مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال اول، شماره ۴، زمستان ۱۳۹۲، ص ۸۶-۷۷

بهینه کردن الگوریتم کلونی مورچگان برای ردیابی آی پی حملات انکار سرویس

محمد حامدی حمزه‌کلایی[1*]، محمدرضا شامانی[2]، محمدجواد شامانی[3]

۱ و ۳- کارشناسی ارشد امنیت اطلاعات، پردیس بین‌المللی کیش دانشگاه تهران ۲- کارشناسی مخابرات دانشگاه آزاد شهر ری

(دریافت: ۹۲/۰۲/۰۲ ، پذیرش: ۹۲/۰۹/۲۷)

چکیده

حمله انکار سرویس، یکی از شایع‌ترین و بزرگ‌ترین تهدیدات در اینترنت به‌شمار می‌آید که به‌وسیله تقلب در منبع آدرس آی پی انجام می‌پذیرد و منجر به استفاده از منابع سامانه و در نتیجه کاهش کارایی شبکه می‌شود. ردیابی حملات انکار سرویس به‌روش الگوریتم «فرا ابتکاری مورچگان»، یکی از راهکارهای مؤثر مقابله با این‌گونه از حملات است که از سطح جریان ترافیک برای ردیابی منبع حمله، بهره می‌برد. در این تحقیق به بهبود ردیابی الگوریتم مورچگان پرداخته شده و با تقویت جریان‌های ترافیک محتمل‌تر و کاستن فضای جستجو و تغییر در انتخاب گره پایانی، موفق شده که این الگوریتم بهبود بخشیده شود. نتایج شبیه‌سازی شده نشان می‌دهد که راهکار پیشنهادی می‌تواند حمله‌ها، حتی اگر شدت ترافیک حمله بسیار کم باشد و یا اگر جریان حمله‌ای غیر از حمله موجود در مسیریاب‌های شبکه وجود داشته باشد، را به‌درستی ردیابی کند و این قدمی جدید در عرصه ردیابی حملات به کمک الگوریتم‌های فرا ابتکاری، جهت ردیابی حملات انکار سرویس توزیع‌شده محسوب می‌شود.

واژه‌های کلیدی: حمله انکار سرویس، ردیابی،کلونی مورچگان، جریان

۱. مقدمه

بر اساس گزارش سالانه سازمان زیرساخت امنیتی در سال ۲۰۱۰ [۱] و گزارش همایش cryptic سال ۲۰۱۲ [۲]، دفعات حمله انکار سرویس در طول دهه هر سال نزدیک به دو برابر اضافه شده و متناسب با آن، خسارات روز به روز افزوده می‌گردد. حملات با ترافیک پایین در حدود ۸۰ درصد حملات DoS، را شامل می‌شود [۱] که شناسایی و ردیابی آنها به‌نسبت دشوارتر است. از سوی دیگر فن‌های دفاعی به دو دسته دفاع و تشخیص تقسیم می‌شوند [۳]. برای دفاع در مقابل حملات انکار سرویس، مکانیزم‌های کنترلی مانند صافی بسته بر روی مسیر [۴]، صافی ورودی [۵] و محدود کردن نرخ سرویس‌دهی[۶]پیشنهاد شده، به‌علت اینکه مکانیزم‌های هشداردهی محدود کردن نرخ سرویس‌دهی، حملات با جریان‌های ترافیکی قوی را فعال می‌کنند. محدود کردن نرخ سرویس‌دهی برای کاهش خسارت حملات با ترافیک پایین بر روی خطوط ارتباطی مناسب نمی‌باشد. روش‌های فرا واکنشی [۷] به یافتن منبع حمله انکار سرویس پرداخته و با هماهنگی ISP[1] یا مدیر شبکه، به مسدود کردن ترافیک از منبع پرداخته و قادر به عادی‌سازی مجدد سرویس شبکه می‌گردد و در نهایت به بازداشت مهاجمین می‌انجامد. با این حال، هنوز حل این مشکل به‌طور کامل محقق نشده و دلیل آن بر اساس این واقعیت است که حملات انکار سرویس جزء دشوارترین مسائل امنیتی جهت تشخیص و دفاع و ردیابی با آن است البته علت آن، محدودیت منابع و ترکیبات شبکه موجود و تعدد روش‌های حمله و در دسترس بودن و قابل استفاده بودن آن، به‌راحتی حتی برای شخصی که اطلاعاتی در مورد امنیت و نفوذ ندارد و همچنین مخفی بودن مقصد برای سایت میزبان می‌باشد که موجب می‌گردد جدا کردن و حذف ترافیک حمله از ترافیک قانونی بسیار دشوار شود [۱۸]. به‌همین دلیل است که به‌تازگی بسیاری از محققین بر روی ردیابی آی پی تمرکز کرده‌اند. ردیابی آی پی، روشی برای پیدا کردن منبع حمله بدون وابستگی به سرآیند آی پی است. روش‌های ردیابی آدرس آی پی فعلی نظیر نشانه‌گذاری بسته‌ها [۸] به‌صورت مبتنی بر هش [۹] و گام به گام [۱۰] از اطلاعات موجود در مسیریاب‌ها در مسیر حمله انکار سرویس استفاده می‌کند.

1– Internet Service Provider (ISP)

* رایانامه نویسنده پاسخگو: m.hamedi@alumni.ut.ac.ir

در نشانه‌گذاری بسته‌ها، نیاز به رمز کردن اضافی اطلاعات مسیر است که بر روی قسمت‌هایی بدون استفاده سرآیند آی پی که برای ردیابی آی پی کمتر استفاده می‌شوند ذخیره‌سازی می‌شود [۱۱]. همچنین در هر دو روش گام به گام و مبتنی بر هش، نیاز به نصب توابع دیگری بر روی مسیریاب‌ها برای ردیابی آی پی است.

علاوه بر این، بیشتر روش‌های پیشین، مانند کم‌کردن اطلاعات مسیر، بر روی قسمت‌های مخصوص سرآیند آی پی و یا ذخیره مقدار قابل توجهی از بسته‌ها در مسیریاب‌ها، برای ردیابی، نیاز به تغییرات در زیرساخت شبکه دارند[۱۱].

علاوه بر اینها، تمامی روش‌ها نیاز به آن دارند که تمام مسیریاب-های در مسیر حمله انکار سرویس، مکانیزم ردیابی آی پی را پشتیبانی کنند تا بتوان ردیابی آی پی را با موفقیت انجام داد. همچنین تغییر زیرساخت‌ها و تغییر در نرم‌افزارهای مسیریابی، بسیار زمان‌بر و پرهزینه می‌باشد[۱۱].

جهت ردیابی حملات با ترافیک پایین نیز ایده‌هایی مطرح شده است، ولی به این علت که از توپولوژی شبیه‌سازی و طراحی شبکه، بر اساس نظر خود بهره برده‌اند یعنی با اصلاح زیرساخت شبکه ایده ردیابی خود را مطرح کرده اند [۱۴]، هم هزینه مالی زیادی در بر دارد و هم هزینه زمانی و نیرو زیادی را می طلبد.

از دیگر روش‌های ردیابی آدرس آی پی، منبع حمله انکار سرویس، که مطرح است ردیابی از طریق بررسی اطلاعات جریان ترافیکی موجود در شبکه با استفاده از الگوریتم مورچگان می‌باشد. این روش نیازی به حمایت کامل مسیریاب‌ها نیز ندارد[۱۱].

الگوریتم‌های فرا ابتکاری محدودی در ردیابی آی پی مورد مطالعه قرار گرفته‌اند. الگوریتم‌های فرا ابتکاری به‌طور ذاتی برای پیدا کردن جواب بهینه قدرتمند هستند. ذات این الگوریتم‌ها، کشف غذا برای بقا است که اولین بار توسط آقای دوریگو [۱۳] در پایان‌نامه دکتری خود جهت یافتن کوتاه‌ترین مسیر از لانه تا منبع غذایی به-کار برده شده است.

از بین روش‌های فراابتکاری برای ردیابی حمله انکار سرویس فقط از کلونی مورچگان بهره برده شده است که آن‌هم به‌خاطر دو ویژگی ذاتی الگوریتم مورچگان، یکی فرا ابتکاری بودن و دیگری همگرایی سریع است که موجب کاربرد بیشتر این الگوریتم در مسیریابی‌های مختلف می‌شود. الگوریتم مورچگان از رفتار طبیعی مورچه‌ها الهام گرفته شده است [۱۹].

الگوریتم پیشنهادی هساین لای [۱۱] اولین کوشش در زمینه ردیابی حملات انکار سرویس به‌وسیله الگوریتم مورچگان بوده است، که در سال ۲۰۰۸ برای ردیابی با ترافیک بالا در نظر گرفته شده است و در توپولوژی ساده پیاده‌سازی شده که حملات تنها از گره کناری صورت می‌پذیرد. و به نتایج خوبی رسیده شده است.

همین‌طور بیشتر راهکارهای ارائه شده، برای شبکه‌های با حجم ترافیک بالا در نظر گرفته شده است. در [۱۲] با بهبود الگوریتم آقای هساین لای [۱۱] که به بررسی حمله از گره‌های کناری پرداخته شده، از کلونی مورچگان برای ردیابی حملاتی که مهاجم در یکی از مسیریاب‌های میانی یا کناری قرار گرفته است استفاده شده است. امّا در ردیابی حملات با حجم ترافیک پائین عاجز است.

چرا که شرط گره پایانی در الگوریتم [۱۲] برای ردیابی حملات با ترافیک پائین مناسب نیست. علاوه بر آن، تحلیل حملات با ترافیک پایین و بالا در [۱۵] انجام شده است، اما با این که این راهکار در صدد برطرف کردن نقص کارهای قبلی بوده است، ولی دارای نقاط ضعفی می‌باشد. از جمله این که درصد خطا و مثبت نادرست در ردیابی حملات با ترافیک پایین مطلوب نبوده است.

همچنین توسط نویسندگان این مقاله در [۱۶] به وسیله سطح جریان و در [۱۷] به‌وسیله واریانس جریان صورت پذیرفته است که شیوه‌های پیشنهادی آن قادر به ردیابی حملات با ترافیک پائین نیز می‌باشد.

دو خصیصه سرعت و دقت از مهم‌ترین اهداف الگوریتم‌های جستجوی فرا ابتکاری است. روش ارائه شده در این مقاله، دارای چند تفاوت اصلی با سایر کارها در این حوزه می‌باشد.

اول آنکه، امکان استفاده این روش برای حملات ترافیک با نرخ پایین وجود دارد. دوم، بالا بردن تعداد تکرار حلقه خارجی به‌عنوان شرط گره پایانی می‌باشد، که منجر به بالا بردن دقت می‌شود. سوم، تقویت جریان‌های محتمل‌تر است که منجر به پُررنگ کردن مسیر جریان حمله می‌شود. چهارم، حذف فضای جستجوی زائد که منجر به کاهش زمان اجرای الگوریتم می‌شود.که همه این موارد منجر به ردیابی با دقتی بسیار قوی‌تر نسبت به سایر روش‌ها می‌گردد.

نمای کلی این مقاله به این‌صورت است، که در بخش دو، مدل پیشنهادی مطرح می‌شود، در بخش سه، الگویتم بهینه شده ارائه می‌شود و در بخش چهار، شبیه‌سازی و نتایج آن شرح داده می‌شود و در انتها مقاله را با نتیجه‌گیری به پایان برده‌ایم.

۲. نمای کلی سامانه

الگوریتم کلونی مورچه الهام گرفته شده از مطالعات و مشاهدات روی کلونی مورچه‌هاست. این مطالعات، نشان داده که مورچه‌ها حشراتی اجتماعی هستند که در کلونی‌ها زندگی می‌کنند و رفتار آنها بیشتر در جهت بقای کلونی است تا درجهت بقای یک جزء از آن. یکی از مهم‌ترین و جالب‌ترین رفتار مورچه‌ها، رفتار آنها برای یافتن غذا است و به ویژه چگونگی پیدا کردن کوتاه‌ترین مسیر میان منابع غذایی و آشیانه. این نوع رفتار مورچه‌ها دارای نوعی هوشمندی توده-ای است که اخیراً مورد توجه دانشمندان قرار گرفته است.

در دنیای واقعی مورچه‌ها، ابتدا به‌طور تصادفی به این سو و آن سو می‌روند تا غذا بیابند. سپس به لانه بر می‌گردند و ردّی از فرمون به‌جا می‌گذارند. چنین ردهایی پس از باران به رنگ سفید در می‌آیند و قابل رویت اند. مورچه‌های دیگر وقتی این مسیر را می‌یابند، گاه پرسه‌زدن را رها کرده و آن را دنبال می‌کنند. سپس اگر به غذا برسند، به خانه بر می‌گردند و رد دیگری از خود در کنار رد قبل می-گذارند؛ و به‌عبارتی مسیر قبل را تقویت می‌کنند.

الگوریتم مورچگان اولین بار برای حل مساله فروشنده دوره گرد[1] معرفی شده است [۲۰] و سپس در بسیاری از مسائل بهینه‌سازی صدق کرده است. نظیر مسیریابی‌های وسایل نقلیه [۲۱ و۲۲] و مسیر یابی بین پُست‌های شبکه‌های توزیع برق ولتاژ بالا [۲۳] و بسیاری از مسیریابی شبکه‌های کامپیوتری [۲۴ و ۲۵] کاربرد دارد.

همچنین، بسیاری از زمان‌بندی منابع و سامانه‌های هوشمند از آن بهره برده‌اند. در این الگوریتم، مورچه‌ها با استفاده از ماده‌ای به‌نام فرمون[2]، که همان اثری است که مورچه‌ها هنگام حرکت بر جای می‌گذارند، به‌صورت غیر مستقیم ارتباط برقرار می‌کنند. که مشابه ردیابی منبع حمله است و اولین بار توسط آقای هسایین لای[3] جهت ردیابی حملات انکار سرویس، به‌کار برده شده است [۱۱].

هر جا که مورچگان بیشتری از یک دنباله پیروی کنند آن دنباله برای پیروی کردن مورچگان جذاب‌تر خواهد شد. در طرح پیشنهادی ردیابی آدرس آی پی، از میانگین تعداد بایت‌های متعلق به حمله انکار سرویس، به‌عنوان اثر فرمون استفاده می‌کنیم. بنابراین مسیریابی که ترافیک آن بیشتر و دارای جریان حمله انکار سرویس بیش‌تر است، مورچگان بیشتری آن مسیریاب را جهت پیمایش به گره بعدی انتخاب خواهند کرد؛ و این به‌شکل یک حلقه بازخورد مثبت خواهد بود و در نهایت اکثر مورچگان به یک مسیر برای پیمایش همگرا خواهند شد [۱۱]. فرومون به مرور تبخیر می شود که از سه جهت مفید است:

۱- باعث می‌شود مسیر جذابیت کمتری برای مورچه های بعدی داشته باشد. از آنجا که یک مورچه در زمان دراز راه‌های کوتاه تر را بیش‌تر می‌پیماید و تقویت می‌کند هر راهی بین خانه و غذا که کوتاه‌تر(بهتر) باشد بیشتر تقویت می‌شود و آنکه دورتر است کمتر.

۲- اگر فرمون اصلاً تبخیر نمی‌شد، مسیرهایی که چند بار طی می‌شدند، چنان بیش از حد جذّاب می‌شدند که جستجوی تصادفی برای غذا را بسیار محدود می‌کردند.

۳- وقتی غذای انتهای یک مسیر جذاب تمام می‌شود رد باقی نمی-ماند.

در حالت فرمت ابتدایی مورچه‌ها بر روی مسیریاب ابتدایی جای خواهند گرفت و مقدار دهی اولیه برای شدت دنباله فرمون در هر مسیریاب، تنظیم خواهد شد. زمانی که یک مورچه از یک هدف شروع می‌کند از اطلاعات توپولوژی برای پیدا کردن مسیریاب های همسایه استفاده می‌شود؛ و سپس به‌خواندن اطلاعات دنباله فرمون باقی مانده بر روی گره همسایه می‌پردازد تا احتمال هدف را محاسبه کند. سپس مسیریاب بعدی را با احتمالات به‌دست آمده برای پیمایش انتخاب می‌کند[۱۱].

از آنجایی که برخی از حملات انکار سرویس به‌صورت توزیع شده چندین جریان حمله را با ترافیک پایین از چندین مسیر به سمت سرویس دهنده یا طعمه می‌فرستند که مجموع این جریان‌ها با هم منجر به از بین رفتن منابع سرویس دهنده می‌شود لذا، ما برای اینکه بتوانیم اینگونه حملات با سطح ترافیک پایین را بیابیم می بایست گره‌های با سطح جریان عادی را نیز جستجو کنیم و با اضافه شدن گره‌ها با جریان عادی به فضای جستجو بر پیچیدگی مسئله افزوده شده و مهم‌تر از آن، می‌بایست شاخصی برای یافتن گره پایانی تعریف می‌کردیم.

گره جواب در روش قدیمی گره‌ای بود که بیشترین مورچه در آخر الگوریتم به آن همگرا شده هستند. به‌عبارتی گره‌ای که بیشترین تعداد مورچه در تکرار آخر به آن همگرا شده باشند، به‌عنوان جواب محسوب می‌گردید[۱۱]. اما در الگوریتم پیشنهادی ما گره‌ای است که بیشترین تعداد مورچگان، مجموعاً در کل دفعات تکرار الگوریتم آن را به‌عنوان گره پایانی و گره هدف معرفی کرده‌اند.

1- TSP
2- Pheromone
3- Hsin Lai

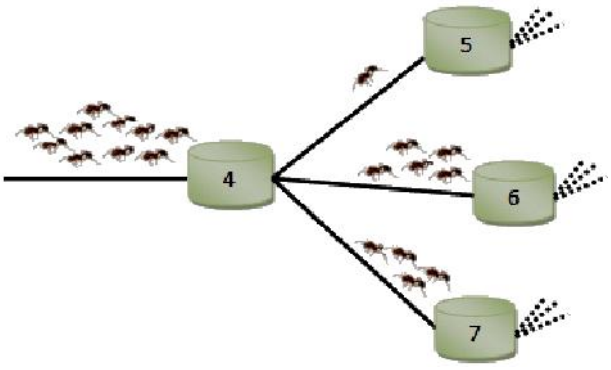
زمانی که تمام مورچه‌ها کاملاً مسیر خود را پیمایش کردند ما از اطلاعات به‌دست آمده از دنباله مورچگان برای بازسازی شدت دنباله فرمون استفاده می‌کنیم؛ و برای تشخیص منبع حمله با رسیدن هر مورچه به آخرین مسیریاب، یک واحد به شمارشگر آن مسیریاب اضافه می‌کنیم. اکنون، حلقه بعدی با شدت دنباله فرمون جدید شروع می‌شود. این عملیات، تا دفعات تکرار حلقه بیرونی الگوریتم و یا همگرایی اکثر مورچگان به یک هدف یکسان انجام می‌پذیرد.

زمانی که IDS یک حمله DoS که منبع خود را در شبکه دست‌کاری کرده، کشف کند به آنالیز بیش‌تر بسته‌های حمله DoS پرداخته و سپس لیستی از آدرس‌های آی پی منبع مشکوک را پیدا خواهد نمود. در مرحله اول، هر گره از شبکه از مقدار مجموع بایت-های فرستاده شده در زمان به‌عنوان و مقدار ابتدایی استفاده می‌کند. اطلاعات جریان برای تعیین احتمالی که مورچه یک مسیر انتخابی حرکت کند برگزیده می‌شود [۱۱]. تعیین احتمال از طریق فرمول (۱) انجام می‌پذیرد [۱۳] .

$$p_i(t) = \frac{[\tau_i(t)]^{\alpha} \cdot [f_i]^{\beta}}{\sum_{i \in \text{neighbor}} [\tau_i(t)]^{\alpha} \cdot [f_i]^{\beta}} \qquad (۱)$$

که Fi به مجموع بایت‌هایی گفته می‌شود که در زمان از مسیریاب شماره i فرستاده شده است؛ و $\tau_i(t)$ شدت دنباله فرمون مسیریاب i، در زمان t است. احتمال حرکت بعدی براساس اطلاعات جریان مسیریاب همسایه تعیین می‌گردد [۱۱].

در شکل ۱ مثالی آورده شده است. فرض را بر این داشته‌ایم که مجموع بایت‌های فرستاده شده از مسیریاب شماره ۵ برابر است با ۱۰۰۰ و از مسیریاب ۶ برابر با ۵۰۰۰ و از مسیریاب ۷ برابر با ۴۰۰۰ است.



شکل ۱. احتمال انتخاب مسیریاب بعدی [۱۱]

بنابراین احتمال انتخاب مسیریاب شماره ۵ برابر با ۱۰٪ می‌باشد و این احتمال برای مسیریاب ۶ برابر با ۵۰٪ و همچنین برای مسیریاب ۷ برابر با ۴۰٪ است. شدت دنباله فرمون بعد از اتمام مسیریابی کامل تمامی مورچگان از هدف تا مسیریاب نهایی اصلاح و بازبینی می‌شود. در شکل ۱ احتمال انتخاب مسیریاب بعدی آورده شده است.

در ردیابی روش سنتی[۱۱]، در صورت بروز حمله‌ای در گره‌های مجاور دچار اختلال گردیده جواب را به‌درستی اعلام نمی‌کند. در-صورتی که در روش بهبود یافته ردیابی حمله، با وجود دو جریان، حمله همزمان دیگر در گره‌های مجاور به‌درستی انجام شده است. همچنین در روش ردیابی مجموع جریان[۱۶] روش ردیابی واریانس جریان [۱۷] اگر ترافیک موجود بر روی یک مسیریاب به‌صورت اتفاقی خیلی بیشتر از سطح عادی باشد، ردیابی به‌سختی انجام می‌شود. که در روش بهبود یافته این مشکل نیز برطرف شده است.

۲.۱. افزایش تعداد دفعات تکرار حلقه بیرونی

در روش بهبود یافته، بر تعداد دفعات حلقه بیرونی نسبت به روش‌های واریانس جریان[۱۶] و مجموع جریان [۱۷] در حدود دو برابر افزوده شده است. متناظراً، زمان جستجو نیز بالا خواهد رفت.

برای رفع این ضعف فضای جستجو در روش بهبود یافته را کاهش داده‌ایم یعنی تنها گره‌هایی با سطح جریان نزدیک به ماکزیمم عادی مورد جستجو قرار می‌گیرند. همچنین این امر باعث می‌گردد تا از پیچیدگی مسئله کاسته شده است و از پراکندگی زیاد به‌خاطر افزایش جریان‌های عادی و جریان‌های نزدیک به‌حمله کاسته شده است؛ و در تمرکز به روی هدف به ما کمک شایانی کرده است.

افزایش تعداد دفعات تکرار باعث بالا رفتن دقت مسئله می‌شود؛ و با توجه به‌اینکه شرط انتخاب گره پایانی تعداد همگرایی کلی است و تعداد همگرایی در آخرین تکرار اجرای الگوریتم مد نظر نیست. این عمل به‌همراه بندهای زیرین مسبب جستجو دقیق‌تر می‌گردد. البته این امر منجر به بالا رفتن زمان اجرا می‌گردد. ولی از آنجا که میزان افزوده شدن زمان اجرا بسیار ناچیز است. قابل چشم‌پوشی است.

۲.۲. تقویت جریان در گره‌های محتمل‌تر

این کار دو مزیت دارد مزیت اول اینکه جریان حملات و جریان‌های ترافیک سطح بالاتر را به‌صورت دستی برجسته کرده و این کار باعث راحتی جستجو می‌شود. مزیت دوم اینکه با توجه به شرط انتخاب گره پایانی که تعداد همگرایی کلی است و تعداد همگرایی در آخرین تکرار اجرای الگوریتم مد نظر نیست.

خصیصه تقویت جریان گره‌های محتمل‌تر همراه با افزایش تعداد دفعات تکرار مسبب برجسته‌سازی و همگرایی بیشتر به گره‌های فعال در حمله به گره یک می‌گردد؛ و این امر باعث ردیابی دقیق‌تر و بهتر می‌گردد. حتی اگر حملاتی در گره‌های مجاور نیز رخ دهد و یا ترافیک جریان در گره‌ای بیش از حد عادی باشد. باز هم ردیابی به‌درستی نتیجه خواهد داد.

۳.۲. حذف فضای جستجوی زائد

به‌جای اینکه حد پایین ترافیک عادی را مورد جستجو قرار داده شود، گره‌ها با جریان نزدیک به ماکزیمم ترافیک در حالت عادی را به‌عنوان گره مجاز اعلام شده است. این کار دو مزیت زیر را در بر داشته است:

با کمتر شدن تعداد گره‌های مجاز به جستجو از فضای جستجو کاسته شده است. در نتیجه زمان اجرای الگوریتم نیز کاسته شده است.

با توجه به اینکه شرط انتخاب گره پایانی تعداد همگرایی کلی است و تعداد همگرایی در آخرین تکرار اجرای الگوریتم مد نظر نیست؛ و همچنین با توجه به اینکه تعداد دفعات تکرار افزوده شده است، اگر ترافیک عادی جریان به‌صورت لحظه‌ای یا کوتاه مدت در یکی از گره‌های مجاور بیشتر گردد، با انتخاب گره‌ها با جریان نزدیک به ماکزیمم ترافیک از برجسته‌سازی گره‌های غیر فعال در حمله جلوگیری کرده‌ایم؛ و این عمل مسبب تمرکز بیشتر به روی هدف شده است از پراکندگی و پیچیدگی مسئله کاسته می‌گردد. در نتیجه بر دقت ردیابی در نهایت افزوده شده است.

۳. الگوریتم بهبودیافته

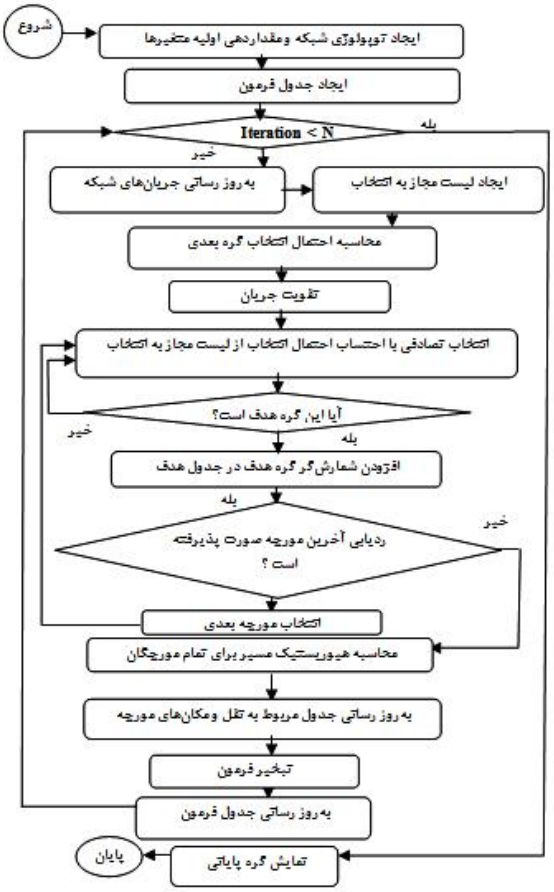
در واقع ما با سه تغییر زیر به بهبود هر چه بیش‌تر الگوریتم ردیابی مورچگان پرداختیم. ترکیب هر سه این تغییرات با هم نتایج قابل قبولی را در بر دارد.

۱- افزایش تعداد دفعات تکرار حلقه بیرونی

۲- تقویت جریان در گره‌های محتمل‌تر

۳- انتخاب گره‌ها با جریان نزدیک به ماکزیمم ترافیک در حالت عادی به‌عنوان گره مجاز.

الگوریتم از گره‌ای که مورد حمله قرار گرفته شروع می‌شود و مورچگان از این گره شروع به حرکت می‌کنند و جریان حمله را خوانده و به‌عنوان منبع غذایی شناسایی می‌کنند. و با برجاگذاری فرمون در روی مسیرهایی که بایت‌های حمله بیشتر است آن مسیر را جذاب‌تر برای دیگر مورچگان می‌کند. مورچه‌های دیگر، وقتی این مسیر را می‌یابند، گاه پرسه زدن را رها کرده و آن را دنبال می‌کنند. سپس اگر به غذا برسند به خانه بر می‌گردند و رد دیگری از خود در کنار رد قبل می‌گذارند؛ و به‌عبارتی مسیر قبل را تقویت می کنند. فلوچارت الگوریتم بهبود یافته در شکل ۲ آورده شده است.



شکل ۲ فلوچارت الگوریتم ردیابی بهبود یافته مورچگان

۴. بررسی عملکرد و شبیه‌سازی

ما با تقویت جریان در گره‌های محتمل‌تر گره‌های فعال در حمله را برجسته‌تر می‌نماییم؛ و این امر به ما در یافتن گره هدف علی‌رغم وجود جریان‌های ترافیکی بالا و نزدیک به جریان حمله کمک می‌کند. تقویت جریان به وسیله قطعه کد زیر انجام پذیرفته است.

توضیح اینکه ابتدا در حلقه اول میانگین جدول فرمون برای هر مسیریاب محاسبه می‌شود. که در سطرهای ۱ و ۲ و ۳ از قطعه کد شکل ۳ این عمل صورت می‌پذیرد. سپس برای هر مسیریاب آن مسیرهایی که جریان در آن بزرگ‌تر از میانگین فرمون است با انحراف معیار یا میزان اختلاف این دو جمع گردیده است؛

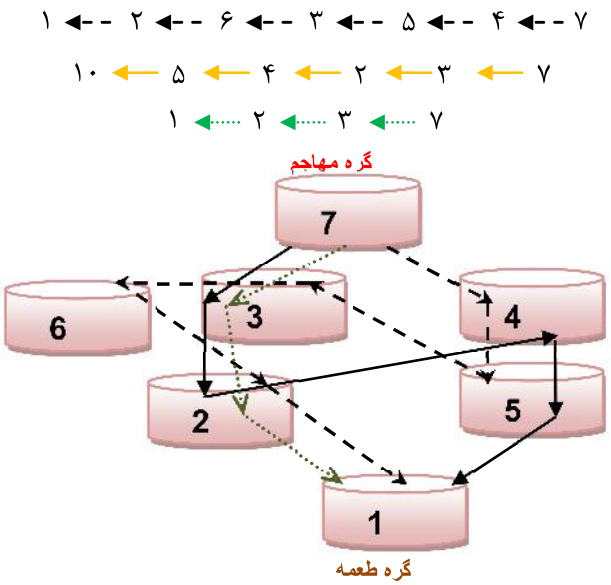
و این عمل موجب افزایش فرمون در این مسیرها شده است؛ و در واقع مسیر حمله برجسته تر شده است. شبه کد تقویت جریان در شکل ۳ آورده شده است.

```
for i=1 : n
avrage(i) = mean(Pheromonetable(i));
end
for i=1 : n
for j=1 : n
if  Pheromonetable(i,j) > avrage(i)
Pheromonetable(i,j)=((Pheromonetable(i,j)-  avrage(i))
+Pheromonetable(i,j));
end
end
end
```

شکل ۳. شبه کد تقویت جریان حمله انکار سرویس

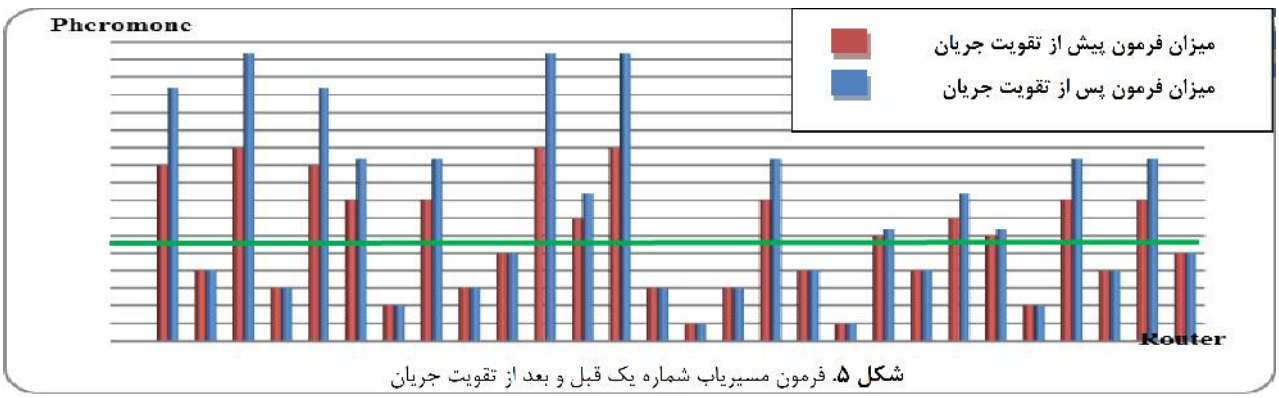
توپولوژی به‌کار رفته شده برای شبیه‌سازی، شبکه توری می‌باشد که از ۲۹ گره تشکیل شده است و علّت انتخاب آن به‌خاطر پیچیدگی شبکه توری و فضای جستجوی بسیار بالاتر نسبت به شبکه‌های ساده است که توانایی‌های الگوریتم پیشنهادی را نسبت به روش‌های قبلی نشان دهیم. برای بررسی عملکرد مسئله حمله‌ای از مسیری کوتاه‌تر را انتخاب نمودیم که مسیر حمله در شکل ۴ نمایش داده شده است.

گره ۷ به‌عنوان مهاجم و گره ۱ به‌عنوان گره طعمه است. حمله از سه مسیر مختلف برای بالا بردن پیچیدگی مسئله انتخاب شده است. همچنین ترافیک جریان حمله برای هر مسیر ۳۳۰ در نظر گرفته شده است. همچنین در هر بار تکرار حلقه بیرونی در الگوریتم ۳۳، جریان عادی در نظر گرفته شده است که با ترافیک بین ۱۱۰ تا ۱۵۰ با طول تصادفی به‌صورت تصادفی در بین دیگر گره‌ها، جریان داده شده است.



شکل ۴. سه مسیر حمله از گره ۷ به گره ۱ در روش بهبود یافته

برای مثال در شکل ۵ گره‌های برجسته شده از مسیریاب یک نمایش داده شده است. که نمودار قرمز رنگ متعلق به پیش از تقویت جریان است و نمودارهای آبی رنگ، بیانگر بعد از اجرای قطعه کد تقویت جریان است. میانگین فرمون برای مسیریاب یک، برابر ۵/۶۲ می‌باشد. پس مسیرهایی که فرمون آنها بیشتر از ۵/۶۲ است می‌بایست با انحراف معیار جمع گردند. این تقویت جریان موجب برجسته‌سازی این مسیرهای محتمل‌تر خواهد شد؛ و این عمل قدرت ردیابی را افزایش می‌دهد. در شکل ۵، عدد ۵/۶۲ با خط سبز نمایش داده شده است. مشاهده می‌نمایید که مسیرهایی که فرمون بیش تر از خط سبز هستند با انحراف معیار جمع گردیده و موجب برجسته‌سازی این مسیرها در جدول فرمون شده است.

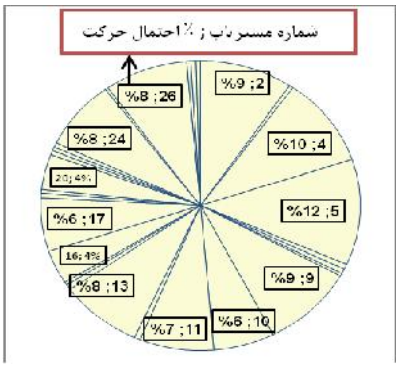


شکل ۵. فرمون مسیریاب شماره یک قبل و بعد از تقویت جریان

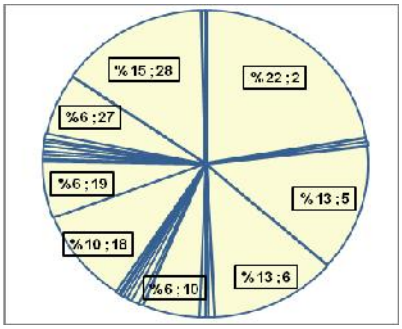
در شکل ۶، احتمال حرکت از مسیریاب طعمه در تکرار اول نشان داده شده است. روشن است که به‌دلیل وجود جریان‌های عادی زیادتر و حتی جریان‌های نزدیک به حمله احتمال حرکت به سمت گره هدف بسیار پیچیده و مشکل است. عملیات تقویت جریان پس از تکرار اول در حلقه بیرونی صورت می‌پذیرد؛ لذا پراکندگی و پیچیدگی حرکت در تکرار اول بسیار بالاست.

اما در تکرارهای بعدی به‌علت تقویت جریان و تغییراتی نظیر بالا بردن تعداد تکرار حلقه بیرونی و صافی کردن گره‌های غیر محتمل تا حد نسبتاً بالا از این پراکندگی کاسته می‌شود. که در شکل ۷، برای تکرار سوم و شکل ۸، برای تکرار یازدهم و در شکل ۹ برای تکرار بیست و دوم و در نهایت در شکل ۱۰، برای تکرار چهل و چهارم نمایش داده شده است.

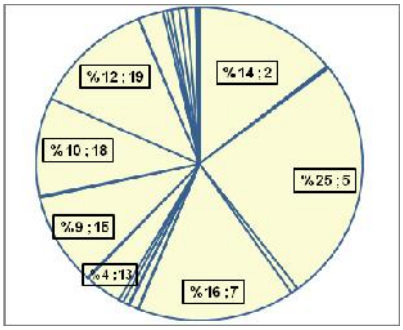
با مشاهده شکل ۶ و شکل ۷ نقش مؤثر تقویت فرمون روشن است. که تعداد گره‌های با احتمال بالا حرکت کاسته شده است. با توجه به شکل ۴، مسیر معکوس حمله، عبور از گره یک به گره‌های دو و پنج است. پس در ردیابی بازگشتی درست، می‌بایست احتمال حرکت به این دو گره بیشتر از بافی گره‌ها باشد. لازم به‌ذکر است که نتیجه الگوریتم ما نیز همگرایی به این دو گره است و احتمال حرکت مورچه از گره ۱ به گره‌های ۲ و ۵، به‌عنوان گره‌های فعال در حمله، بیش‌تر از بقیه گره‌هاست؛ و این نقش تعیین کننده‌ای در حرکت مورچگان به سمت هدف و گره مهاجم داراست. در شکل ۸ مشاهده می‌کنید که گره ۵ محتمل‌ترین گره برای انتخاب بعدی است؛ و گره ۲ پس از گره ۷ سومین گره محتمل‌تر برای انتخاب است. گره هفتم اگرچه در این تکرار به‌عنوان گره دوم محتمل‌تر نشان داده شده است ولی با نگاهی به شکل ۶ می‌بینیم که در آنجا به‌عنوان گره‌ای با احتمال انتخاب بسیار پایین یک درصد نمایش داده شده است. که به‌علت حضور غیر دائمی به‌عنوان گره‌های محتمل، جواب کلی مسئله را به‌سمت گره‌های با حضور دائمی سوق خواهد داد.



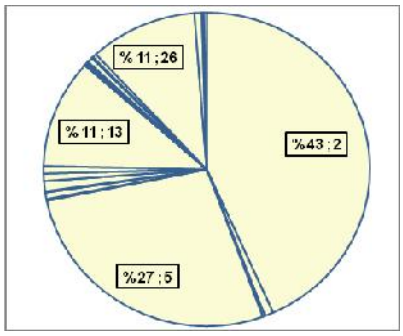
شکل ۶. احتمال حرکت از مسیریاب یک در تکرار اول در روش بهبودیافته



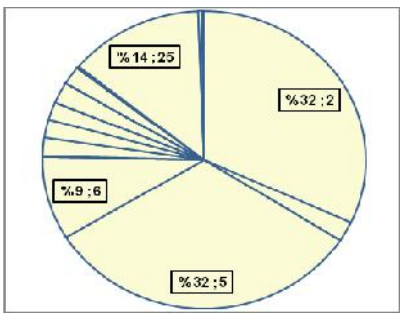
شکل ۷. احتمال حرکت به گره بعدی از مسیریاب یک در تکرار سوم در روش بهبود یافته



شکل ۸. احتمال حرکت به گره بعدی از مسیریاب یک در تکرار یازدهم در روش بهبود یافته



شکل ۹. احتمال حرکت به گره بعدی از مسیریاب یک در تکرار بیست و دوم در روش بهبودیافته



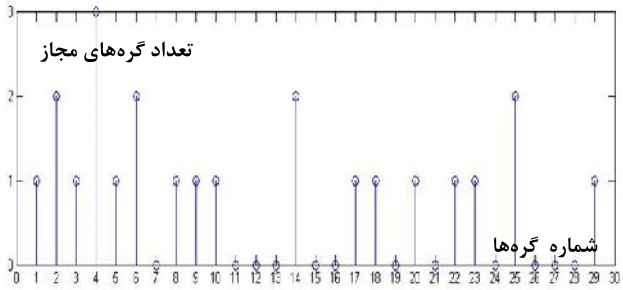
شکل ۱۰. احتمال حرکت به گره بعدی از مسیریاب یک در تکرار چهل و چهارم در روش بهبودیافته

با توجه به شکل‌های۵ تا ۱۰ مشاهده می‌شود که گره‌های ۲ و ۵ که به‌عنوان گره‌های موجود در مسیر حمله به یک هستند همواره در همه تکرارها، به‌عنوان گره‌های محتمل حضور دارند و رفته رفته با تکرارهای متوالی‌تر حضور آن‌ها نیز پر رنگ‌ترمی‌گردد. اما گره‌های محتملی که در مسیر حقیقی حمله قرار ندارند دوام چندانی نداشته و گذرا هستند و حتی همین حضور گذرای این‌ها نیز در بین گره‌های محتمل به خاطر واگرایی مسئله و جستجو در بین گره‌ها با سطح جریان حضور دارند و رفته رفته با تکرارهای متوالی‌تر حضور آن‌ها نیز پر رنگ‌ترمی‌گردد، اما گره‌های محتملی که در مسیر حقیقی حمله قرار ندارند دوام چندانی نداشته و گذرا هستند و حتی همین حضور گذرای این‌ها نیز در بین گره‌های محتمل به خاطر واگرایی مسئله و جستجو در بین گره‌ها با سطح جریان عادی است. تقویت جریان در برجسته‌سازی این مسیرها نقش بسزایی داشته است به گونه‌ای که ما بدون تقویت جریان هرگز به چنین تغییری دست نمی‌یافتیم.

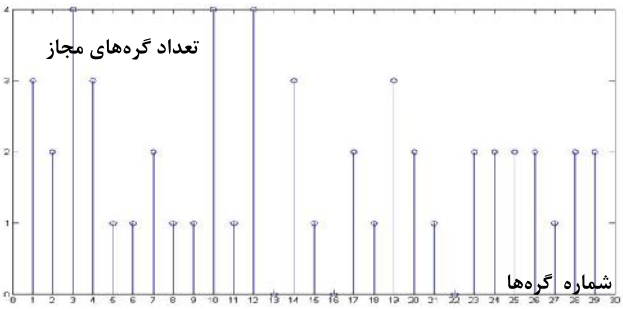
برای انتخاب گره‌های مجاز نیز می‌توانیم هم به روش مجموع جریان ترافیکی و هم واریانس جریان ترافیکی استفاده نمود. برای بهبود انتخاب گره پایانی نیز به‌جای اینکه کمینه یا حد پایین جریان عادی را جستجو کنیم. جریان‌های نزدیک به ماکزیمم جریان عادی را مجاز به جستجو کرده‌ایم؛ و با این عمل فضای جستجوی را به میزان قابل قبولی کاهش داده‌ایم.

به‌عنوان نمونه حرکت‌های مجاز در تکرار اول و سوم به‌ترتیب در شکل ۱۱ و شکل ۱۲ نمایش داده شده است. که در تکرار اول مجموع کل حالت‌های مجاز برابر ۲۳ شده است. بدین معنی که از ۸۱۲ حالت ممکن (۲۹ گره که به‌صورت توری به هم متصل شده است یعنی ۸۱۲ = ۲۸×۲۹ حالت ممکن در جستجو) تنها ۲۳ مورد (مجموع تعداد گره‌های مجاز که در شکل ۱۰ نشان داده شده است) یعنی ۰/۰۲۸ از حالات ممکن تنها جستجو شده است در حالی که تعداد جریان‌های عادی را برابر با ۲۱ مورد قرار داده‌ایم. همچنین یک جریان حمله با ترافیک ۲۷۰ نیز در مسیر جاری ساختیم. تقریباً یک چهارم از فضای جستجو نسبت به‌روش غیر بهبود یافته از فضای جستجو کاسته شده است. که تأثیر بسزایی در کاهش زمان جستجو نیز دارا است.

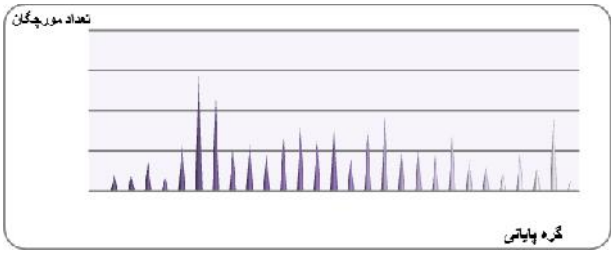
همچنین با توجه‌به ویژگی بازگشتی الگوریتم با کمتر شدن فضای جستجو رفته رفته به‌جایی می‌رسیم که دیگر گره‌ای مجاز برای جستجو باقی نمی‌ماند. گره جواب، گره‌ای است که در پایان الگوریتم بیشترین تعداد مورچگان آن را به‌عنوان گره پایانی و گره هدف در مجموع کل تکرارها معرفی کرده‌اند. که در شکل ۱۳ در پایان الگوریتم برای مجموع پنجاه و پنج تکرار نشان داده شده است که گره هفتم با مجموع تعداد ۱۵۴ مورچه به‌عنوان گره جواب به‌درستی انتخاب شده است. در شکل ۱۴ نمودار تغییرات دقت متناسب با افزایش تغییر دفعات تکرار حلقه خارجی برای روش بهبودیافته آورده شده است. مشاهده می‌فرمایید که نقطه کمینه دقت، برابر با ۰/۷ است. همچنین با افزایش تعداد تکرار حلقه خارجی دقت نیز افزایش داشته است. این افزایش دقت تا تکراری خاص صورت پذیرفته است و پس از آن نوسانات، تقریباً ثابت شده است.



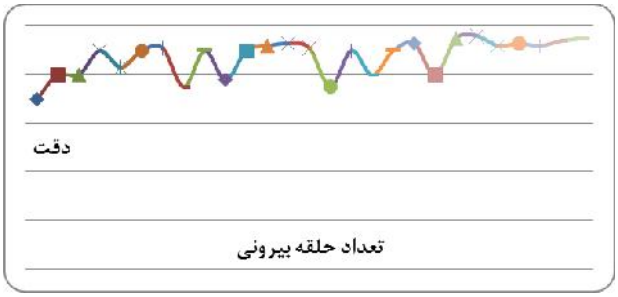
شکل ۱۱. تعداد گره‌های مجاز در تکرار اول در روش بهبودیافته



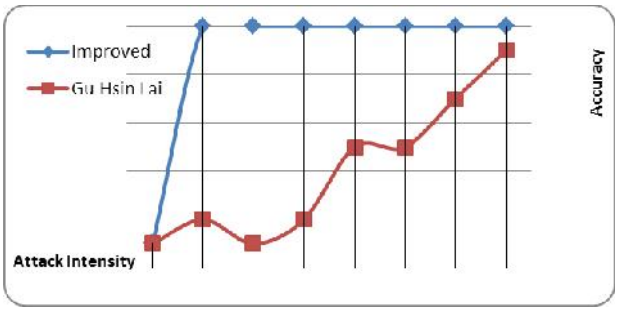
شکل ۱۲. تعداد گره‌های مجاز در تکرار سوم در روش بهبودیافته



شکل ۱۳. گره‌های جواب در مجموع پنجاه و پنج تکرار در روش بهبودیافته



شکل ۱۴. نمودار تغییرات دقت با تغییر تکرار حلقه خارجی در روش بهبودیافته



شکل۱۵. نمودار تغییرات دقت با تغییر تکرار حلقه خارجی در روش بهبودیافته و روش آقای هسین لای

از نظر دقت الگوریتم در ردیابی مهاجم الگوریتم بهبودیافته بسیار قوی‌تر از الگوریتم آقای هسین لای عمل کرده است. که در شکل ۱۵ مشاهده می‌فرمائید. مزیت‌های روش بهینه بر روش الگوریتم مورچگان آقای هسین لای[۱۱] به‌صورت خلاصه در زیر آورده شده است.

افزایش تعداد دفعات تکرار حلقه بیرونی با توجه به شرط گره پایانی جدید، این عمل باعث بالا رفتن دقت مسئله و همچنین افزوده شدن فضای جستجو می‌شود؛ و با توجه به اینکه شرط انتخاب گره پایانی تعداد همگرایی کلی است و تعداد همگرایی در آخرین تکرار اجرای الگوریتم مد نظر نیست. این عمل به‌همراه بندهای زیرین مسبب جستجو دقیق‌تر می‌گردد. البته این امر منجر به بالا رفتن زمان اجرا می‌گردد. ولی از آنجاکه میزان افزوده شدن زمان اجرا، بسیار ناچیز است. قابل چشم‌پوشی است.

تقویت جریان در گره‌های محتمل‌تر: این کار دو مزیت دارد: جریان حملات و جریان‌های ترافیک سطح بالاتر را، به‌صورت دستی برجسته کرده و این کار باعث راحتی جستجو می‌شود. با توجه به اینکه شرط انتخاب گره پایانی تعداد همگرایی کلی است و تعداد همگرایی در آخرین تکرار اجرای الگوریتم مد نظر نیست. خصیصه تقویت جریان گره‌های محتمل‌تر همراه با افزایش تعداد دفعات تکرار مسبب برجسته‌سازی و همگرایی بیشتر به گره‌های فعال در حمله به گره یک می‌گردد؛ و این امر باعث ردیابی دقیق‌تر و بهتر می‌گردد.

حتی اگر حملاتی در گره‌های مجاور نیز رخ دهد و یا ترافیک جریان در گره‌ای بیش از حد عادی باشد. باز هم ردیابی به‌درستی نتیجه خواهد داد. انتخاب گره‌ها با جریان نزدیک به بیشینه ترافیک در حالت عادی به‌عنوان گره مجاز: به‌جای اینکه حد پایین ترافیک عادی را مورد جستجو قرار داده شود، گره‌ها با جریان نزدیک به بیشینه ترافیک در حالت عادی را به‌عنوان گره مجاز اعلام شده. این کار، دو مزیت زیر را در بر داشته است. با کمتر شدن تعداد گره‌های مجاز به جستجو از فضای جستجو کاسته شده است. در نتیجه زمان اجرای الگوریتم نیز کاسته شده است. با توجه به اینکه شرط انتخاب گره پایانی تعداد همگرایی کلی است و تعداد همگرایی در آخرین تکرار اجرای الگوریتم مد نظر نیست؛ و همچنین با توجه به اینکه تعداد دفعات تکرار افزوده شده است.

اگر ترافیک عادی جریان به‌صورت لحظه‌ای یا کوتاه مدت در یکی از گره‌های مجاور بیشتر گردد. با انتخاب گره‌ها با جریان نزدیک به ماکزیمم ترافیک در حالت عادی ما از برجسته‌سازی گره‌های غیر فعال در حمله جلوگیری کرده‌ایم؛ و این عمل مسبب تمرکز بیشتر به روی هدف شده است از پراکندگی و پیچیدگی مسئله کاسته می‌گردد. در نتیجه بر دقت ردیابی در نهایت افزوده شده است.

۵. نتیجه‌گیری

حملات انکار سرویس با ترافیک پایین عمده‌ترین نوع حملات انکار سرویس است؛ و شناسایی و ردیابی آن‌ها به نسبت دشوارتر است. در ردیابی به کمک الگوریتم مورچگان از راهکار برگشت به مهاجم استفاده می‌شود و از سطح جریان برای ردیابی منبع حمله انکار سرویس استفاده شده است. ما در این تحقیق، به بهبود ردیابی الگوریتم مورچگان پرداخته‌ایم. ما با تقویت جریان‌های محتمل‌تر و ارائه روش جدیدی در جستجو و انتخاب گره هدف، موفق به بهبود این الگوریتم شده‌ایم. نتایج شبیه‌سازی شده نشان می‌دهد که راهکار پیشنهادی می‌تواند حمله‌ها را حتی اگر شدت ترافیک حمله بسیار کم باشد، به‌درستی ردیابی کند.

همچنین با توجه به نتایج حاصله از شبیه‌سازی ردیابی حمله در کنار دو جریان حمله در گره‌های مجاور در شبکه موفقیت آمیز بوده است؛ و قدمی جدید در عرصه ردیابی حملات به کمک الگوریتم‌های فرا ابتکاری جهت ردیابی حملات انکار سرویس توزیع شده محسوب می‌شود. اگرچه ردیابی حملات انکار سرویس با توزیع بالا هنوز میسر نگشته است ولی این امر، ما را به ردیابی این دسته از حملات به‌روش الگوریتم مورچگان نزدیک‌تر ساخته است. نیاز است که سرمایه‌گذاری بیش‌تری بر روی الگوریتم مورچگان و یا تولید دیگر روش های هوش مصنوعی برای مسائل مربوط به ردیابی آی پی صورت پذیرد و یا حملات انکار سرویس با توزیع بیشتر را بررسی نمود. مدیریت جریان می‌تواند برای شبکه‌های بزرگ مقیاس‌پذیرتر باشد. علاوه بر این مطالعات عملی برای پیاده‌سازی و گسترش در شبکه‌های بزرگ می‌تواند برای ارزیابی مقیاس‌پذیری این راه‌حل پیشنهادی صورت بپذیرد.

۶. مراجع

[1] Anstec. D, "DDoS Attack Trends Through 2010," 6th Annual Survey Infrastructure Security Report & ATLAS Initiative, 2010.

[2] Shinoda. Y, "What's happening out there? Global Information Security Threats Trend(2012)," in Proc. Cryptrec Symposim 2012, 9 March 2012.

[3] Lu. K, Wu. D, Fan. J, Todorovic. S, Nucci. A, "Robust and efficient detection of DDoS attacks for large-scale internet," Computer Networks vol. 51, pp. 5036-5056, 31 August 2007.

[4] Park. K, Lee. H, "On the efectiveness of route-based packet filtering for distributed dos attack prevention in power-law internets,"in Proc. of ACM SIGCOMM, 2001.

[5] Ferguson. P, Senie. D, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," RFC 2267 Report, 1998.

[6] Chen. S, Song. Q, "Perimeter-based defense against high bandwidth DDoS attacks," IEEE Transaction. Parallel Distribut System. Vol. 16 (6), pp. 526–537, 2005.

[7] Shahzad. A, Naseem. R, Aadil. F, Khayyam. Sh, "Trends in defensive techniques against Denial of Service (DoS) Attacks," Canadian Journal on Network and Information Security, vol. 1, no. 1, April 2010.

[8] Aljifri. H, Smets. M, Pons. A, "IP traceback using header Compression," Computers & Security, vol. 22(2), pp. 136-151, 2003.

[9] Soneren. A, Partridge. C, Sanchez. A, Jones. E, Tachakountio. F, B. Schwartz, et al., "Single-packet IP traceback," IEEE/ACM, Transactions on Networking, vol. 10(6), pp. 721-734, 2002.

[10] Baba. T, Matsuda. S, "Tracing network attacks to their sources," IEEE Internet Computing, vol. 6(3), pp. 20-26, 2002.

[11] Hsin Lai. G, Chen. Ch, Chiang Jeng. B, Chao. W, "Ant-based IP traceback," Expert Systems with Applications vol. 34 pp. 3071-3080, 2008.

[12] Hamedi- Hamzekolaie. M, Ghaznavi- Ghushchi. M. B, Shamani. M. J, IP Tracing the source of denial of service attacks using Genetic Algorithm, 5th Iran Electronic Warfare Conf, Imam Hossein University, 2013 (In Persia)

[13] Dorigo. M, "Optimization, Learning and Natural Algorithms," PhD thesis, Politecnico di Milano, Italie, 1992.

[14] Goodrich. M, "Probabilistic packet marking for large-scale IP traceback," IEEE/ACM Transactions on Networking, vol. 16, pp. 15-24, 2008.

[15] Chen. H, Yang. W, "The Design and Implementation of a Practical Meta-Heuristic for the Detection and Identification of Denial-of-Service Attack Using Hybrid Approach," in Proc. Second International Conference on Machine Learning And Computing, Feb 2010.

[16] Hamedi-Hamzehkolaie. M, Shamani. M. J, M.B. Ghaznavi -Ghoushchi, "Low Rate DOS Traceback Based On Sum of Flows," in Proc. the Sixth International Symposium On Telecommunication(IST 2012), 2012.

[17] Hamedi-Hamzehkolaie. M, Shamani. M. J, Ghaznavi-Ghoushchi. M. B, "Ant colony traceback for low rate DOS attack," IJCA Special Issue on Computational Intelligence & Information Security CIIS vol.1, pp.22-26,2012.

[18] Kumarasamy. S, Asokan. R, "DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS DETECTION MECHANISM,"International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol. 1, no.5, December 2011.

[19] Adesina Anifowose. F, Ibiyemi Eludiora. S, "Application of Artificial Intelligence in Network Intrusion Detection,"A Succinct Review World Applied Programming, vol. 2, no. 3, pp. 158-166, March 2012.

[20] Dorigo. M, Gambardella. L. M, "Ant Colony System : A Cooperative Learning Approach to the Traveling Salesman Problem," IEEE Transactions on Evolutionary Computation, vol1, no. 1, pp. 53-66, 1997.

[21] Toth. P, Vigo. D, "Models, relaxations and exact approaches for the capacitated vehicle routing problem," Discrete Applied Mathematics, vol.123, pp. 487-512, 2002.

[22] Donati. A. V, Montemanni. R, Casagrande. N, Rizzoli. A. E, Gambardella. L. M, "Time Dependent Vehicle Routing Problem with a Multi Ant Colony System," European Journal of Operational Research, vol. 185, no. 3, pp. 1174–1191, 2008.

[23] Zhang. J, Chung. H, Lo. W. L, Huang. T, "Extended Ant Colony Optimization Algorithm for Power Electronic Circuit Design," IEEE Transactions on Power Electronic, vol.24, no.1, pp. 147-162, Jan 2009.

[24] Caro. G. D, Dorigo. M, "Extending AntNet for best-effort quality-of-service routing," in Proc. the First Internation Workshop on Ant Colony Optimization (ANTS'98), 1998.

[25] Caro. G. D, Dorigo. M, "Two ant colony algorithms for best-effort routing in datagram networks," in Proc. the Tenth IASTED International Conference on Parallel and Distributed Computing and Systems (PDCS'98), pp. 541-546, 1998.