

Сигурност у BGP Протоколу

Маријана Тосовић, Слободан Обрадовић

Електротехнички факултет

Источно Сарајево, Босна и Херцеговина

marijana@etf.unssa.rs.ba, slobo.obradovic@gmail.com

Садржај— У раду је описана важност, недостаци као и аспекти сигурности BGP протокола. Посебна пажња је посвећена BGP Update поруци којом се размијењују информације рутирања између сусједних BGP рутера. Описани су атрибути путање.

Кључне ријечи – BGP; BGP поруке; сигурност

I. УВОД

Рутирање је поступак одабира пута кроз мрежу којим ће се слати промет. Свака мрежа мора имати рјешено усмјеравање. За рутирање на већини мрежа потребно је имплементирати протоколе рутирања који омогућавају аутоматску и самосталну размјену података о мрежи и путевима између рутера те одабир пута за просљеђивање саобраћаја. Тиме се постиже динамичко прилагођавање тренутном стању и промјенама на мрежи без уплитања људског фактора те се омогућава непрестано функционисање и повезаност саме мреже. BGP протокол у својој основној верзији нема рјешења која би помогла у сигурности протокола. Због тога се недостаци у BGP протоколу могу искористити за разне нападе попут напада ускраћивањем услуга (DoS напад), неовлаштени приступ, прислушкивање, управљање пакетима, упад у сесије итд. Напади могу искоришћавати недостатке у BGP протоколу, али будући да он користи TCP протокол, нападачи могу искоришћавати и пропусте у TCP или IP протоколу. Највећи проблем је засигурно губитак везе између основних дијелова система због чега неки битни сервиси (електронска пошта, VoIP сервиси и сл.) могу престати с радом. Други ризик је повјерљивост података која може бити нарушена ако су подаци погрешно преусмјерени што може бити резултат погрешних информација у Update поруци. У сљедећим поглављима ће се разматрати BGP протокол, BGP поруке, затим недостаци BGP протокола и начини којима се могу спријечити или барем ублажити напади на BGP протокол.

II. BGP ПРОТОКОЛ

BGP је најпопуларнији системски рутинг протокол и представља надоградњу EGP протокола. Користи се за усмјеравање међу аутономним системима (AS) и тренутно се користи верзија 4 BGP-а која омогућава бескласно међудоменско усмјеравање (CIDR-Classless Inter-Domain Routing), агрегацију рута, инкременталне додатке, боље

могућности филтрирања и способности одређивања политике усмјеравања. Последња верзија BGP-а описана је у документу RFC 4271 [1] који је исправио многе недостатке RFC 1771 [2]. Основни алгоритам рада BGP протокола је модификована верзија протокола вектора удаљености који се зове протокол вектора пута (Distance vector).

BGP је врло комплексан и протокол бројних могућности и као такав BGP представља стандард за размјену информација између пружалаца Интернет услуга (ISP), те између ISP-ова и већих корисника (нпр. Универзитета који унутар своје мреже користе неки од унутрашњих протокола за рутирање као што су протоколи вектора удаљености попут EIGRP-а, RIP-а или протоколи стања везе попут OSPF-а).

Постоје два типа BGP протокола који се разликују по функцији везе између рутера, а то су интерни BGP (iBGP) и екстерни BGP (eBGP). Интерни BGP се користи за повезивање рутера унутар истог аутономног система, док се екстерни BGP користи за повезивање различитих аутономних система. Треба нагласити да се iBGP користи само за координацију и синхронизацију BGP информација кроз аутономни систем зато јер је преспор за улогу класичног унутрашњег протокола рутирања. Спорост BGP-а произлази из чињенице да рутери који подржавају поменути протокол могу садржавати комплетне рутинг табеле (неколико 100.000 рута). Из истог разлога, BGP рутери су обично најјачи и најскупљи уређаји у цијелој мрежи.

BGP користи TCP протокол који подразумева успостављање TCP везе између рутера на порту 179. Додавање рутера са којим ће се комуницирати обавља се ручно због чега није потребно дефинисати поступке откривања сусједа који се користе у IGP протоколима. BGP рутер у свом раду успоставља TCP везе са свим својим сусједима, те затим размјењује цијеле табеле рутирања у којима се налазе информације о путевима према AS-у у коме се налази одредишна мрежа. Обзиром да су табеле BGP рутера на Интернету велике, оне се међу сусједним рутерима размјењују само једном тј. када се први пут повежу, док се касније само ажурирају објављивањем нових или повлачењем постојећих префикса. BGP пут се састоји од низа аутономних система које треба проћи до одредишта. При томе може постојати неколико путева с истим одредиштем, а допушта се и примјена различитих политика усмјеравања, дефинисаних

са скупом атрибута. Пут којим се усмјеравају пакети према неком одредишту бира се на основу параметара пута, доступности пута, додатних правила о прихватању пакета, правила о пропуштању пакета, уговора између АС-ова и атрибута.

III. BGP ПОРУКЕ

У свом раду BGP рутери размјењују четири врсте порука: Open, Update, Keep Alive и Notification. Поруком типа Open се успоставља BGP веза. Садржи основне информације попут идентификатора рутера, кориштене верзије BGP-а, броја AS-а. Ако постоји неусаглашеност у конфигурацијским параметрима нпр. AS бројеви или адресе, BGP сесија се неће успоставити и одговарајућа Notification порука ће бити послана. Када се успостави BGP сесија рутери размјењују све познате руте користећи поруку Update, а након тога само када дође до промјене BGP рута у рутинг табелама. Update поруке се састоје од префикса, AS-path-а и атрибута AS-path-а којима се ближе одређује начин третирања дате руте. BGP рутери чувају број верзије BGP рутинг табеле сусједних рутера. Број верзије се инкрементира приликом сваког убацивања или избацивања руте. Ако нема никаквих промјена размјењују се Keep Alive поруке које су мале величине и шаљу се често. BGP Update порука је срж BGP-а па ће бити детаљније описана у наставку.

A. BGP Update Порука

Update поруке се користе за размјену информација рутирања између сусједних BGP рутера. Једна Update порука служи за оглашавање само једне доступне руте свом сусједу, или за повлачење једне или више раније објављених рута које су постале недоступне, или више нису у употреби. Update порука може такође истовремено оглашавати једну руту и повлачити више претходно оглашених рута. Свака Update порука обавезно садржи заглавље фиксне величине од 19 бајта. Три главне компоненте Update поруке приказане на сл. 1 су: network-layer reachability information (NLRI), path атрибути, и повучене руте.

- Поље Unfeasible Routes Length:

Ово поље је дужине 2 бајта и садржи укупну дужину у бајтима слједећег поља Withdrawn Routes. Из ове вриједности се може израчунати вриједност дужине поља Network Layer Reachability Information. Ако је вриједност овог поља 0, Update порука не садржи руте које су постале недоступне па у складу са тим не постоји нити поље Withdrawn Routes.

- Поље Withdrawn Routes:

Ово поље је промјењљиве дужине и садржи листу IP префикса за руте које се повлаче из употребе. Сваки IP префикс кодиран је паром састављеним од дужине мрежне маске префикса (length) и самог префикса (prefix).

- Поље Total Path Attribute Length:

Ово поље је дужине 2 бајта и садржи укупну дужину у бајтима поља Path Attributes. Из ове се вриједности касније може израчунати вриједност дужине поља Network Layer

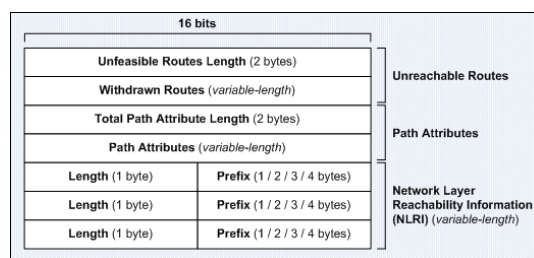
Reachability Information. Ако је вриједност овог поља 0, Update порука не садржи поље Network Layer Reachability Information.

- Поље Path Attributes:

Секвенца варијабилне дужине атрибута пута (Path Attributes) присутна је у свакој Update поруци. Сваки атрибут састављен је од три члана: типа атрибута (attribute type), његове дужине (attribute length) и вриједности самог атрибута (attribute value) па самим тим може бити промјењљиве дужине.

- Поље Network Layer Reachability Information:

Ово поље је промјењљиве дужине и садржи листу IP префикса. Дужина овог поља у бајтима се може посредно израчунати из дужине осталих поља.



Слика 1. Формат BGP Update поруке

Update порука може оглашавати само једну руту која може бити описана са више атрибута, од којих су неки увијек обавезни. Сви атрибути у једној Update поруци односе се на све мреже, односно на све префиксе оглашене у тој поруци путем поља NLRI. Update порука може имати више префикса који се повлаче из употребе а који су наведени у пољу Withdrawn Routes. Обзиром да сусједни BGP рутери размјењују само по једну руту за сваки префикс овакав начин повлачења једнозначно одређује комбинацију руте и префикса који се повлачи. Update порука може имати и само оглашену нову руту и само повучене префиксе, а може и обоје истовремено. Уколико Update порука само повлачи префиксе тада неће бити поља атрибута као ни поља NLRI а ако Update порука само оглашава руту, тада неће бити поља са повученим префиксима.

B. Атрибути Путање

BGP протокол користи пуно параметара за рутирање који се још називају и атрибути, а њима се дефинишу правила рутирања. Број атрибута варира, неки су обавезни тако да морају бити присутни у свакој поруци, док су други допунски и не морају се појавити у поруци. Конфигурација BGP-а подразумева конфигурисање атрибута рута и путања. За сваку руту постоје дефинисани атрибути који се дијеле у 4 групе:

- Добро познати обавезни - морају да постоје у свакој BGP Update поруци придружен одговарајућој NLRI. Све имплементације BGP-а морају да користе ове поруке. Недостатак ових атрибута у Update поруци генерише грешку.

- Добро познати необавезни - атрибути који препознају све BGP имплементације и у складу са њима се понашају, али који не морају бити придружени неком NLRI.
- Опциони преносиви - који не морају да препознају све BGP имплементације и да се понашају у складу са њима (опциони). Ако рутер добије овакав атрибут који не препознаје онда треба да га прослиједи осталим BGP сусједима (преносивост).
- Опциони непреносиви - који не морају да препознају све BGP имплементације и да се понашају у складу са њима (опциони). Ако рутер добије овакав атрибут који не препознаје, онда га не прослијеђује даље (непреносивост).

Приликом одабира руте BGP користи сљедеће атрибуте: `origin`, `AS_path`, `next_hop`, `local_preference` (атрибути локалне предности), `multi_exit_disc` (вишеизлазни дискриминирајући атрибути), `atomic_aggregate` и `aggregate`.

Атрибут `origin` је обавезни атрибут пута који дефинише поријекло пута и генерише га рутер од кога пут потиче. Атрибут садржи информацију о томе да ли се рутер које је примио Update поруку и изворни рутер налазе у истом AS-у и његова вриједност не смије бити мијењана од стране других рутера.

`AS_path` је обавезни атрибут пута који дефинише пут као листу сегмената пута које треба проћи до одредишта. Сваки сегмент пута је дефинисан са скупом AS-ова које је Update порука прошла, број пређених AS-ова и бројевима AS-ова.

Атрибут `next_hop` дефинише IP адресу рутера који је први на путу до одредишта. Обично се узима адреса рутера који се налази на почетку најкраћег пута ка неком одредишту. Ако је сљедећи рутер у другом AS-у онда се вриједност атрибута мора промијенити.

`Local preference` атрибут је необавезни атрибут пута који одређује политику усмјеравања одлазног промета.

`Multi-exit discriminator` је изборни локални атрибут који служи за одабир једног од више понуђених путева према истом AS-у.

`Atomic aggregate` атрибут је необавезни атрибут пута који омогућује спајање путева према одредишту тако да се више путева спаја и објављује као један у Update поруци.

`Aggregate` је изборни транзитни атрибут везан за претходни и њим се остварује спајање путева.

IV. НЕДОСТАЦИ BGP ПРОТОКОЛА

BGP протокол има неколико недостатака који се углавном јављају због великог броја чворова (рутера, AS-ова итд.) у данашњем Интернету. Ови недостаци нису били јако изражени у времену када се BGP протокол развијао управо из разлога што Интернет није било тако велик као данас.

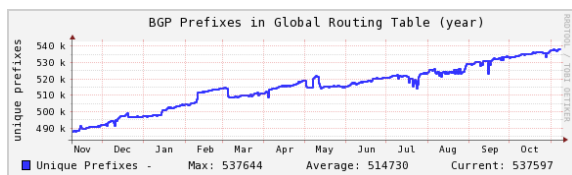
Један од највећих недостатака BGP протокола је захтјев да сви рутери у AS-у међусобно морају бити повезани директно како би се избјегле петље (loop prevention). Овај проблем није изражен у мањим мрежама, али код великих AS-ова, може доћи до смањења перформанси због великог броја порука које рутери измјењују.

Овај проблем се рјешава методама рефлектора путева и конфедерације које се међусобно надопуњују. Прва метода описана документом RFC 4456 [3] користи један рутер (или два због редундантности) као рефлектор пута како би се смањио број веза између рутера у AS-у. Рефлектор пута је увези с неколико BGP рутера који му шаљу своје табеле. Због тога се остали BGP рутери не морају повезивати с њима, него је довољно повезати се с рефлектором како би добили све информације које имају рутери са којима нису директно повезани.

Други начин којим се рјешава прије описани проблем су конфедерације [4]. Овом методом се велики AS дијели у неколико мањих AS-ова које је лакше надгледати. Мањи AS-ови се према другим AS-овима представљају као матични AS коме припадају. Иако ове методе смањују проблем који може настати због захтјева за директном повезаношћу свих рутера, њиховим кориштењем настају нови проблеми као што су осцилације путева, неоптимално рутирање и спорија конвергенција.

Још један недостатак BGP протокола је велика осјетљивост на грешке у рутеру због које он често прелази између активног и неактивног стања (route flapping). Ова појава може бити резултат погрешно конфигурисаног рутера или намјерног напада. У сваком случају, путеви који користе тај рутер наизмјенично се изузимају из табеле рутирања и поново додају у кратким размацима (20-50 пута у секунди). Због тога што BGP рутер мора сваку промјену пута одмах дојавити својим сусједима, долази до великог броја Update порука које рутери измјењују. Ово загушује цијелу мрежу непотребним порукама које су резултат кvara само једног рутера. Утицај route flapping-a се смањује методом описаном у документу RFC 2439 [5], која се зове route flap damping. Недостатак ове методе је спора конвергенција тако да се данас се све више савјетује избјегавање кориштења route flap damping-a. Разлог је све већи напредак рутера који имају довољно процесорске снаге за смањење утицаја route flapping појаве.

Ипак, највећи проблем протокола је раст табела за рутирање. Приказан на слици 2 је раст табела рутирања, што представља проблем за старије BGP рутере који најчешће немају довољно меморије или процесорске снаге за управљање с новим путевима. Велике табеле могу повећати нестабилност система у смислу реакције на велике промјене у систему када је потребан одређен временски период док сви рутери не израчунају нове путеве. Раст табела рутирања је дјелимично успорен кориштењем CIDR-a и агрегације путева, али ове методе нису довољне. Због великог броја путева, долази до размјене велике количине порука којима се информације о путевима измјењују између рутера путем Update порука.



Слика 2. Раст табела рутирања у претходној години [6]

V. СИГУРНОСТ У BGP ПРОТОКОЛУ

У развоју BGP протокола није се водило рачуна о сигурности тако да је BGP подложен разним врстама напада [7]. BGP протокол у основној верзији нема механизам аутентикације којим би се провјерило да ли извориште поруке које је наведено у поруци одговара AS-у одакле је порука послана. Нападаци могу искористити ове пропусте како би нпр. слали лажне Update поруке са погрешним путевима рутирања, због чега пакети неће долазити на своје одредиште. Други облик напада је када дође до загушење рутера због великог броја посланих порука. BGP протокол је подложен горе поменутим сигурносним пропустима који се покушавају исправити разним додацима.

Током година је развијено неколико препорука чијом примјеном се може повећати сигурност BGP протокола. Једна од таквих препорука је документ RFC 2385 [8] који уводи облик заштите BGP сесије користећи једну могућност TCP протокола. Темељи се на додавању 16 битног MD5 hash вриједности у TCP заглавље. На тај начин се чува интегритет посланог пакета и онемогућује злоупотреба. Са друге стране имамо као недостатке поменуте сигурносне имплементације повећано вријеме обраде BGP поруке и повећање величине пакета. Препорука уводи један релативно једноставан механизам заштите, али он ипак није довољан како би се важни BGP рутери очували од напада.

Неколико архитектура је предложено у сврху избјегавања напада на BGP протокол. Обзиром да BGP нема подржану аутентикацију, јер се заправо не провјерава исправност порука, може бити изложен разним нападима. S-BGP архитектура је један од првих приједлога за повећање сигурности BGP протокола. У случају S-BGP уведена је инфраструктура јавног кључа (PKI) којом се врши аутентикација власништва над блоком IP адреса, аутентикација броја AS-а и идентитет BGP рутера и провјера његове овлаштености да заступа одређени AS. Поред тога је уведен нови изборни транзитни атрибут пута (Attestation) којим се преносе дигитални потписи у Update поруци тако да рутер може провјерити префиксе адреса и информације о путу које је добио у самој поруци. Посљедњи сигурносни механизам је кориштење IPSec протокола како би се провјерио интегритет података. Уведени сигурносни механизми пружају јако добру заштиту у смислу провјере исправности IP префикса и интегритета AS_path атрибута. Са друге стране предложена структура је сложена а провјера AS_path атрибута захтјевна за процесоре.

Као алтернатива S-BGP предложене су soBGP и psBGP архитектуре. soBGP архитектура је једноставнија за имплементацију и у својој основи путем сертификата провјерава податке у атрибуту AS_path, односно могућност да рутер који је објавио одређени пут проводи пакете тим путем или му је пут уствари недоступан. У овом случају би се могло закључити да је та порука дио напада којим се покушава пакете скренути на погрешан пут.

Архитектура psBGP је мање сигурна од S-BGP архитектуре због мањег броја сертификата који се користе и непостојања централног сертификационог тијела. Са друге стране, једноставнија је за увођење од S-BGP али ипак не толико као soBGP. soBGP архитектура је најједноставнија за имплементацију али и најнесигурнија архитектура од разматраних.

Неке од имплементација BGP протокола су Quagga [9], OpenBGPD [10], и XORP [11].

VI. ЗАКЉУЧАК

У раду је описана важност BGP протокола, али и његови недостаци. Константно се трага за новим препорукама и рјешењима за два главна проблема BGP протокола: раст табела за рутирање и повећање сигурности. Стални раст Интернета условљава стални развој нових рјешења овог проблема. Други проблем је уствари битнији јер осјетљивост BGP рутера на нападе директно утиче на саму инфраструктуру Интернета. У претходном дијелу описано је неколико рјешења којима се може повећати сигурност BGP протокола. Област сигурности BGP протокола ће се и даље наставити интензивно истраживати јер рјешења која сада постоје су или непримјенива или имају пресложену структуру сертификата или не пружају довољну заштиту каква би била задовољавајућа за тако кључан дио Интернета

Други смјер истраживања којим би се ријешили проблеми у BGP протоколу је замјена новим протоколом за усмјеравање између AS-ова. HLP протокол би требало бити бољи од BGP протокола у конвергенцији, изоловању грешке, скалабилности те би требало слати мање порука за промјену путева. Међутим, HLP протокол би користио заједничку политику рутирања у свим AS-овима при чему се користи претпоставка да је Интернет највећим дијелом организован као хијерархија AS-ова. Ово значи да би се особина BGP протокола о чувању информације о политици усмјеравања требало жртвовати. Међутим, BGP протокол не открива алгоритам којим одређује пут рутирања пакета, па самим тим ни политику рутирања у AS-у.

ЛИТЕРАТУРА

- [1] Y. Rekhter, et al. "A Border Gateway Protocol 4 (BGP-4)," RFC 4271, IETF, 2006 [Online]. Available: <http://ietf.org/rfc/rfc4271>
- [2] Y. Rekhter, T. Li, "A Border Gateway Protocol 4 (BGP-4)," RFC 1771, IETF, 1995 [Online]. Available: <http://ietf.org/rfc/rfc1771>
- [3] T. Bates, et al. "BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)," RFC 4456, IETF, 2006 [Online]. Available: <http://tools.ietf.org/html/rfc4456>

- [4] P. Traina, et al. "Autonomous System Confederations for BGP," RFC 3065, IETF, 2007 [Online]. Available: <http://tools.ietf.org/html/rfc5065>
- [5] C. Willamizar, et al. "BGP Route Flap Damping," RFC 2439, IETF, 1998 [Online]. Available: <http://ftp.ietf.org/rfc/rfc2439>
- [6] Team Cymru [Online]. Available: http://www.cymru.com/BGP/bgp_prefixes.html
- [7] S. Kent, C. Lynn, and K. Seo, "Secure Border Gateway Protocol (SBGP)," IEEE Journal on Selected Areas in Communications, Vol. 18, No. 4, April 2000.
- [8] A. Heffernan, "Protection of BGP Sessions via the TCP MD5 Signature Option," RFC 2385, IETF, 1998 [Online]. Available: <http://ietf.org/rfc/rfc2385>
- [9] Quagga Routing Suite [Online]. Available: <http://www.nongnu.org/quagga/>
- [10] OpenBGPD Project [Online]. Available: <http://www.openbgpd.org/>
- [11] XORP Project [Online]. Available: <http://www.xorp.org/>

ABSTRACT

The paper addresses importance, disadvantages and security aspects of Border Gateway Protocol (BGP). Special attention is dedicated to BGP update message used for exchange of routing information between neighboring routers. Path attributes are also discussed.

BGP SECURITY ISSUES

Marijana Čosović, Slobodan Obradović