ردیابی بسته‌های IP مبتنی بر نشانه‌گذاری در شبکه BGP در سطح AS باقابلیت Extended Community

علیرضا فرجی
دانشجو ارشد مهندسی کامپیوتر گرایش شبکه‌های کامپیوتری، دانشگاه جامع امام حسین (ع)
سید جواد موسوی حسینی
دانشجو ارشد مهندسی کامپیوتر گرایش شبکه‌های کامپیوتری، دانشگاه جامع امام حسین (ع)

چکیده

ردیابی IP یکی از مسائل امنیتی مهم در شبکه‌های کامپیوتری است. در شبکه‌های کامپیوتری امروزی، ارسال و دریافت بسته‌های اطلاعاتی در سطح بسیار بالایی انجام می‌شود و معمولاً تعداد زیادی بسته در شبکه ارسال و دریافت می‌شود؛ بنابراین، در صورت وقوع حملات مخرب، مشخص‌کردن منشأ حمله و دسترسی به اطلاعات لازم برای افشای جزئیات حمله بسیار مهم است. یکی از روش‌های مورداستفاده برای ردیابی‌ای پی، استفاده از پروتکل BGP با Extended Community(EC) است. در پروتکل BGP، اطلاعات ارسال‌شده از طریق بسته‌های Update با استفاده از EC به سایر دستگاه‌ها ارسال می‌شود. با استفاده از این EC، می‌توان برای هر بستهٔ اطلاعاتی مشخص کرد که از کدام سیستم خودمختار به شبکه واردشده است. این امر اجازه می‌دهد تا در صورت وقوع حملات، مسیر بسته‌های مخرب با استفاده از اطلاعات EC مشخص‌شده و مکان منشأ حمله مشخص شود. به همین دلیل، استفاده از پروتکل BGP با EC یکی از روش‌های مؤثر برای ردیابی‌ای پی است و می‌تواند در جلوگیری از حملات مخرب به شبکه کمک کند. بااین‌حال، برای استفاده از این روش، باید پروتکل BGP را در شبکه پیکربندی کرد و از دستگاه‌های قابل پیکربندی استفاده کرد.

واژه‌های کلیدی: نشانه‌گذاری جریان، سیستم خودمختار، ردیابی IP، پروتکل BGP

مقدمه

در این مقاله، به بررسی مفهوم ردیابی بسته‌های IP مبتنی بر نشانه‌گذاری در شبکه BGP[1] باقابلیت EC[2] می‌پردازیم. EC این امکان را فراهم می‌کند تا اطلاعات اضافی به مسیریابی اضافه شود و بسته‌های IP با دستگاه‌های مختلفی مدیریت شوند. در این راستا، اهمیت و کاربردهای EC در بهبود امنیت و کنترل ترافیک در شبکه BGP را بررسی می‌نماییم.

در روش ردیابی‌ای پی با استفاده از پروتکل BGP و ویژگیEC ، چالش‌های مختلفی وجود دارد که در این مقاله می‌توان به برخی از آن‌ها اشاره کرد .درروش ردیابی‌ای پی با استفاده از پروتکل BGP و ویژگیEC ، ذخیره تعداد AS[3] دربسته‌های IP می‌تواند چالش‌هایی ایجاد کند که بهتر است در نظر گرفته شوند:

- افزایش حجم داده: ذخیره تعداد AS دربسته‌های IP می‌تواند باعث افزایش حجم داده می‌شود. این افزایش حجم داده می‌تواند مشکلاتی مانند کاهش سرعت انتقال داده، افزایش زمان پاسخ و تأخیر در شبکه ایجاد کند.
- تداخل با دیگر ویژگی‌های EC: دیگر ویژگی‌های EC نیز دربسته‌های IP استفاده شوند، ممکن است تداخلی در مقادیر آن‌ها با تعداد AS ایجاد شود و این مشکلاتی مانند ازدست‌دادن اطلاعات یا عملکرد نامناسب را به همراه داشته باشد.

برای مقابله با این چالش، می‌توان از راهکارهای زیر استفاده کرد:

- استفاده از روش‌های فشرده‌سازی: این روش‌ها می‌توانند به کاهش حجم داده کمک کنند و درنتیجه کاهش هزینه و زمان انتقال داده را به دنبال داشته باشند.
- استفاده از فیلترهای BGP: استفاده از فیلترهای BGP برای حذف اطلاعات اضافی و اجازه دهی به تنها ارسال تعداد AS موردنیاز می‌تواند در کاهش حجم داده و هزینه به دلیل انتقال داده‌های اضافی کمک کند.

پیشینه تحقیق

فروشانی و همکاران(Aghaei-Foroushani & Zincir-Heywood, 2016) ایده ای جدید برای پیاده سازی ردیابی ای پی با استفاده از BGP و ویژگی Extended Community معرفی می کند. این مقاله برای حل مشکلات مربوط به تکنیک های پیشین در ردیابی ای پی با استفاده از BGP ارائه شده است. این روش از بسته های IP استفاده می کند که در شبکه جابجا می شوند و به AS های مختلف ارسال می شوند. برای ردیابی بسته های ای پی، اطلاعات مربوط به ASهایی که بسته از آنها عبور می کند در Extended Community آن بسته قرار می گیرد. در این مقاله، یک شیوه علامت گذاری جدید بر اساس اطلاعات Autonomous System به نام (ASFM[4]) ارائه شده است که با استفاده از آن، می توان بسته های ردیابی شده را به آدرس مقصد اصلی رساند. به طور خلاصه، یک روش نوآورانه برای ردیابی ای پی با

[1] Border Gateway Protocol

[2] Extended Community

[3] Autonomous System

[4] Autonomous System based Flow Marking

استفاده از BGP و Extended Community ارائه می دهد که با استفاده از اطلاعاتAutonomous System ، مشکلات روش های قبلی را برطرف می کند.

اختر و همکاران(Aktar & Nur, 2021) یک روش جدید برای ردیابی حملات (DoS[5]) در شبکه‌ها ارائه می‌دهد. در این روش، با استفاده از تابع هش برای محاسبه یک شناسه برای بسته‌های شبکه، بسته‌ها مشخص و با استفاده از این شناسه، مسیر طی شده توسط بسته‌ها تا مبدا آن‌ها پیدا می‌شود. سپس با استفاده از پروتکل BGP و ویژگی extended community، اطلاعات مسیر طی شده توسط بسته‌ها به مسیریاب‌های مختلف در شبکه ارسال می‌شود. در نهایت، با استفاده از اطلاعات ارسالی از طریق extended community و تابع هش محاسبه شده برای بسته‌ها، مسیر طی شده توسط بسته‌ها تا مبدا آن‌ها ردیابی می‌شود. این روش مزیت‌هایی مانند کم بودن هزینه‌ها و عملکرد بالایی در برابر حملات DoS دارد.

ارجمند پناه و همکاران(Arjmandpanah-Kalat et al., 2020) به طراحی و ارزیابی عملکرد یک تکنیک ردیابی آی‌پی تک جریان در سطح AS می‌پردازد. در این تکنیک از پروتکل BGP و ویژگی‌های extended community برای برچسب‌گذاری جریان‌های داده استفاده می‌شود. سپس با استفاده از جدول(FIB[6]) ، مسیر جریان‌های داده به سمت مقصد پیدا شده و در پیام بازگشتی ICMP در قالب فیلد Source AS Number قرار داده می‌شود.

نتایج آزمایش‌ها نشان می‌دهد که تکنیک ارائه شده بادقت ۱۰۰٪ در تعقیب جریان‌های داده با سرعت بالا عمل می‌کند. همچنین این تکنیک با توجه به میزان حافظه و پردازش مورد نیاز، از کارایی خوبی برخوردار است. در نتیجه، تکنیک پیشنهادی می‌تواند گزینه مناسبی برای ردیابی جریان‌های داده در شبکه‌های مبتنی بر AS باشد.

کروپ و همکاران(Krupp & Rossow, 2021) یک روش فعال و مبتنی بر BGP برای ردیابی DDOS حملات تقویت شده است. این روش از ویژگی های BGP Extended Community استفاده می کند تا بسته های مربوط به حملات را تشخیص دهد و آنها را به سمت مبدا برگرداند. برای افزایش کارایی، این روش از یک الگوریتم بازگشتی استفاده می کند که اطلاعات دریافت شده از پیکربندی BGP را استفاده می کند تا به طور هوشمندانه بهترین مسیر را انتخاب کند. آزمایش ها نشان می دهد که Bgpeek-a-boo قادر است به طور دقیق و به موقع به تشخیص و ردیابی حملات DDOS کمک کند.

فدال و همکاران(M Fadel, 2021) به بررسی چگونگی ترکیب دو روش مختلف در ردیابی IP می‌پردازد: یک روش مبتنی بر فشرده‌سازی بر پایه فضای بردار و یک روش مبتنی بر هش. در این مقاله، یک ساختار مختلط به نام "گروه‌بندی هش‌شده‌ی سریع [7]"برای ردیابی IP پیشنهاد شده است. با استفاده از این ساختار، برای هر بسته تنها یک پیغام از یک نود در شبکه ارسال می‌شود و سیستم ردیابی تنها با استفاده از یک پیغام، می‌تواند مسیر بسته را تعیین کند. این ساختار، بر خلاف روش‌های مشابه، تنها یک سطح از محاسبات هش را نیاز دارد و در نتیجه کمترین تأخیر را در ردیابی IP ارائه می‌دهد. همچنین، برای افزایش امنیت، این سیستم با استفاده از یک الگوریتم ترکیب کلید پویا و پروتکل‌های امنیتی، مقاومت خود را در برابر حملات نفوذی و حملات کاهش کارایی افزایش می‌دهد.

---

[5] Denial of Service

[6] Forwarding Information Base

[7] Fast Hashed Grouping

ویتونو وهمکاران(Witono & Yazid, 2022) به بررسی یک روش تریس بک به منظور تشخیص منبع حملات DDoS و حفاظت از شبکه‌های کامپیوتری پرداخته است. در این روش، برچسب‌گذاری احتمالی بسته‌ها با استفاده از مدل‌های احتمالی انجام می‌شود. برچسب‌هایی که به بسته‌ها اختصاص می‌دهند، شامل شناسه AS مبدا و زمان رسیدن بسته به روترها است. این اطلاعات در روترهای مقصد ذخیره می‌شوند و در صورت وقوع حملهDDoS ، با بازیابی اطلاعات این برچسب‌ها، اطلاعات مورد نیاز جهت تشخیص منبع حمله و پیدا کردن راه‌های موثر برای مقابله با آن فراهم می‌شود. بهره‌گیری از مدل‌های احتمالی در این روش، باعث کاهش تعداد بیت‌های مورد نیاز برای برچسب‌گذاری می‌شود و سبب بهبود کارایی روش می‌شود.

نور وهمکاران(Nur, 2021) یک روش بهبود یافته برای تعقیب پیام‌های IP است. این مقاله بهبود یافته ای بر روش (PPM) ارائه می دهد که از این الگوریتم در کاهش زمان و میزان حافظه مصرفی برای تعقیب استفاده می شود. الگوریتم پیشنهادی با استفاده از دو کد AS یکتا به عنوان برچسب های ترکیبی، قابل اعمال است و امکان اطمینان از صحت پیام تعقیب شده را فراهم می کند. نتایج آزمایش های مقاله نشان می دهد که الگوریتم پیشنهادی با حداقل تأثیر بر کیفیت خدمات، نیاز به حافظه کمتر و کارایی بیشتری نسبت به الگوریتم PPM ارائه شده در مقالات قبلی دارد.

ردیابی **Ip** مبتنی بر شبکه

ایده اصلی این روش، بررسی ارتباطات شبکه‌ای بین مسیریاب‌ها تا ردگیری مبدأ حمله است. در این روش الگوی خاصی از حملات، توسط مدیر شبکه، مشخص و با آن به ردگیری حمله می‌پردازد. بعد از تشخیص حمله، با استفاده از اتصال جریان بالا گره به گره به مبدأ حمله نزدیک‌تر شده تا مبدأ اصلی حمله شناسایی شود. روش‌های ردگیری باتوجه‌به ساختار شبکه‌ای که در آن ردگیری صورت می‌پذیرد ارائه می‌شوند. این روش‌ها دارای ایرادات فراوانی هستند و باید به‌صورت دستی کنترل شوند. در این بخش می‌توان به Control Flooding و Input Debugging اشاره کرد.

ردیابی مبتنی بر نشانه‌گذاری

ایده اصلی این روش تزریق داده‌های ردگیری درون چند فیلد از سرآیند بسته‌های IP است و هدف آن بازسازی مسیر حمله و شناسایی گره حمله یا نزدیک‌ترین گره به آن است. به‌طورکلی به دودسته‌ی نشانه‌گذاری احتمالی و نشانه‌گذاری قطعی تقسیم می‌شود.

عبدالله یاسین و همکاران (Nur & Tozal, 2021) اولین بار روش نشانه‌گذاری احتمالی بسته (PPM[8]) را معرفی کردند. در این روش، هر مسیریاب در طول مسیر حرکت بسته، با احتمال P بخشی از اطاعات مربوط به شبکه را درون سرآیند بسته قرار می‌دهد. این اطلاعات نشانه‌گذاری شده می‌توانند شامل آدرس IP مسیریاب فرستنده، آدرس IP مسیریاب بعدی و یا تعداد پرش‌های طی شده باشد. iTrace با عبور هر ۲۰۰۰۰ بسته یک بسته‌ی جدید ICMP تولید کرده و به مقصد بسته‌های عبوری ارسال می‌کند. پیام‌های ICMP تولیدشده، شامل داده‌های ردگیری، مهر زمانی و داده‌های احراز هویت بین مبدأ و مقصد هستند. قربانی با توجه به داده‌های موجود در پیام‌های ICMP دریافت شده، مسیر حمله را بازسازی می‌کند.

یاسین و همکاران (Nur & Tozal, 2018)روش نشانه‌گذاری قطعه‌ی بسته DPM را ارائه دادند. در این روش، تنها مسیریاب‌های مرزی ورودی شبکه، در مقایسه اطلاعات نشانه‌گذاری شامل بخشی از داده‌های شناسایی رابط ورودی

[8] Probabilistic Packet Marking

است. شبکه‌ی جدیدی وارد شود، توسط مسیریاب مرزی ورودی آن شبکه، نشانه‌گذاری می‌شود. درنهایت گره قربانی قادر تواند بود آدرس مسیریاب‌های مرزی شبکه‌هایی که بسته از آن عبور کرده است را شناسایی کند.

ردیابی **IP** مبتنی بر ثبت

در مقابل روش‌های نشانه‌گذاری بسته، روش‌های مبتنی بر ثبت، فضایی را در گره‌های میانی مسیر برای ثبت داده‌های نشانه‌گذاری به خود اختصاص می‌دهند. در این روش، نشانه‌ای از همه یا بخش زیادی از بسته‌های عبوری در هر گره ثبت و از این داده‌ها برای ردگیری استفاده می‌شود. اصلی‌ترین ضعف این روش‌ها، نیاز به فضای ذخیره‌سازی زیاد، پردازش سنگین آن و نیاز به سن افزارهای خاص است.

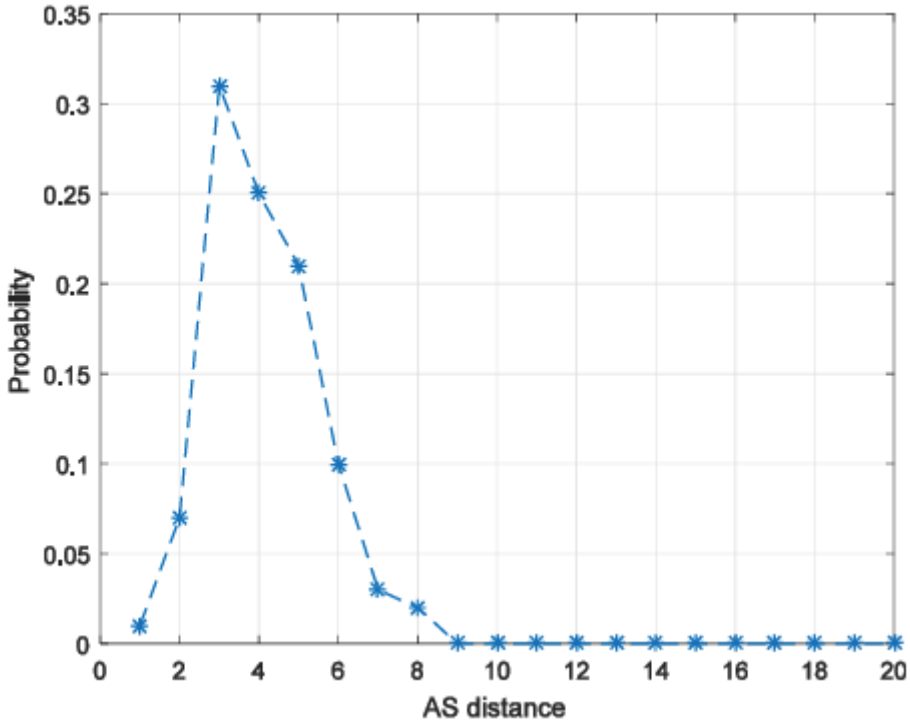
توزال و همکاران (Nur & Tozal, 2018)روش SPIE را ارائه دادند. ایده اصلی این روش ذخیره کردن نشانه‌ای از بسته‌های عبوری در ساختار داده‌ای به نام فیلتر بلوم در مسیریاب‌های طول مسیر است. در این روش نیاز به فضای ذخیره‌سازی زیاد در مسیریاب‌های عبوری داریم و همچنین این نوع ذخیره‌سازی مثبت کاذب بالایی دارد. از معایب این روش می‌توان به این مورداشاره کرد که اگر تعداد AS های کمی از روش پیشنهادی پشتیبانی کنند، نرخ ردگیری در این روش به‌شدت کاهش پیدا خواهد کرد و داده‌های ردگیری زیادی تولید می‌کند که نیاز به فضای ذخیره‌سازی زیادی دارد.

ردیابی **IP** در سطح **AS**

در این بخش به روش‌های ردگیری که در سطح AS ارائه‌شده‌اند، می‌پردازیم نویسنده روش ردگیری را برای شناسایی AS مهاجم ارائه کرده است در این روش با احتمال نشانه‌گذاری سیستم خودمختار (ASN) نشانه‌گذاری می‌شود این روش درزمانی که شماره ۱۶AS بیت بوده است ارائه‌شده است.

مای تیلی و همکاران(Nur & Tozal, 2018) درروش AS-SPT که قابلیت اجرا در حالتی که بخشی از شبکه تحت پوشش از روش پیشنهادی پشتیبانی نمی‌کند را دارد ارائه داد و از روش ردگیری ترکیبی برای ردگیری AS مهاجم استفاده می‌کند AS قربانی با دریافت ترافیک حمله از همسایه‌هایش درخواست بررسی داده‌های ثبت‌شده را دارد در صورت بازخورد جواب مثبت از یکی از همسایه‌ها این درخواست تکرار شده تا AS مهاجم شناسایی شود. از مهم‌ترین معایب این روش می‌توان به این مورداشاره کرد که به دلیل ارائه شدن این روش در سطح بسته مقدار زیادی داده‌ی ردگیری تولید کرده که نیاز به فضای زیاد ثبت در گره‌های میانی دارد.

بی هوانی و همکارانش(Bhavani et al., 2020) روش FAST را ارائه کرده‌اند که تنها قابلیت ردگیری پنج AS را دارد و در صورت وجود بیش از این تعداد AS در طول مسیر حمله قابل‌شناسایی نمی‌باشد.



شکل ۱: فراوانی تعداد AS بین مبدأ و مقصد

نقش پروتکل **BGP**

BGP یک پروتکل مسیریابی است که برای تبادل اطلاعات مسیریابی بین روترهای مختلف در اینترنت استفاده می‌شود. هر روتر در شبکه، دارای یک جدول مسیریابی است که حاوی اطلاعاتی درباره مسیرهای احتمالی به سمت مقصد است. وقتی یک بسته در شبکه به سمت مقصد حرکت می‌کند، روترهای مختلف به دنبال بهترین مسیر برای رساندن بسته به مقصد، در جداول مسیریابی خود جستجو می‌کنند. برای این منظور، هر روتر به‌صورت دوره‌ای با سایر روترها در شبکه، اطلاعات مسیریابی خود را به‌روزرسانی می‌کند(Beer, 2022).

بنابراین، هنگامی‌که یک بسته وارد یک روتر می‌شود، این روتر یک ارجاع BGP برای آدرس مقصد بسته ایجاد می‌کند به این صورت که به سایر روترها در شبکه، اعلام می‌کند که برای این آدرس، بهترین مسیر به سمت مقصد، از طریق خروجی مشخصی است. سپس سایر روترها نیز این اطلاعات را در جداول مسیریابی خود به‌روزرسانی می‌کنند و در صورت لزوم، این اطلاعات را برای روترهای دیگر در شبکه منتشر می‌کنند.

ECA در BGP، یک نوع پیام کنترلی است که برای افزودن اطلاعات تکمیلی به مسیرهای BGP استفاده می‌شود. با اضافه کردن ECA به ارجاع BGP، می‌توان اطلاعات دیگری را به‌جز اطلاعات مربوط به مسیر BGP، به ارجاع اضافه کرد.(Kala et al)

پیام BGP شامل چندین فیلد است که هرکدام اطلاعات مختلفی را درباره‌ی مسیریابی و تنظیمات مربوط به آن، در برمی‌گیرد. برخی از این فیلدها عبارت‌اند از:

- Marker: یک فیلد ۶۴ بیتی که برای تشخیص پیام‌های BGP ارسال‌شده به دستگاه در دو طرف این پروتکل استفاده می‌شود.
- Length: یک فیلد ۲ بایتی که نشان‌دهنده‌ی طول کلی پیام BGP است.

- Type: یک فیلد ۱ بایتی که نشان‌دهنده‌ی نوع پیام BGP است. برخی از نوع‌های معروف پیام BGP شامل Update، Open، Notify و Keepalive هستند.
- Withdrawn Routes Length: یک فیلد ۲ بایتی که نشان‌دهنده‌ی تعداد مسیرهایی است که از جدول مسیریابی حذف‌شده‌اند.
- Withdrawn Routes: یک فیلد متغیر که حاوی لیست مسیرهایی است که از جدول مسیریابی حذف‌شده‌اند.
- Total Path Attribute Length: یک فیلد ۲ بایتی که نشان‌دهنده‌ی طول کلی تمام Path Attributes در پیام Updateاست.
- Path Attributes: یک فیلد متغیر که حاوی مسیرها و خصوصیات مختلف آن‌ها، ازجمله نوع NLRI و MED[9] است.
- NLRI[10]: یک فیلد مربوط به آدرس IP و طول پیشوند.CIDR
- Multiprotocol Extension: یک فیلد برای ارسال پیام‌های BGP روی پروتکل‌هایی به‌جزIPv4 ، ازجمله IPv6.

نشانه‌گذاری بسته در **BGP**

ECAدر قسمت Update Message BGP ذخیره می‌شود. در فیلد Path Attributes این پروتکل،[11] ECA به‌عنوان یکی از ویژگی‌های مسیریابی نگهداری می‌شود که اطلاعات بیشتری درباره‌ی مسیر و خصوصیات مرتبط با آن را در اختیار مسیریابان قرار می‌دهد.

ECA شامل دو بخش است که هر بخش شامل یک یا چندین شماره AS می‌باشد. بسته به نوع ECA می‌تواند شامل یک تا چندین شماره AS باشد. علاوه بر این، برخی از نوع‌های ECA حاوی داده‌های دیگری نیز هستند که در کنار شماره AS ذخیره می‌شوند. برای مثال، ECA نوع Route Target شامل یک شماره ASN و یک شناسه (ID) بوده که برای تحقق مسیریابی MPLS استفاده می‌شود.(AlArnaout et al., 2022)

سیستم خودمختار AS

شماره[12] ASمسیریاب منتقل‌کننده[13] در پروتکل BGP به‌عنوان یکی از BPA[14] در همه‌ی مراحل از مسیریابی بین مسیریابان منتقل می‌شود. هر مسیریابBGP ، شماره AS خود و شماره AS همسایگان را در جدول مسیریابی‌اش نگه می‌دارد(Yang et al., 2020)

وقتی یک Prefix به یک مسیریاب BGP فرستاده می‌شود، آن مسیریاب BGP شماره AS خود را به کنار prefix اضافه می‌کند و این اطلاعات به‌صورت یک مجموعه از BPA به سایر مسیریابان BGP منتشر می‌شود. در همه‌ی مراحل از مسیریابی، این مجموعه از BPA با prefix همراه است و شامل اطلاعاتی مانند شماره AS مسیریاب Ingress و همچنین ASهایی که Prefix در آن‌ها تبلیغ‌شده است می‌باشد.

---

[9] Multiple Exit Discriminator

[10] Network Layer Reachability Information

[11] Extended Community Attribute

[12] Autonomous System

[13] ingress router

[14] BGP Path Attributes

بنابراین، شماره AS در BGP در قالب BPA در همه‌ی مراحل از مسیریابی بین مسیریابان منتقل می‌شود و در جدول مسیریابی هر مسیریاب BGP نگهداری می‌شود.

BPA یا ویژگی‌های مسیریابی، به اطلاعاتی اشاره دارند که در پیغام‌های BGP برای توصیف مسیرهای شبکه استفاده می‌شوند. این ویژگی‌ها شامل اطلاعاتی هستند که مسیریاب‌ها برای تصمیم‌گیری در رابطه با انتخاب مسیر مناسب بین شبکه‌های مختلف استفاده می‌کنند(Afzaal, 2022)

تعدادی از این ویژگی‌ها عبارت‌اند از:

- AS Path: این ویژگی نشان می‌دهد که بسته توسط چه AS هایی عبور کرده است.
- Next Hop: این ویژگی نشان می‌دهد که بسته بعد از دریافت توسط یک مسیریاب BGP به چه IP آدرسی ارسال خواهد شد.
- Local Preference: این ویژگی برای تصمیم‌گیری درون یک AS مورداستفاده قرار می‌گیرد.
- MED[15]: این ویژگی برای تصمیم‌گیری در مورد چند نقطه خروج از یکAS استفاده می‌شود.
- Community: این ویژگی برای گروه‌بندی روت‌ها و پیکربندی سیاست‌های مسیریابی استفاده می‌شود.

BPA در هنگام ارسال یک مسیر به یک مسیریاب BGP توسط یک مسیریاب دیگر، توسط مسیریاب مبدأ که مسیر را اعلام می‌کند، تکمیل می‌شود. به‌طورکلی، ویژگی‌های مسیریابی BGP در پیام‌های UPDATE ساخته‌شده توسط مسیریاب مبدأ قرار می‌گیرند و در طول مسیر، هر مسیریاب BGP ممکن است بعضی از این ویژگی‌ها را تغییر دهد یا حذف کند(Yang)

AS Path و Next Hop به‌طور خودکار توسط مسیریاب مبدأ به پیام UPDATE اضافه می‌شوند. به‌علاوه، مسیریاب‌های BGPممکن است از Local Preference برای تصمیم‌گیری درون یک AS استفاده کنند و MED برای تصمیم‌گیری در مورد چند نقطه خروج از یک AS استفاده می‌شود.

درنهایت، مسیریاب‌های BGP ممکن است از Community برای گروه‌بندی روت ها و پیکربندی سیاست‌های مسیریابی استفاده کنند. بااین‌حال، این ویژگی‌ها در هر مسیریاب BGP ممکن است تغییر کنند و یک مسیریاب BGP نباید بر اساس اطلاعاتی که دریافت می‌کند، فرض کند که این ویژگی‌ها ثابت هستند.(Yang et al., 2020)

ویژگی مسیر EC در پروتکل BGP

Attributeیک ویژگی در مسیریابی BGP است که به شبکه‌های BGP اجازه می‌دهد بیشترین کنترل را بر روی مسیریابی‌شان داشته باشند. این ویژگی، برای تعیین ترافیک عبوری از یک ISP به سمت دیگر ISP ها بسیار مفید است(Afzaal, 2022).

ECA شامل دو بخش است: Typeو Value

Typeشامل نوع EC است و Value شامل مقادیر مربوط به آن است. برخی از انواع EC عبارت‌اند از:

- Route Target (RT): برای تعیین ارتباط بین یک VRF و یک Route Distinguisher (RD) استفاده می‌شود.
- Site of Origin (SoO): برای حفظ محدوده جغرافیایی یک شبکه استفاده می‌شود.
- Cost Community: برای تعیین قیمت هزینه مربوط به مسیریابی از یک ISP به سمت دیگر ISP ها استفاده می‌شود.

[15] Multi-Exit Discriminator

- Bandwidth Community: برای تعیین پهنای باند مربوط به یک لینک استفاده می‌شود.
- OSPF Domain ID: برای تعیین شناسه دامنه OSPF استفاده می‌شود.
- Large Community: برای تعیین وابستگی‌های مسیریابی بین AS ها استفاده می‌شود.
- EC ۶IPv: برای پشتیبانی از مسیریابی ۶IPv استفاده می‌شود.

نتیجه‌گیری

در این مقاله روش ردگیری IP مبتنی بر نشانه‌گذاری جریان در سطح AS ارائه‌شده است. برای تشکیل شبکه تحت پوشش از ویژگی مسیر Community Extended پروتکل BGP، استفاده کرده‌ایم. این ویژگی نیاز به گسترش شبکه تحت پوش را بر روی تمام مسیریاب‌ها، حذف کرده است. سازوکار نشانه‌گذاری در سطح جریان و رشته‌های کنترلی، برای بازسازی داده‌های دریافت شده در مقصد، ارائه‌شده است. همچنین با استفاده از سازوکار تولید امضای مسیر، قادر به شناسایی ترافیک‌های جعل‌شده خواهیم بود و در کمترین زمان ممکن با حداقل سربار در حین اجرای حملات می‌توان AS مهاجم را شناسایی و با حمله مقابله کرد. ازجمله کارهایی که در ادامه‌ی این تحقیق می‌توان انجام داد، ارائه روش ردگیری در پروتکل اینترنت نسخه ۶ است، زیرا با توجه به گسترش این پروتکل در سطح اینترنت، نیازمند روش‌هایی برای ردگیری در آن هستیم.

مراجع

Afzaal, M. (۲۰۲۲). An Overview of Defense Techniques Against DoS Attacks. ۹ ۲۰۲۲th International Conference on Internet of Things: Systems, Management and Security (IOTSMS),

Aghaei-Foroushani, V., & Zincir-Heywood, A. N. (۲۰۱٦). Autonomous system based flow marking scheme for IP-Traceback. NOMS ۲۰۱٦-۲۰۱٦IEEE/IFIP Network Operations and Management Symposium ,

Aktar, S., & Nur, A. Y. (۲۰۲۱). Hash based AS traceback against DoS attack. ٤ ۲۰۲۱th International Conference on Advanced Communication Technologies and Networking (CommNet) ,

AlArnaout, Z., Mostafa, N., Alabed, S., Aly, W. H. F., & Shdefat, A. (۲۰۲۲). RAPT: A Robust Attack Path Tracing Algorithm to Mitigate SYN-Flood DDoS Cyberattacks. *Sensors*, ۲۳(۱), .۱۰۲

Arjmandpanah-Kalat, M., Abbasinezhad-Mood, D., Mahrooghi, H. R., & Aliabadi, S. (۲۰۲۰). Design and performance analysis of an efficient single flow IP traceback technique in the AS level. *International Journal of Communication Systems*, ۳۳(۹), e .٤۳۸۲

Beer, F. (۲۰۲۲). A Hybrid Flow-based Intrusion Detection System Incorporating Uncertainty .

Bhavani, Y., Janaki, V., & Sridevi, R. (۲۰۲۰). IP traceback using flow based classification. *Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science)*, .٤۹۰-٤۸۲ ,(۳)۱۳

Kala, T. S., Rajakumaran, V., & Saradha, S. Detecting IP Spoofing Attack with SDN-Based Integrated Architecture using Distributed Packet Filtering .

Krupp, J., & Rossow, C. (۲۰۲۱). Bgpeek-a-boo: Active bgp-based traceback for amplification ddos attacks. ۲۰۲۱IEEE European Symposium on Security and Privacy (EuroS&P) ,

M Fadel, M. (۲۰۲۱). HDSL: A Hybrid Distributed Single-packet Low-storage IP Traceback Framework. *MEJ. Mansoura Engineering Journal*, ٤٦(٤), .۸۹-۷٥

Nur, A. Y. (۲۰۲۱). Efficient probabilistic packet marking for AS traceback. ۲۰۲۱International Symposium on Networks, Computers and Communications (ISNCC) ,

Nur, A. Y., & Tozal, M. E. (۲۰۱۸a). Identifying critical autonomous systems in the Internet. *The Journal of Supercomputing*, .٤۹۸٥-٤۹٦٥ ,۷٤

Nur, A. Y., & Tozal, M. E. (۲۰۱۸b). Record route IP traceback: Combating DoS attacks and the variants. *Computers & Security*, ۷۲, .۲٥-۱۳

Nur, A. Y., & Tozal, M. E. (۲۰۲۱). Single packet AS traceback against DoS attacks. ۲۰۲۱IEEE International Systems Conference (SysCon) ,

Witono, T., & Yazid, S. (۲۰۲۲). A review of internet topology research at the autonomous system level. Proceedings of Sixth International Congress on Information and Communication Technology: ICICT ۲۰۲۱, London, Volume ,۱

Yang, M.-H., Luo, J.-N., Vijayalakshmi, M., & Shalinie, S. M. (۲۰۲۰). Hybrid multilayer network traceback to the real sources of attack devices. *IEEE Access*, ۸, .۲۰۱۰۹۷-۲۰۱۰۸۷

Yang, M. H. Research Article Storage-Efficient ۱٦-Bit Hybrid IP Traceback with Single Packet .

Marking-based IP packet tracing in AS-level BGP network with Extended Community capability

Alireza Faraji **Seyed Javad Mousavi**

Abstract

IP tracking is one of the most important security issues in computer networks. In today's computer networks, the sending and receiving of information packets is done at a very high level, and usually a large number of packets are sent and received in the network; Therefore, in case of malicious attacks, it is very important to determine the source of the attack and access the necessary information to reveal the details of the attack. One of the methods used for IP tracking is the use of BGP protocol with Extended Community (EC). In BGP protocol, information sent through Update packets is sent to other devices using EC. By using this EC, it is possible to determine for each information packet from which autonomous system it entered the network. This allows, in case of attacks, the path of malicious packets using the specified EC information and the location of the origin of the attack. For this reason, using BGP protocol with EC is one of the effective methods for IP tracking and can help prevent malicious attacks on the network. However, to use this method, the BGP protocol must be configured in the network and configurable devices must be used.

Keywords: Flow marking, autonomous system, IP tracking, BGP protocol