjut ke tahap konfigurasi perangkat. Konfigurasi dimulai dengan melakukan konfigurasi perangkat yang akan dijadikan *relying party*. Perangkat tersebut akan diuji serta dicek terlebih dahulu apakah berjalan sesuai atau tidak sebelum dilanjut proses pengambilan data yang ada pada perangkat *relying party* tersebut.

Data yang sudah diambil perangkat akan di masukan ke dalam *router* untuk menjalankan BGP RPKI. Proses berikutnya adalah melakukan konfigurasi terhadap *router* yang menjalankan BGP RPKI baik mencakup dari sisi *routing*, RPKI, sampai konfigurasi dasar bagi *router* lain yang akan bertindak sebagai *client* di dalam jaringan. Setelah semua konfigurasi beserta pengujianya telah berhasil tahap berikutnya adalah mengkollektifkan hasil data dari hasil RPKI yang sudah berjalan, kemudian dilanjut di tahap akhir yaitu penulisan ke dalam laporan yang ada.

B. Jaringan Komputer

Jaringan komputer merupakan interkoneksi yang terjadi antara dua perangkat komputer atau lebih yang umumnya digunakan saling berkomunikasi atau bertukar data. Jaringan komputer di dalamnya memiliki sebuah titik ujung atau yang biasa dikenal dengan *end point*. *End point* dalam jaringan dikenal dengan IP *address* atau alamat *Media Access Control (MAC) address*. Jaringan komputer berdasarkan sifatnya terdiri dari jaringan pribadi dan jaringan *public*. Jaringan pribadi merupakan jaringan yang memerlukan akses khusus atau hak ases tersendiri agar bisa mengakses serta menggunakan layanan jaringan tersebut, sedangkan jaringan *public* merupakan jaringan yang tidak memerlukan akses khusus agar bisa mengakses dan menggunakannya. Internet merupakan salah satu contoh dari jaringan *public* dimana setiap orang bisa saling terhubung dan saling bertukar data tanpa perlu hak akses atau izin tersendiri selama pemakaiannya [5].

C. Border Gateway Protocol (BGP)

BGP adalah satu dari jenis *routing protocol* yang bertujuan untuk menghubungkan serta memilih jalur *inter domain* dengan didasarkan dengan sistem *path vector protocol*. Fungsi utama BGP yaitu mempertukarkan *network reachability information* antara BGP *router* dengan *router* BGP lainnya. AS merupakan suatu *set routing* dalam domain yang dikelola oleh satu otoritas sehingga pengaruhnya dapat langsung diketahui oleh *router* maupun *peer – router*. Dengan adanya informasi ini, dapat dibentuk grafik dari AS *path* yang saling terkoneksi sehingga dapat menghindari terjadinya *routing loop*. Fungsi utama BGP adalah untuk bertukar informasi aksesibilitas jaringan antara *router* BGP dan *router* BGP lainnya melalui sebuah identitas dari suatu jaringan yang disebut AS. AS adalah seperangkat *route* dalam domain yang dikelola oleh otoritas sedemikian rupa sehingga pengaruhnya dapat diketahui secara langsung oleh *router* dan pasangan lawannya. Informasi rute tersebut akan membuat suatu grafik jalur AS yang terhubung dapat dibentuk untuk menghindari terjadinya *loop* perutean [6].

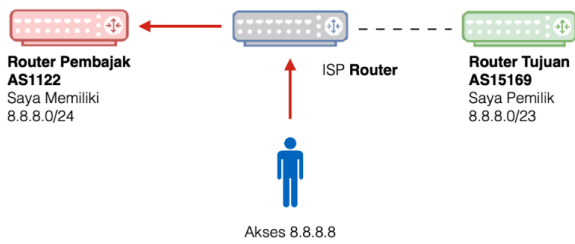
D. Internet Routing Registry (IRR)

IRR adalah suatu layanan yang merupakan bagian dari *Indonesian Network Information Center (IDNIC)* yang berisi sebuah *database* untuk digunakan sebagai publikasi informasi tentang *routing* sumber daya nomor internet. Informasi *database* tersebut digunakan untuk merute validasi, pengujian dan pemfilteran. Kegunaan IRR selain untuk mempublikasikan niat perutean dari jaringan yang dikelola juga berguna untuk membangun, memelihara filter perutean, sampai sebagai layanan informasi dan diagnosis untuk manajemen jaringan yang umum.

IRR hanya akan digunakan sebagai pengelola *filter rule* dalam pengoperasiannya memerlukan penggunaan dari perangkat lunak seperti *irrtoolset* atau *rtconfig*. Perangkat lunak tersebut difungsikan untuk mengekstrak semua rute yang diketahui yang kemudian dari informasi tersebut tinggal menentukan kebijakan apa saja yang diperlukan seperti pemilihan preferensi terhadap koneksi dari AS lain. Keberadaan IRR juga bisa dimanfaatkan untuk mengelola pelanggan serta koneksi dengan AS lain dengan menanamkan kebijakan perutean yang rumit [7].

E. Resource Public Key Infrastructure (RPKI)

RPKI merupakan metode kriptografi yang memastikan rute jaringan (*prefix*) dimana akan mengelompokan informasi tabel *routing* dalam BGP dengan *origin* AS yang *valid*. RPKI dirancang



Gambar 2. Ilustrasi pembajakan informasi *prefix* [9]

untuk mencegah adanya pembajakan rute antar AS. Pembajakan rute sangat mungkin terjadi dikarenakan infrastruktur internet yang berjalan sekarang terdiri dari 700.000 *prefix* yang diatur oleh 5 *region internet registries*. Jumlah *prefix* yang sangat banyak tersebut berakibat pada sulitnya mengetahui pemilik dari IP *address* yang akhirnya dimanfaatkan oleh para *cracker* untuk melakukan pembajakan IP *address* didalam protokol BGP [8]-[10].

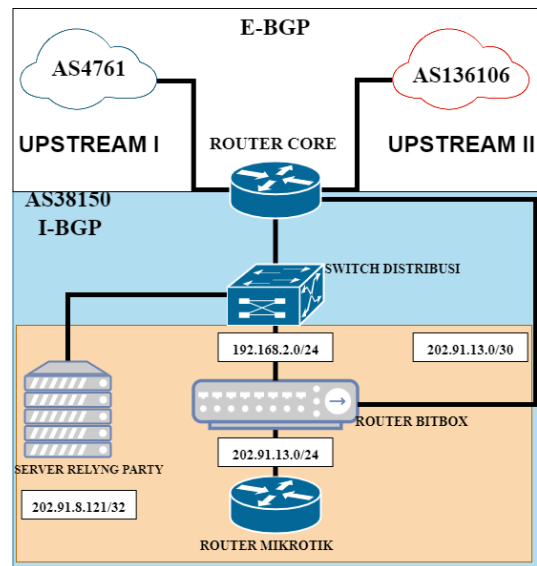
Gambar 2 merupakan ilustrasi dimana sebuah ISP *router* mengalami pembajakan (*BGP Hijacking*) dimana informasi rute yang seharusnya mengarah ke 8.8.8.0/23 diubah ke arah *router* pembajak 8.8.8.0/24. RPKI menghadirkan solusi untuk mengatasi hal semacam tersebut. Nantinya setiap IP *address* atau *prefix* yang akan menerapkan RPKI akan disertifikasi secara khusus. Sertifikasi tersebut berperan agar memastikan bahwa hanya pemilik IP *address* tersebut yang dapat menggunakannya di internet [8]-[10].

F. Routinator 3000

Routinator 3000 atau biasa disebut sebagai *routinator* merupakan perangkat lunak RPKI *relying party* berbasis *open source* yang ditulis oleh NLnet Labs dalam bahasa pemrograman Rust. *Routinator* dirancang agar bisa digunakan secara aman dan juga bisa dipasang dan berjalan secara minimalis tanpa menggunakan kebutuhan perangkat keras dengan spesifikasi tinggi di hampir semua sistem operasi. *Routinator* terhubung ke *Trust Anchors* dari lima *Regional Internet Registries (RIR)* — *APNIC, AFRINIC, ARIN, LACNIC, dan RIPE NCC* yang kemudian akan mengunduh semua sertifikat dan *ROA* di berbagai repositori, melakukan verifikasi tanda tangan, dan membuat hasilnya tersedia agar bisa digunakan didalam *router* yang nantinya akan menerapkan RPKI [11].

G. Bird Internet Routing Daemon (BIRD)

BIRD yang merupakan perangkat berbasis *open source* menggunakan sistem Linux sebagai *software router*-nya. Kernel yang ada akan berperan sebagai *forwarding plane* dengan fungsinya meneruskan trafik yang masuk. Di sisi lain BIRD akan berperan



Gambar 3. Topologi jaringan PT. Time Excelindo

sebagai *control plane* yang bertugas berkomunikasi dengan *router* lain di dalam jaringan, menemukan topologi jaringan, dan melakukan kalkulasi terhadap *routing table*. BIRD terdiri dari *daemon* yang digunakan untuk melakukan konfigurasi terhadap jaringan dan *birdc* yang fungsinya untuk memasukan berbagai perintah-perintah CLI dari *client* dimana digunakan untuk berbagai hal seperti melihat tabel perutean, informasi topologi, konfigurasi *routing*, dan sebagainya. BIRD sejauh ini sudah bisa mendukung berbagai protokol *instances* dan menjalankan banyak *routing table* sekaligus. Berbeda dengan *routing* berbasis *open source* lainnya seperti FRRouting yang mekanisme menjalankan berbagai protokol yang dijalankan secara terpisah, BIRD mengadopsi mekanisme dimana semua protokol dijalankan dan ditangani dengan satu proses [12].

III. HASIL DAN PEMBAHASAN

A. Topologi Jaringan

BGP RPKI diimplementasikan secara langsung ke dalam jaringan yang berisi *prefix* baru dan tidak mengikuti *prefix* yang disediakan. Gambar 3 merupakan topologi jaringan yang ada di PT. Time Excelindo. Topologi terdiri dari 3 bagian yang masing-masing bagian memiliki peran serta hak administrasi. Bagian daerah putih merupakan topologi dimana *router core* PT. Time Excelindo melakukan *peering* dengan *upstream* agar bisa mendapat akses ke internet. PT. Time Excelindo sejauh ini memiliki dua buah *upstream* yang terhubung secara langsung. Bagian berikutnya merupakan daerah biru yang merupakan jaringan internal dari PT. Time Excelindo yang dihubungkan

Tabel 1. Alokasi IP address

No.	Perangkat	Interface	IP address
1	Server Relying Party	ens160	202.91.8.121/32
2	Router Bitbox	enp2s0	192.168.2.251/24
		enp3s0	202.91.13.1/24
		enps90	180.214.249.10/30
3	Router Mikrotik	Eth0	202.91.13.2/24

dengan menggunakan *switch* distribusi yang tersambung langsung tentunya dengan *router core*. Jaringan tersebut merupakan jaringan dimana posisi *customer* PT. Time Excelindo dan jaringan di dalam kantor berada dimana jika dispesifikasikan lagi di dalam jaringan kantor tersebut terdapat bagian berwarna *orange* yang merupakan jaringan tempat mengimplementasikan BGP RPKI dan juga jaringan yang diperbolehkan peneliti untuk dikonfigurasi dan diimplementasikan berbagai konfigurasi yang berhubungan dengan BGP RPKI, dengan cakupan perangkatnya terdiri dari *server relying party*, *router bitbox*, dan *router mikrotik*. Jaringan yang akan diimplementasikan BGP RPKI akan memiliki *interface* yang langsung terkoneksi *secara point to point* dengan *router core*. Koneksi tersebut memiliki alokasi IP address menggunakan IP *public* dan juga ada yang terkoneksi melalui *switch* distribusi menggunakan IP *private* untuk keperluan *remote management* akses dengan detail IP address yang ada tercantum dalam Tabel 1. Sementara itu terkait perangkat *server relying party* akan dikoneksikan menggunakan IP *public* sehingga akses yang ada tidak *point to point* secara langsung menuju *router bitbox*.

B. Pemakaian Resource Jaringan BGP RPKI

Pengambilan data *resource* ditujukan untuk mengetahui bagaimana *resource* yang diperlukan pada jaringan BGP RPKI baik itu dari segi pemakaian alokasi perangkat keras yang dibutuhkan maupun alokasi terhadap waktu konvergensi jaringan baik sebelum ataupun sesudah menerapkan BGP RPKI. Nilai pemakaian CPU dan memori yang didapatkan pada *router bitbox* akan dipantau secara terus menerus sampai pemakaian *resource* pada perangkat stabil.

Pengambilan skenario tersebut karena berdasarkan sampel pengamatan yang dilakukan didapatkan apabila pemakaian *resource* CPU dan memori cenderung tidak stabil dan akan selalu mengalami kenaikan nilai secara terus menerus untuk pemakaian memori, sedangkan pemakaian CPU pada saat proses mendapat *prefix* akan naik turun secara konstan sebelum akhirnya nilai

Tabel 2. Hasil pengukuran resource jaringan

Kondisi jaringan	Jumlah prefix	CPU (%)	Memori (MB)	Waktu konvergensi (s)
Pra-RPKI	897.846	50,81	518,20	255,88
RPKI	897.033	54,41	522,13	258,83

resource CPU tersebut akan stabil ketika *prefix* sudah berada diangka 890 ribuan yang artinya jaringan internet sudah konvergensi. Nilai tersebut mengindikasikan apabila *resource* yang dipakai kembali turun seperti pemakaian sebelum *router* mengimpor informasi *prefix*.

Pengukuran akan mengambil nilai tertinggi dari pemakaian CPU dan memori pada saat nilai belum stabil. Untuk nilai *prefix* sendiri akan mengikuti sejauh mana pemakai CPU dan memori kembali stabil, sedangkan nilai waktu konvergensi mengambil dari waktu ketika *router* belum mendapat *prefix* sampai ketika mendapat sejumlah *prefix* dengan kondisi alokasi pemakaian CPU dan memori kembali stabil.

Tabel 2 menunjukkan hasil pengukuran berbagai *resource* yang didapatkan pada jaringan sebelum dan sesudah menerapkan RPKI. Hasil pengukuran menunjukan bahwa nilai tertinggi konsumsi CPU yang dihasilkan pada jaringan sebelum menerapkan RPKI untuk mendapatkan sebuah *prefix* sampai dalam kondisi stabil berada di angka 50,81% dengan total memori yang diambil *router* adalah 518,20 atau sekitar 3,32% dari total memori yang dimiliki sistem yaitu 16 GB. Jaringan yang telah menerapkan RPKI mengalami kenaikan pada kedua nilai tersebut dimana nilai CPU yang dihasilkan naik ke angka 54,41% dan penggunaan memori menghasilkan nilai 522,13 MB.

Nilai dari pemakaian *resource* dari jaringan sebelum menerapkan RPKI selalu berubah-ubah sebelum *router* mendapatkan *prefix* sebanyak 897.846 buah dimana untuk mendapatkan *prefix* sebanyak itu jaringan yang sebelum menerapkan RPKI memerlukan waktu selama 255,88 detik. Jadi dalam hitungan setiap detiknya *router* selalu mendapatkan informasi *prefix* baru sejumlah 3509 rute *prefix*. Di sisi lain nilai yang tidak berbeda jauh didapatkan pada jaringan yang telah menerapkan RPKI dengan nilai yang didapatkan sama-sama di angka 890 ribuan lebih tepatnya 897.033 yang didapatkan dalam rentang waktu 258,33 detik. Nilai tersebut menunjukan apabila jumlah *prefix* yang didapatkan oleh *router* yang telah menerapkan jaringan RPKI setiap detiknya berjumlah 3466 rute *prefix*. Berdasarkan hasil pengukuran yang ada terbukti apabila *filtering* RPKI pada suatu jaringan akan mengurangi tingkat performa perangkat keras

yang ada dan juga daya *input prefix* suatu *router* dalam menerima *prefix* yang masuk dari internet. Hal tersebut wajar mengingat *router* memiliki beban kerja tambahan berupa memeriksa dan memilah lagi *prefix* yang masuk.

Selama proses pengamatan *resource* yang digunakan, titik tertinggi dari memori didapatkan saat *prefix* sudah mencapai 890 ribuan, sedangkan titik tertinggi CPU saat *router* sudah mencapai 3/4 dari 890 ribuan *prefix*. Saat *router* sudah mendapatkan *prefix* sebesar 890 ribu *prefix* didapatkan apabila baik dari kondisi perangkat keras ataupun jaringan dari *router* sudah sangat stabil. Berdasarkan pengamatan yang dilakukan peneliti didapatkan apabila ketika jumlah rute mencapai 890 ribuan *prefix* maka *router* sudah mampu terkoneksi ke internet secara optimal atau dalam jumlah *prefix* yang ada di internet kurang lebih terdiri dari 890 ribuan *prefix* atau informasi rute.

C. Performansi Jaringan BGP RPKI

Pengujian serta pengambilan data yang dilakukan menggunakan uji pengetesan menggunakan Web Speedtest. Pengukuran dilakukan untuk meninjau bagaimana *filtering* rute yang ada di dalam *router bitbox* mempengaruhi jaringan yang ada di bawahnya yaitu perangkat mikrotik. Pengambilan data dilakukan dengan melakukan pengujian sebanyak 30 kali untuk memastikan data akurat dan meminimalisir kesalahan atau ketidaksesuaian data. Hasil pengambilan data tersebut terlampir dalam Tabel 3.

Kualitas jaringan internal mikrotik yang belum menerapkan RPKI didapatkan apabila nilai rata-rata *download* berada di angka 94,71 Mbps dengan nilai terkecil 94,38 Mbps sedangkan terbesarnya menyentuh angka 94,96 Mbps. Ketiga nilai parameter tersebut lebih sedikit lebih besar apabila dibandingkan dengan kualitas jaringan yang sudah menerapkan RPKI dimana nilai rata-ratanya untuk trafik *download* sebesar 94,61 Mbps mencakup nilai maksimal yang menyentuh angka 94,74 Mbps sedangkan nilai terendah berada di angka 92,57 Mbps. Trafik *download* merupakan sebuah trafik yang berasal dari jaringan internet menuju jaringan

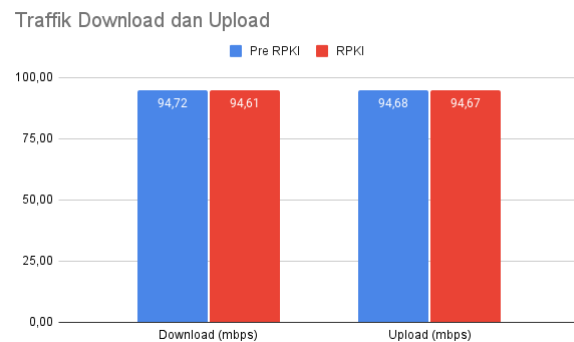
internal mikrotik, sedangkan untuk trafik yang berasal dari jaringan internal menuju internet untuk kondisi yang belum menerapkan RPKI didapatkan rata-rata sebesar 94,68 Mbps dengan nilai terbesar di angka 94,1 Mbps. Nilai tersebut juga mengalami penurunan tetapi tidak signifikan pada jaringan yang sudah menerapkan RPKI dengan rata-ratanya mencapai 94,66 Mbps. Nilai maksimal dan nilai minimal berada di angka 94,98 Mbps dan 93,62 Mbps secara berturut turut. Nilai *latency* yang merupakan nilai waktu yang diperlukan untuk mengirimkan paket dalam proses pengujian menuju sumber diperoleh apabila jaringan tanpa RPKI rata-ratanya mencapai 1,36 ms, nilai maksimal di angka 7 ms, dan minimal di angka 0 ms. Di sisi lain bagi jaringan yang sudah menerapkan RPKI didapatkan nilai rata-rata *latency* menyentuh 1,5 ms dengan nilai 1 ms dan 6 ms sebagai nilai *latency* terendah dan tertinggi. Perbandingan nilai kedua kondisi tersebut secara lebih jelas dapat diamati dalam Gambar 4.

IV. KESIMPULAN

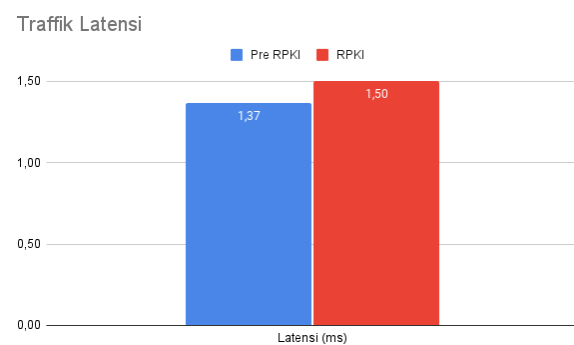
Hasil implementasi BGP RPKI di dalam jaringan I-BGP didapatkan apabila penggunaan *filtering* akan meningkatkan pemakaian *resource*

Tabel 3. Hasil pengukuran jaringan

Kondisi jaringan	Nilai	Download (Mbps)	Upload (Mbps)	Latency (ms)
Pra-RPKI	Min	94,38	94,1	0
	Max	94,96	95,02	7
	Avg	94,71	94,68	1,36
RPKI	Min	92,57	93,62	1
	Max	94,79	94,98	6
	Avg	94,61	94,66	1,5



(a)



(b)

Gambar 4. Trafik rerata pengujian jaringan: (a) trafik *download* *upload*, (b) trafik *latensi*

CPU, memori, sekaligus mengurangi daya *input router* dalam menerima informasi *prefix* meskipun pengaruhnya sedikit atau tidak signifikan. Dari segi performansi jaringan yang berjalan menunjukkan apabila jaringan sebelum menerapkan RPKI mempunyai kualitas jaringan lebih maksimal dengan selisih angka 0,11 Mbps, 0,01 Mbps untuk nilai *upload*, serta nilai latensi sebesar 0,13 ms.

REFERENSI

- [1] A. Reuter, R. Bush, I. Cunha, E. Katz-Bassett, T. C. Schmidt, and M. Wählisch, "Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering," *Comput. Commun. Rev.*, vol. 48, no. 1, pp. 19–27, 2018.
- [2] C. Testart, P. Richter, A. King, A. Dainotti, and D. Clark, "To Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 12048 LNCS, pp. 71–87, 2020.
- [3] T. Chung, "RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins," *Proc. ACM SIGCOMM Internet Meas. Conf. IMC*, pp. 406–419, 2019.
- [4] M. Ando, M. Okada, and A. Kanaoka, "Simulation Study of BGP Origin Validation Effect against Mis-Origination with Internet Topology," *Proc. - 12th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2017*, pp. 75–82, 2017.
- [5] A. A. Winarsih, "Jaringan Komputer, Pengertian, Jenis, Transmisi, dan Topologi," 2021. <https://mediaindonesia.com/teknologi/433330/jaringan-komputerpengertian-jenis-transmisi-dan-topologi> (accessed Dec. 31, 2021).
- [6] H. A. Musril, "Simulasi Interkoneksi Antara Autonomous System (As) Menggunakan Border Gateway Protocol (Bgp)," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 1, pp. 1–9, 2017.
- [7] Idnic, "Internet Routing Registry (IRR)," 2021. <https://idnic.net/service/whois/irr> (accessed Dec. 31, 2021).
- [8] Y. Jia, Y. Liu, G. Ren, and L. He, "RISP: An RPKI-based inter-AS source protection mechanism," *Tsinghua Sci. Technol.*, vol. 23, no. 1, pp. 1–12, 2018.
- [9] Idnic, "Apa itu RPKI dan mengapa membutuhkan RPKI?," 2021. <https://idnic.net/service/rpki> (accessed Dec. 31, 2021).
- [10] "BGP Advanced — Prevent BGP Hijacking With RPKI," 2021. <https://medium.com/netshoot/bgp-advanced-prevent-bgp-hijacking-with-rpki-6be91fa4a9e0> (accessed Dec. 31, 2021).
- [11] N. Labs, *Routinator User Manual NLnet Labs*. 2021.
- [12] E. W. Taringan, "Performance Evaluation and Comparison Between FRRouting and BIRD Open Source Routing Platform," *Telkom University*, 2021.

