مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۱، بهار ۱۳۹۷، ص ۸۶-۶۹

تخمین شبکه بات با استفاده از سرورهای نیابتی در حملات منع خدمت توزیع‌شده

حمید اکبری[۱]*، سید مصطفی صفوی همامی[۲]

۱- دانشجوی دکتری، دانشگاه جامع امام حسین (ع) ۲- دانشیار، دانشگاه صنعتی امیرکبیر

(دریافت: ۹۵/۰۸/۲۵، پذیرش: ۹۶/۰۲/۱۱)

چکیده

رصد حملات منع سرویس توزیع‌شده که توسط شبکه‌های بات صورت می‌گیرد، کماکان دارای چالش‌های عدم قطعیت در حین حمله است. در این پژوهش روشی پیشنهاد شده است که شبکه بات، کسری از بسته‌های حمله را به سمت میزبان‌های خودی (حسگر نیابتی) در اقصی نقاط شبکه ارسال کنند و سپس داده حسگرهای نیابتی را ادغام کرده تا برآوردی از قدرت شبکه بات حاصل شود. منابع عدم قطعیت اعم از وجود فیلترینگ دفاعی (محلی و منطقه‌ای)، خرابی حسگرها و گم‌شدن بسته‌ها می‌تواند موجب مخدوش‌شدن تخمین قدرت شبکه بات شود. از این‌رو، در دو مرحله، طرح پیشنهادی در شرایط عدم قطعیت، به‌صورت تک‌حسگر و چندحسگر نیابتی مورد مدل‌سازی قرار گرفت. سپس با استفاده از شبیه‌ساز آمنت، مدل پیشنهادی با استفاده از سه سناریو تحت آزمایش قرار گرفت و نتایج آن در قالب شاخص‌های نرخ دریافت بسته، درصد اشغال پهنای باند، تاخیر زمان پاسخگویی قربانی و زمان نرخ گم‌شدن بسته‌ها، اندازه‌گیری و مورد تجزیه و تحلیل قرار گرفت. همچنین، از داده‌های تولیدشده توسط شبیه‌ساز برای مرحله تلفیق داده استفاده گردید. در ادامه پژوهش، برای ادغام داده از روش‌های رأی‌گیری بیشینه، کمینه و متوسط‌گیری بهره گرفته شد و نتایج با استفاده از روش اقلیدسی مورد مقایسه و ارزیابی قرار گرفت و نشان داد که روش کمینه بیشینه (مین ماکس) در شرایط فوق دارای دقت ۹۵ ٪ است. آزمایش فوق در محیط اینترنت با بهره‌مندی از بسته‌های علامت‌دار، نشان داد که روش بیشینه از دقت ۹۶ درصدی برخوردار است. در نهایت، طرح پیشنهادی اثبات کرد که می‌توان قدرت شبکه بات را حین حمله، به‌وسیله میزبان‌های خودی (نیابتی) و ادغام اطلاعات آن‌ها اندازه‌گیری کرد.

واژه‌های کلیدی: بات نت، سرور نیابتی، ادغام داده، شبکه حسگری سایبری، عدم قطعیت، فیلترینگ، حملات منع خدمت توزیع‌شده

۱- مقدمه

شبکه بات مجموعه‌ای از میزبان‌های آلوده است که تحت کنترل مهاجم، برای مقاصد گوناگونی ازجمله حمله منع خدمت توزیع‌شده[۱]، بر روی میزبان‌های قربانی مورد استفاده قرار می‌گیرند [۱]. بخش فرماندهی و کنترل شبکه بات وظایفی ازقبیل حضوروغیاب و دستور برای اجرای اقدام به بات‌ها را به‌عهده دارد. همواره تخمین اندازه، جمعیت و رفتار بات‌ها مورد توجه مهاجمین و محققین بوده است و می‌توانند قبل از حمله، حضور زنده آن‌ها را در کانال فرمان و نیز ردگیری از طریق DNS رصد کنند [۲]. مهاجم به فرمانی که به بات‌ها داده است، آگاه می‌باشد ولیکن چالش اصلی این است که از اقدام واقعی آن‌ها و رسیدن بسته‌های حمله به سمت قربانی با وجود فیلترینگ، ازکارافتادن و یا عقیم‌شدن شبکه بات در حین حمله آگاهی نداشته و برای هدایت بات‌ها با شرایط عدم قطعیت مواجه است [۳]. این پژوهش با ارائه پیشنهادهایی درصدد کاهش عدم قطعیت و افزایش آگاهی از وضعیت شبکه بات می‌باشد. روش تحقیق مبتنی‌بر مدل‌سازی و شبیه‌سازی طرح، در محیط شبیه‌ساز و محیط اینترنت می‌باشد. ساختار این پژوهش در هفت فصل شامل مقدمه، کارهای انجام‌گرفته، طرح پیشنهادی، شبیه‌سازی و ارزیابی طرح در محیط شبیه‌ساز، آزمایش طرح در محیط واقعی اینترنت، نتیجه‌گیری نهایی و مراجع ارائه شده است.

۲- کارهای مرتبط

در مرجع [۴]، کریستین برای اندازه‌گیری انتشار بات‌نت‌ها (میزان مخاطره آن‌ها)، معیارهایی را معرفی کرده و آن‌ها را با مدل

* رایانامه نویسنده مسئول: kphakbari@ihu.ac.ir

1- Distributed Denial of Service (DDoS)

پیشنهادی خود تبدیل به یک رابطه ریاضی نموده است. او ۱۷ نوع شبکه‌بات متداول دنیا را با استفاده از مدل خود مورد سنجش و مقایسه قرار داده است. معیارهای پیشنهادی شامل تعداد بات‌های شبکه، شیوه آلوده‌سازی، پنهان ماندن، میزان فعالیت، انعطاف‌پذیری، ارزشمندی اهداف مورد حمله و خسارات مالی می‌باشد که ملاک ارزیابی ایشان است. در مرجع [۵]، ایگور کوتنکو و همکاران، چارچوبی را در محیط شبیه‌ساز آمنت[1] طراحی کردند که بتوان شبکه بات و روش‌های دفاعی در برابر حمله منع خدمت را در سطح بسته آزمایش کرد. در این طرح، تیم‌های مهاجم مبادرت به حمله کرده و مدافع با سیستم‌های دفاعی خدمات‌دهندگان محلی و منطقه‌ای دفاع می‌کند. وی با اجرای چند سناریو نشان داد که اگر خدمات‌دهندگان بتوانند با یکدیگر همکاری کنند و در مرحله اول، حمله را تشخیص داده و در مراحل بعدی اقدام به فیلتر کنند، می‌توانند نقش به‌سزایی در کاهش حمله به قربانی را داشته باشند. در مرجع [۶]، ایگور کوتنکو تلاش کرده تا هستان‌شناسی[2] از حملات و روش‌های دفاعی در برابر حملات منع خدمت در سطح بالا را ارائه دهد. سپس، فرآیند کلی حمله منع خدمت را در سه سطح مختلف (بالایی، میانی و پایین) بیان کرد. به‌طوری‌که آن‌ها را در سه مرحله مقدماتی، اصلی و پایانی دسته‌بندی نموده و جزئیات فعالیت‌های هر یک را به‌صورت سلسله مراتبی نشان داده است. در ادامه، شبیه‌سازی حملات را با تسخیر میزبان‌ها و نصب عامل-ها و مصورسازی ایجاد حمله (با پارامترهای مختلف) نشان داده است. با پارامترهایی چون میزان دانش نفوذگر (درباره شبکه قربانی)، میزان حفاظت در برابر حمله، نتایج معناداری را ارائه داده است. تلاش شده است اقدامات مهاجم در هریک از مراحل حمله، به‌صورت مصور نمایش داده شود. در مرجع [۷]، سایریل بن‌وارت ادعا کرده است که می‌توان از راه دور بدون نصب ابزاری در ماشین قربانی، مبادرت به اندازه‌گیری اثر حمله منع خدمت کرد. او در محیط آزمایشگاه نشان داد که حمله فلش کرود بر روی دو معیار گذردهی مفید (داخلی) و زمان رفت‌وبرگشت درخواست و پاسخ (خارجی) تأثیرگذار است و ضریب همبستگی مثبتی بین آن‌ها وجود دارد. در مرجع [۸]، محب ابو رجب و همکاران وی به‌دنبال ارائه معیاری می‌باشند تا بتوانند بزرگی شبکه بات را تخمین بزنند. چالش‌هایی چون مهاجرت موقت و ساختار مخفی بات‌نت‌ها، دقت اندازه‌گیری را مخدوش کرده است.

ایشان چالش‌های تخمین شبکه بات را با استفاده از تغییر در مسیر DNS مورد بررسی قرار داده است. سپس، نویسنده با استفاده از زیرساخت توزیع‌شده‌ای مبادرت به ردگیری و جمع‌آوری داده در یک دوره ۹ ماهه و ثبت رفتار بات‌نت‌ها نموده است. در نتایج اولیه از یک میلیون جمعیت در شبکه بات، فقط ۴۰۰ IP آدرس رؤیت شده بود که مربوط به آدرس‌دهی‌های پویا بوده و این در حالی است که حدود ۸۰۰ هزار بات در DNS فعالیت داشته‌اند و نیز حدود ۱۱ ٪ آن‌ها با سایر بات‌نت‌ها با یکدیگر هم‌پوشانی داشته است. همچنین، حدود ۴۸ ٪ بات‌نت‌ها ثبت نشدند. با توجه به مغایرت‌های به‌وجودآمده، نمی‌توان به آمار ثبت‌شده DNS اطمینان کرد و به جمعیت واقعی بات‌ها پی برد. در مرجع [۹]، پینگ وانگ و همکاران، طرحی پیشنهاد کردند تا بات‌نت‌ها به‌راحتی توسط بات‌های ارشد[3] قابل مانیتورکردن باشند. همچنین، مانیتورکردن برای مدافعان را سخت کند و از خود مقاومت نشان دهد و هم‌زمان جهت اجرای حملات مؤثرتر، اطلاعات دقیقی از بات‌نت‌ها از قبیل جمعیت بات‌ها، توزیع آن‌ها، پهنای باند، وضعیت روشن یا خاموش‌بودن آن‌ها، انواع آدرس IP و... توسط بات ارشد جمع‌آوری گردد. همچنین، هنگامی‌که بات-نت‌ها با انواع ضدحملات از طرف مدافعان مواجهه هستند، بتوانند آن‌ها را حفظ و کنترل نمایند. در روش پیشنهادی، دستورات متفاوتی از سمت حسگرهای میزبان صادر می‌شود و از این‌رو امکان کشف بات‌های ارشد و بات‌های معمولی بسیار کم می‌شود. لذا با استفاده از خدمات‌دهنده‌هایی مانند وب یا رایانامه بتوانند کار گزارش‌دادن به حسگرها را انجام دهند و بدین‌صورت از ترافیک غیرطبیعی شبکه جلوگیری کنند. همچنین، به‌جای استفاده از یک حسگر، از چند میزبان حسگر که دارای قابلیت اطمینان و دسترس‌پذیری زیاد هستند (به‌عنوان مثال از ماشین‌هایی که در کشورهای دیگر بوده و دارای حداقل امنیت اینترنتی هستند و نیز همکاری بین‌المللی ندارند)، استفاده شود. دست‌آخر هارددیسک میزبان حسگر را بلافاصله پس از برداشتن گزارش داده‌ها، پاک کرد. در مرجع [۱۰]، ونتائو چانگ و همکاران یک کار مطالعاتی جهت اندازه‌گیری بات نت‌ها انجام دادند که اکثر بات‌نت‌های مطرح و شناخته‌شده در اینترنت در آن مشارکت داشتند. اطلاعات مورد استفاده در یک مجموعه داده (هفت ماهه) قرار داشت که توسط یک نهاد رصدگری[4]، جمع‌آوری شده بود. آن‌ها انواع توانمندی بات‌نت‌های شناخته‌شده را مورد بررسی و مقایسه قرار دادند، به‌طوری‌که، تحلیل آن‌ها به‌طور واضح نشان

1- Omnet
2- Ontology
3- Bot Master
4- Monitoring

داد که انواع باتنت‌ها برای اجرای یک حمله منع خدمت، با یکدیگر همکاری دارند. در مرجع [۱۱]، گوبتا و همکاران یک طرح جدید برای تخمین قدرت حمله منع خدمت ارائه کردند، بطوری‌که، توانستند بین قدرت حمله و میزان انحراف آنتروپی (مشاهده‌شده)، رابطه‌ای پیدا کرده و مدل خود را به‌صورت یک رگرسیون چندجمله‌ای ارائه دهند. همچنین، برای ارزیابی مدل، از انواع اندازه‌گیری عملکردهای آماری استفاده کردند و نیز با استفاده از شبیه‌ساز شبکه NS2، حملات منع خدمت توزیع‌شده را با انواع قدرت‌های حمله راه‌اندازی کردند. نتایج شبیه‌سازی نشان داد که می‌توانند قدرت کارآمدی حمله منع خدمت توزیع‌شده را تخمین بزنند.

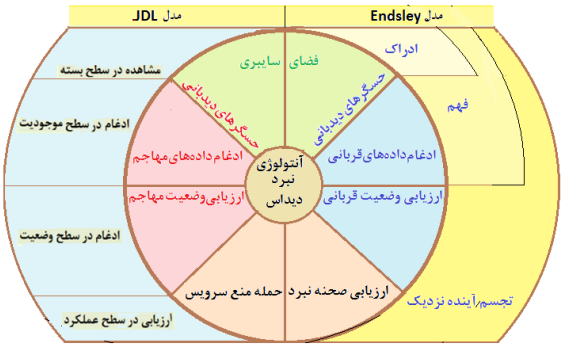
در مرجع [۲]، ارنه ولزل و همکاران توانستند سرورهای فرماندهی و کنترل ۱۴ باتنت شناخته‌شده DIRTJUMPER و YODDS را رصدکرده و اهداف مورد حمله منع خدمت توزیع‌شده آن‌ها را ثبت و ضبط[1] کردند. سپس، آن‌ها با استفاده از انواع اندازه‌گیری‌ها ازقبیل زمان پاسخ TCP و تحلیل محتوای HTTP توانستند دسترس‌پذیری قربانی‌ها را ارزیابی کنند. آن‌ها نشان دادند که بیش از ۶۵ ٪ قربانی‌ها توسط حملات منع خدمت توزیع‌شده، به‌شدت آسیب‌پذیر هستند و حملات کم‌تری به شکست منجر می‌شوند. در مرجع [۱۲]، ژیتانگ لی و همکاران برای اندازه‌گیری شبکه‌باتی که مبادرت به ارسال هرزنامه می‌کند، دو چارچوب را ارائه کرده‌اند. چارچوب اول، اندازه‌گیری از سطح شبکه[2] است که در این روش وقتی رایانه‌ای مبادرت به ارسال بسته SMTP می‌کند، آن‌ها را مورد توجه قرار داده و آماری از تکرار فعالیت‌های آن‌ها (IP آدرس ارسال‌کننده) را ثبت می‌کند، به‌طوری‌که اگر آمار ارسال از هر آدرس IP بیش از حد آستانه یک کاربر عادی باشد، آن را به‌عنوان بات درنظر گرفته و عضوی از جمعیت شبکه‌بات قرار می‌دهد. در چارچوب دوم، اندازه‌گیری از سطح لایه کاربرد[3] صورت می‌گیرد، به‌طوری‌که با همکاری خدمات‌دهنده رایانامه، آدرس ارسال‌کننده نامه‌ها استخراج شده و آماری از تکرار آن‌ها را به‌دست‌آورده و آدرس‌هایی که بیش از حد متعارف یک کاربر معمولی، نامه ارسال کرده باشند را نیز به‌عنوان بات محسوب کرده و در فهرست جمعیت شبکه‌بات قرار می‌دهد.

همان‌گونه که ملاحظه گردید، هیچ یک از طرح‌های پیشنهادشده، پاسخ‌گوی اندازه‌گیری قدرت و عملکرد شبکه‌بات در حین حمله‌ی منع خدمت توزیع شده نبوده و طرح پیشنهادی این پژوهش، در نظر دارد این چالش را پاسخ دهد.

1- Log
2- Measuring From the Network Level
3- Measuring From The Application Level

۳- طرح پیشنهادی

حسگرهای رصد قربانی و شبکه بات مهاجم در فضای سایبری قرار دارند که مبادرت به دیده‌بانی می‌کنند. در ادامه لازم است اطلاعات حسگرها مورد تلفیق قرار گیرند و شرایط را برای ارزیابی وضعیت صحنه طرفین فراهم آورند. در این میان وجود یک آنتولوژی کارآمد، تمامی بخش‌ها را پشتیبانی کرده و سؤال «چه کارهایی باید کرد؟» را پاسخ‌گو است [۱۳]. در حالت کلی، می‌توان ارزیابی وضعیت صحنه نبرد حمله منع خدمت توزیع‌شده را به‌صورت شکل (۱) متصور شد. مدل پیشنهادی با مدل پنج‌لایه JDL[4] [۱۴] و مدل سه‌لایه آگاهی وضعیتی اندسلی[5] [۱۵] دارای هم‌پوشانی است با این تفاوت که این مدل توسط یک آنتولوژی نبرد منع خدمت توزیع‌شده پشتیبانی می‌گردد.



شکل (۱): شمای کلی طرح پیشنهادی برای ارزیابی صحنه نبرد حمله منع خدمت توزیع‌شده

سمت راست مربوط به قربانی و سمت چپ مربوط به مهاجم می‌باشد. به‌منظور تجزیه و تحلیل و ارزیابی دیده‌بان‌های حملات منع خدمت توزیع‌شده، لازم است مدل‌سازی در این خصوص صورت گیرد. در این تحقیق، به ارزیابی وضعیت مهاجم پرداخته می‌شود. از این‌رو، در ابتدا مدل شبکه حسگر نیابتی پیشنهادشده و در ادامه، مدل فوق مورد شبیه‌سازی قرار می‌گیرد. سپس با انجام آزمایش در محیط شبیه‌سازی، نتایج، ارزیابی شده و میزان دقت و خطای مدل، اندازه‌گیری می‌شود. طرح اصلی این پژوهش به ایجاد یک شبکه حسگری با استفاده از میزبان‌های تحت کنترل (نیابتی) برمی‌گردد. میزبان‌های نیابتی ماشین‌هایی هستند که در نقاط مختلف شبکه (اینترنت) مستقر می‌شوند و مبادرت به جمع‌آوری اطلاعات از شبکه بات می‌کنند و سپس اطلاعات را در یک نقطه تجمیع کرده و مورد تجزیه و تحلیل قرار می‌دهند. کارکرد آن‌ها بدین‌صورت است که هر عضو از شبکه بات ضمن

4- Joint Direction Literary
5- Endsley

ارسال بسته‌های انبوه به ماشین قربانی، کسری از آن بسته‌ها ($\frac{1}{N}$) را نیز به سرور نیابتی ارسال نماید. (هر بسته حاوی آدرس IP بات، آدرس IP قربانی، پروتکل و درگاه می‌باشد که می‌توان با استفاده از آن‌ها، قدرت حمله، نوع حمله و محدوده جغرافیایی و غیره را به‌دست آورد. در این پژوهش، فقط اندازه‌گیری قدرت حمله مبتنی بر بسته مدنظر می‌باشد.

بنابراین، اگر هر بسته دریافتی توسط سرور نیابتی، N برابر گردد، می‌توان به تخمینی از قدرت شبکه بات پی برد. نظر به این‌که در شبکه اینترنت احتمال گم‌شدن و فیلترشدن بسته‌ها وجود دارد، از این‌رو، ممکن است نتایج هریک از سرورهای نیابتی با یکدیگر متفاوت بوده و برآورد را با بی‌دقتی مواجه کنند. از این‌رو، به‌منظور اندازه‌گیری دقیق توان شبکه بات با استفاده از سرور نیابتی نیاز است در این خصوص مدل‌سازی و شبیه‌سازی صورت پذیرد. لذا در ابتدا یک سرور نیابتی مورد مدل‌سازی قرار گرفته و سپس به‌منظور بالابردن قابلیت اطمینان تخمین، تعداد بیشتری از سرورهای نیابتی مورد استفاده قرار می‌گیرد، بدیهی است مباحث عدم قطعیت اعم از قطعی یا خرابی سرور نیابتی و در معرض فیلترینگ قرارگرفتن و گم‌شدن بسته‌ها و همچنین ترافیک مجاز (کاربران و تجهیزات شبکه) که ممکن است در نتایج ارزیابی تأثیرگذار باشد [۱۶]، نیاز است مدل پیشنهادی، آن‌ها را هم مدنظر قراردهد.

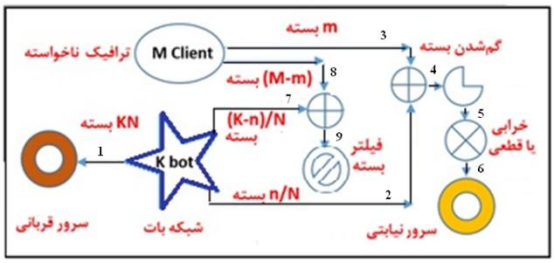
لازم به ذکر است که شکل (۱) چارچوب کلانی از ارزیابی صحنه نبرد را ارائه می‌دهد و لیکن در انتهای این پژوهش، با روشن‌شدن مراحل کار، چارچوب دقیق‌تری پیشنهاد می‌گردد.

۳-۱- مدل‌سازی طرح حسگر نیابتی

طرح پیشنهادی نیاز دارد در سه سطح تک حس‌گر، شبکه حس‌گر نیابتی و تلفیق اطلاعات، به‌صورت مجزا مورد مدل‌سازی قرار گیرد و نیز در ادامه، هر یک از آن‌ها شبیه‌سازی شده و در نهایت طرح فوق مورد ارزیابی قرار گیرد.

۳-۱-۱- مدل‌سازی تک حسگر نیابتی

در مدل تک حسگر نیابتی، گم‌شدن هریک از این بسته‌ها موجب کاهش تخمین محاسبات می‌گردد و همچنین دریافت بسته‌هایی خارج از شبکه بات (ترافیک کاربران عادی یا ترافیک تجهیزات شبکه) موجب افزایش تخمین محاسبات می‌شود (با فرض علامت‌دار نبودن بسته‌ها). از طرفی، عواملی همچون فیلترینگ منطقه‌ای یا بین‌المللی موجب عدم دریافت برخی از بسته‌های شبکه بات می‌گردد و درنتیجه، شبیه به گم‌شدن بسته‌ها موجب کاهش تخمین محاسبات می‌گردد؛ بنابراین، لازم است در مدل‌سازی و شبیه‌سازی صورت گرفته، مسائل فوق لحاظ گردند. به‌منظور مدل‌کردن سرور نیابتی، ابتدا تمام عناصر اثرگذار اعم از ترافیک ناخواسته، خرابی سرور، گم‌شدن بسته و فیلترینگ منطقه‌ای را درنظر گرفته و با توجه به تأثیر آن‌ها، نحوه ارتباط آن‌ها به یکدیگر را لحاظ کرده که می‌توان آن را در شکل (۲) ملاحظه کرد.



شکل (۲): مدل‌سازی تک حس‌گر نیابتی

شبکه بات که با نماد ستاره نشان داده شده است، دارای K بات می‌باشد که هر بات به ازای هر N بسته ارسالی به سرور قربانی، یک بسته به سمت سرور نیابتی ارسال می‌کند ($\frac{1}{N}$ برای یک بات و $\frac{K}{N}$ برای K بات). این بسته با احتمال $P_{fil.}$ ممکن است در معرض فیلترینگ قرار گیرد. به‌عبارتی، تعداد این بسته‌ها از K- n بات ارسال می‌شود و باقیمانده بات‌ها (n) در معرض فیلتر نیستند. از طرفی، اعمال M بسته ترافیک ناخواسته (کاربران عادی یا تجهیزات شبکه) در مدل وجود دارد که به اندازه M-m بسته در معرض فیلترینگ و درنتیجه، m بسته از فیلتر عبور می‌کنند که موجب دریافت (اضافی) غلط حسگر را به‌دنبال خواهد داشت. همچنین، کلیه بسته‌های عبوری (m + $\frac{n}{N}$ بسته) ممکن است با احتمال P_L گم شود و هرگز به سرور نیابتی نرسد. و نیز با احتمال P_{fail} ممکن است سرور نیابتی خراب باشد و از گردونه رصدگرها خارج گردد. بنابراین؛ می‌توان آن را در رابطه (۱) درنظر گرفت:

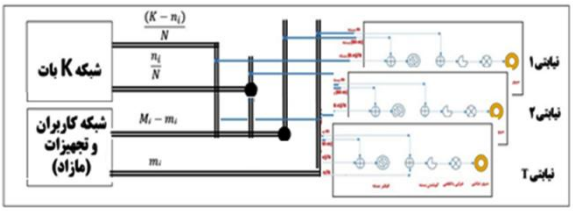
$$\text{بسته دریافتی سرور نیابتی} = \left(m + \frac{n}{N}\right) * \text{بسته} * (1 - P_{fail}) * (1 - P_L) \qquad (۱)$$

با وضعیت فوق، ممکن است سرور نیابتی دریافتی غلط داشته باشد که اگر مقدار آن در N ضرب گردد، مقداری متفاوتی از ترافیک دریافتی توسط سرور قربانی ملاحظه می‌شود که لازم

است تدبیری مناسب صورت گیرد. گم‌شدن بسته‌ها به عوامل مختلفی بستگی دارد. در این خصوص می‌توان قبل از شروع حمله نرخ گم‌شدن بسته هریک از مسیرهای سرور نیابتی را اندازه‌گیری نمود و سپس هنگام حمله این نرخ را در تصحیح محاسبات لحاظ کرد. برای جلوگیری از ترافیک مازاد (m) می‌توان از بسته‌های علامت‌دار استفاده کرد [۱۷] و یا با داشتن آدرس IPهای شبکه بات، آن‌ها را از بسته‌های ناخواسته جداسازی کرد. پیشنهاد دیگر این‌که قبل از حمله نرخ ترافیک مازاد اندازه‌گیری شده و سپس هنگام حمله این نرخ در تصحیح محاسبات لحاظ گردد.

۳-۱-۲- مدل‌سازی شبکه حسگر نیابتی

این مدل، شبیه مدل‌سازی تک‌حسگر نیابتی است با این تفاوت که هرکدام از سرورهای نیابتی ممکن است در معرض ترافیک کاربران مجاز (ترافیک ناخواسته) و فیلترینگ‌های خاص خود باشند. در این مدل، تعداد سرورهای نیابتی برابر T درنظر گرفته شده است و نیز $\frac{K-n_i}{N}$ تعداد بسته‌هایی هستند که در معرض فیلترینگ سرور نیابتی i ام قرار می‌گیرد و هرگز به مقصد نمی‌رسند. همچنین، $\frac{n_i}{N}$ تعداد بسته‌هایی هستند که در معرض فیلترینگ قرار نگرفته‌اند و به سمت سرور نیابتی iام ارسال شده‌اند. همچنین، $M_i - m_i$ تعداد بسته‌هایی هستند که از طرف کاربران عادی در معرض فیلترینگ سرور نیابتی iام قرار می‌گیرند و نیز، m_i تعداد بسته‌هایی از ترافیک ناخواسته است که در معرض فیلترینگ قرار نمی‌گیرند و به سمت سرور نیابتی iام ارسال می‌شوند. این مدل در شکل (۳) نشان داده شده است.



شکل (۳): مدل‌سازی چندحسگر نیابتی

بدیهی است که کارکرد هریک از سرورهای نیابتی شبیه به همدیگر بوده و با توجه به شرایط شبکه، نتایج هریک می‌تواند متفاوت باشد. لذا ممکن است s سرور نیابتی خراب شود و T-s سرور، حاوی اطلاعات باشند. همچنین، ممکن است p سرور نیابتی در معرض فیلترینگ قرار بگیرند و اطلاعات آن‌ها نسبت به سایر سرورها دارای کمی و کاستی باشد؛ بنابراین، می‌توان انتظار داشت در این مرحله اطلاعات گوناگونی از قدرت شبکه بات توسط هریک از سرورهای نیابتی گزارش شود که لازم است با پردازش اطلاعات، به یک گزارش واحد و کامل از ترافیک شبکه بات برسیم. این پردازش اطلاعات، در قالب ادغام و تلفیق داده‌ها در بخش بعدی موردبررسی قرار می‌گیرد.

۳-۲- مدل‌سازی تلفیق اطلاعات شبکه حسگری نیابتی

شبکه حس‌گری باید بتواند داده‌های خام چند (N) حسگر نیابتی را با استفاده از تلفیق داده، تجمیع کرده و کوچک‌سازی کند. نظر به این‌که اعمال فیلترینگ منطقه‌ای ممکن است بر کارکرد حسگرهای نیابتی تأثیر منفی بگذارد از این‌رو، فرض می‌شود که حداقل q سرور ثابت نیابتی از T سرور نیابتی، در نقاط جغرافیایی خاصی قرار گیرند که در معرض فیلترینگ قرار نداشته باشند. همچنین، فرض بر آن است که داده‌ها در فاصله‌های زمانی یکسان دریافت شده و مورد ارزیابی قرار می‌گیرند. روش ادغام را می‌توان به دو صورت ترکیبی[1] یا انتخابی[2] پیشنهاد داد. در روش ترکیبی، داده سرورهای نیابتی با یکدیگر ممزوج شده و یک نتیجه را حاصل می‌دهند (مانند میانگین گرفتن). در روش انتخابی (رأی‌گیری[3])، داده مربوط به یکی از سرورهای نیابتی گزینش شده و مورد استفاده قرار می‌گیرد. عملیات ادغام داده در هر رکورد زمانی، به‌صورت جداگانه و مستقل انجام می‌گردد. لذا به‌طور اجمال روش‌های پیشنهادی به شرح ذیل ارائه می‌گردد.

۳-۳- روش‌های پیشنهادی ادغام (ترکیب و انتخاب)

۱- متوسط‌گیری (مقدار میانگین): در این روش از داده سرورهای نیابتی، میانگین گرفته می‌شود و عدد حاصل، نماینده سرورهای نیابتی می‌باشد. این روش از نوع ترکیبی می‌باشد.

۲- مقدار بیشینه[4]: در این روش از بین داده سرورهای نیابتی، سروری که دارای بیشترین مقدار است، انتخاب (رأی‌گیری) می‌شود.

۳- مقدار کمینه[5]: در این روش از بین داده سرورهای نیابتی، سروری که دارای کمترین مقدار است، انتخاب (رأی‌گیری) می‌شود.

۴- رأی‌گیری kتای بزرگ‌تر: در این روش از N سرور نیابتی k تا (k =<۳) که دارای بیشترین مقدار داده باشند انتخاب می‌گردند و

1- Fusion
2- Selection
3- Voting
4- Maximum
5- Minimum

سپس مقدار برگزیده از این k سرور، به یکی از طرق زیر انتخاب می‌گردد:

الف) گزینش داده کمینه: از بین k سرور نیابتی منتخب، سروری که دارای کمترین مقدار است، انتخاب می‌شود.

ب) گزینش مقدار بیشینه: از بین k سرور نیابتی منتخب، سروری که دارای بیشترین مقدار است، انتخاب می‌شود (که نتایج حاصل مشابه روش دوم می‌باشد).

ج) متوسط‌گیری: در این روش، از داده‌های k سرور نیابتی منتخب، مقدار میانگین گرفته می‌شود.

۵- رأی‌گیری kتای مشابه: در این روش از N سرور نیابتی، k تا (۳ <=k) که دارای شبیه‌ترین مقادیر داده نسبت به‌هم داشته باشند، انتخاب می‌گردند و سپس مقدار برگزیده از این k سرور، به یکی از طرق اشاره‌شده در روش ۴، انتخاب می‌گردد.

هریک از این روش‌ها ممکن است دارای دقت و خطای خاصی باشند که می‌توان با آزمایش‌های مختلف آن‌ها را مورد بررسی قرار داد.

۳-۳-۱- نحوه ارزیابی روش‌های ادغام

به‌منظور انتخاب بهترین روش ادغام، ضروری است که آن‌ها با استفاده از روش‌های مشابهت‌سنجی، مورد مقایسه و ارزیابی قرار گیرند. از این‌رو، روش‌های متنوعی برای مشابهت‌سنجی وجود دارد که در این‌جا از روش فاصله منهتنی و اقلیدسی [۱۸] و نیز به‌منظور اندازه‌گیری دقت از تناسب مساحت‌های زیرمنحنی استفاده می‌شود که در ادامه به آن پرداخته خواهد شد.

۳-۳-۱-۱- روش فاصله

در این روش، اختلاف بین نتایج تخمین با نتایج واقعی می‌تواند به‌عنوان معیار مشابهت‌سنجی قرار گیرد. بدیهی است که این اختلاف از جنس خطا بوده و هرچقدر اندک باشد، نشان‌دهنده شباهت تخمین روش پیشنهادی با نتایج واقعی است و برعکس آن، اگر این اختلاف زیاد باشد، بیانگر مطلوب‌نبودن روش پیشنهادی می‌باشد. برای به‌دست‌آوردن اختلاف بین نتایج تخمین با نتایج واقعی می‌توان از روابط (۴-۲) شناخته‌شده منهتن، اقلیدسی و حتی از درجه‌های بالاتر فرمول جامع مربوط به مینکوفسکی بهره برد [۱۸] که در این پژوهش از رابطه (۳) استفاده می‌شود.

تعریف فاصله مینکوفسکی با نُرم یک (فاصله منهتن): برای دو بردار $V=(y_1, y_2, \dots, y_n)$ و $W=(x_1, x_2, \dots, x_n)$ برابر است با:

$$d = \|V-W\|_1=\sum_{i=1}^{n} |x_i - y_i| \qquad (۲)$$

تعریف فاصله مینکوفسکی با نُرم دو (فاصله اقلیدسی): برای دو بردار $V=(y_1, y_2, \dots, y_n)$ و $W=(x_1, x_2, \dots, x_n)$ برابر است با:

$$d = \| V - W \|_2 = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \qquad (۳)$$

تعریف فاصله مینکوفسکی با نُرم سه: برای دو بردار $V=(y_1, y_2, \dots, y_n)$ و $W=(x_1, x_2, \dots, x_n)$ برابر است با:

$$d = \| V - W \|_3 = \sqrt[3]{\sum_{i=1}^{n} |x_i - y_i|^3} \qquad (۴)$$

با توجه به فاصله مینکوفسکی با نُرم دوم یا سوم، بدیهی است اگر فاصله دو بردار V و W بیشتر یا کمتر باشد، مقدار توان دوم یا سوم، موجب افزایش یا کاهش مضاعف مقدار حاصل شده و درنتیجه، باعث پراکندگی یا تراکم محسوس نتایج می‌شود که در تفکیک یا مقایسه نتایج، دقت مضاعفی را به‌وجود می‌آورد. از آن‌جایی‌که، نتایج تغییرات نُرم سوم به نُرم دوم، (با توجه به پیچیدگی‌های محاسباتی بیشتر) قابل صرف‌نظرکردن می‌باشد، متداول است از نُرم دوم استفاده شود.

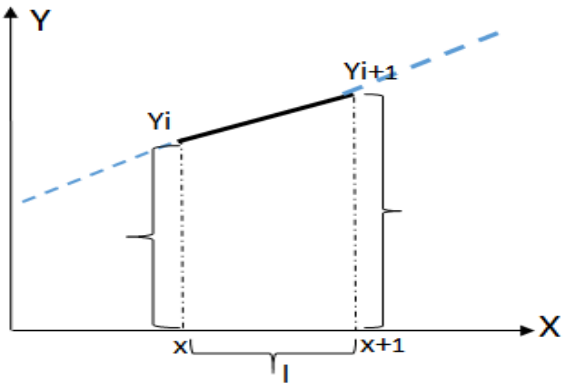
۳-۳-۱-۲- روش نسبت مساحت

در این روش می‌توان از اندازه‌گیری نسبت مساحت‌ها بهره‌مند شد. به‌طوری‌که، مساحت زیرمنحنی روش‌های تخمین نسبت به مساحت زیرمنحنی شبکه بات اندازه‌گیری شده و برای ارزیابی نزدیکی یا مشابهت‌سنجی، مورد استفاده قرار گیرد. بدیهی است هرقدر مقدار این نسبت به عدد یک نزدیک‌تر باشد، بیانگر شباهت روش تخمین مطلوب به شبکه بات است. مساحت مورد نظر برای هریک از روش‌های تخمین در هر گام به‌صورت انتگرال ذوزنقه‌ای که در شکل (۴) آمده است، طبق روابط (۶-۵) محاسبه می‌شود.

$$SF_i = \frac{yf_i + yf_{i+1}}{2} * L \qquad (۵)$$

$$SB_i = \frac{yb_i + yb_{i+1}}{2} * L \qquad (۶)$$

که در آن، SF_i به‌عنوان مساحت (لحظه‌ای) زیرمنحنی تخمینی (روش ادغام) و SB_i به‌عنوان مساحت (لحظه‌ای) زیرمنحنی شبکه بات معرفی می‌گردد. به‌طوری‌که، با مجموع هریک از مساحت‌ها، طبق روابط (۸-۷) می‌توان به مساحت کل زیرمنحنی‌های SF و SB دست یافت.



شکل (۴): مساحت با استفاده از انتگرال ذوزنقه‌ای

$$SF = \sum_{i=1}^{end\ time} SF_i \qquad (۷)$$

$$SB = \sum_{i=1}^{end\ time} SB_i \qquad (۸)$$

$$Rs = \begin{cases} \frac{SF}{SB} & SF < SB \\ \frac{SB}{SF} & SF > SB \end{cases} \qquad (۹)$$

لذا در هر گام، yf_i مقدار تخمین ترافیک لحظه‌ای که در زمان iام رخ داده است و همچنین مقدار L واحدهای زمانی یکسان می‌باشند. برای به‌دست‌آوردن مقدار مشابهت هریک از روش‌های تخمین مورد نظر با شبکه بات، از رابطه (۹) استفاده می‌شود که بیانگر دقت نزدیکی و مشابهت می‌باشد، از تقسیم مجموع مساحت تخمین و مجموع مساحت شبکه واقعی بات نسبت به یکدیگر به‌دست می‌آید؛ بنابراین، برای ارزیابی روش‌های ادغام از روش فاصله مینکوفسکی با نُرم دوم (فاصله اقلیدسی) استفاده می‌گردد و برای اندازه‌گیری دقت از تناسب مساحت‌ها بهره گرفته می‌شود. حال نیاز است از بین روش‌های پیشنهادی ادغام (ترکیب و انتخاب) گزینه یا گزینه‌های مطلوب را انتخاب کرده و مورد ارزیابی قرار داد. وجود فیلترینگ در مسیر هریک از سرورهای نیابتی موجب می‌شود تا بسته‌های کمتری به آن‌ها برسد و درنتیجه، میزان تخمین را کاهش دهد. بنابراین، گزینه‌های میانگین‌گیری و کمینه، تخمین کمتری را در شرایط فیلترینگ ارائه می‌دهند. همچنین، وجود ترافیک ناخواسته که سوار بر ترافیک شبکه بات شده است، موجب افزایش میزان تخمین می‌گردد. از این‌رو، گزینه مقدار بیشینه مناسب نمی‌باشد ولی اگر بسته‌ها علامت‌گذاری شده باشند، هیچ ترافیک ناخواسته‌ای وجود ندارد و گزینه مقدار بیشینه می‌تواند مناسب باشد و نیز اگر بیش از یک مسیر از سرورهای نیابتی درمعرض فیلترینگ قرار گیرد نتیجه گزینه رأی‌گیری k تای مشابه شبیه گزینه رأی‌گیری k تای بزرگ‌تر می‌گردد؛ بنابراین، با توجه به این‌که داده‌های شبیه‌ساز علامت‌گذاری نشده است، گزینه‌های منتخب می‌تواند، روش‌های کمینه و رأی‌گیری k تای مشابه باشد که به شرح ذیل بیان می‌گردد.

۳-۳-۲- رأی‌گیری ۳ تای بزرگ‌تر

در این روش، ۳ تا از ۵ سرور نیابتی که دارای بیشترین مقدار داده باشند انتخاب می‌گردند و سپس مقدار برگزیده از این ۳ سرور، به یکی از دو طرق زیر انتخاب می‌گردد:

۱) گزینش داده کمینه: از بین ۳ سرور نیابتی منتخب، سروری که دارای کمترین مقدار است، انتخاب می‌شود که آن را مین‌ماکس[1] می‌نامیم (انتخاب کمترین از حداکثرها).

۲) متوسط‌گیری: در این روش از داده‌های ۳ سرور نیابتی منتخب، مقدار میانگین گرفته می‌شود.

۳-۳-۲-۱ گزینش مقدار کمینه

از بین ۵ داده سرورهای نیابتی، سروری که دارای کمترین مقدار است، انتخاب می‌شود. حال به‌منظور یافتن بهترین روش ادغام مذکور، با استفاده از مجموعه داده پنج سرور نیابتی (در قالب سناریوهای مختلف)، آزمایش‌های ویژه‌ای انجام شده است. در این آزمایش‌ها، مقادیر گزینش‌شده هریک از روش‌های ادغام ۵۰ برابر شده و با استفاده از روش فاصله اقلیدسی نسبت به ترافیک اصلی شبکه بات، مورد مقایسه قرار می‌گیرند و درنتیجه، روشی که دارای مقدار کمتری نسبت به بقیه است، از تخمین بهتری برخوردار می‌باشد.

۴- شبیه‌سازی و ارزیابی طرح پیشنهادی

در ابتدا مدل شبکه حسگر نیابتی با استفاده از سه سناریو مورد شبیه‌سازی قرار گرفته و در ادامه به شبیه‌سازی مدل تلفیق اطلاعات به سه روش پرداخته می‌شود. در این مرحله، مدل شبکه حسگر نیابتی با استفاده از شبیه‌ساز Omnet++ مورد آزمایش قرار

1- MinMax

می‌گیرد. برای تسهیل در کار فرض می‌شود که دو احتمال خرابی حسگر و فیلترینگ برابر صفر است (Pfail = 0 , Pfil = 0). همچنین، فرض می‌شود که در هر بات به ازای هر ۵۰ بسته ارسالی به سمت قربانی، یک بسته به سمت سرور نیابتی ارسال شود (N = ۵۰). آزمایش را در مدت ۸۰۰ ثانیه درنظر گرفته شد که از ثانیه ۲۰۰ حمله آغاز شده و در مدت ۶۰۰ ثانیه به اوج خود می‌رسد؛ بنابراین، تا قبل از ثانیه ۲۰۰ همه ترافیک، مربوط به کاربران مجاز و تجهیزات شبکه می‌باشد و از ثانیه ۲۰۰ به بعد ترافیک حمله و ترافیک کاربران با هم تجمیع می‌گردد. با توجه به رابطه (۱)، تنظیمات اولیه شبیه‌ساز به شرح جداول (۱) می‌باشد. در این شبیه‌سازی، مدنظر است چند آزمایش با ویژگی‌های متفاوت صورت گیرد که در قالب سه سناریو در جدول (۲) ارائه شده است.

جدول (۲): پیکربندی اجرای سناریوها

مکانیسم حمله	سناریو حمله ۱	سناریو حمله ۲	سناریو حمله ۳
	شبیه‌سازی بدون حمله	شبیه‌سازی با احتمال وقوع ۱۰۰٪ حمله	شبیه‌سازی با احتمال وقوع ۵۰٪ و احتمال قطع ۵۰٪
احتمال قطع حمله	۰	۰	۵۰
احتمال فعال‌شدن حمله	۰	۱۰۰	۵۰
بازه اوج حمله	۶۰۰	۶۰۰	۶۰۰
لحظه شروع حمله	۲۰۰	۲۰۰	۲۰۰
مدت شبیه‌سازی	۸۰۰	۸۰۰	۸۰۰

جدول (۱): مشخصات گره‌های شبکه و شرایط آزمایش

End user	۹۰۷
Mail server	۲۷
Interactive server	۲۷
Web server	۷۱
Edge router	۱۷۵
Gateway router	۳۱
Core router	۲۰
تعداد بات	۲۳۸
نرخ بسته ارسالی بات به نیابتی	۱/۵۰
درصد احتمال فیلترینگ (Pfil)	۰
درصد احتمال گم شدن بسته (PL)	۳
درصد احتمال خرابی نیابتی (Pfail)	۰
نرخ بسته‌های عادی (M) (توزیع پوآسن)	۸۰۰ <= M <= ۱۰۰۰

۴-۱- تبیین و اجرای سناریوها در سطح بسته‌های شبکه

با تبیین و اجرای سناریوهای مختلف، می‌توان رفتار مدل پیشنهادی را مورد تجزیه و تحلیل قرار داد. از این‌رو، سه سناریو هدفمند به شرح ذیل تعریف می‌گردد:

سناریوی اول: هدف این سناریو بررسی کارکرد عادی شبکه بدون وجود حملات، نرخ ارسال و دریافت بسته‌های عادی و زمان پاسخگویی قربانی بدون حمله است.

سناریوی دوم: هدف این سناریو بررسی وضعیت شبکه و به‌خصوص قربانی تحت حملات با بهره‌گیری از سرور نیابتی است. در این حالت، پارامترهایی مثل نرخ دریافت بسته‌های حمله، زمان پاسخگویی قربانی، نرخ متوسط دریافت بسته و غیره با استفاده از سرور نیابتی اندازه‌گیری می‌شود. هدف این سناریو بیان لزوم استفاده از سرور نیابتی و ویژگی‌های آن است.

سناریوی سوم: پس از بیان لزوم استفاده از سرور نیابتی و ویژگی‌های آن در سناریوی دوم، در این سناریو با تغییر در پارامترهای احتمال وقوع و قطع حمله درنظر است نقش کاهش تعداد بات‌ها در کارایی شبکه و همچنین، رفتار قربانی بررسی شود.

۴-۲- نتایج شبیه‌سازی آزمایش‌ها

بعد از اجرای شبیه‌ساز با مفروضات فوق، نتایجی استخراج شده است که نمودارهای آن در قالب پارامترهای زیر ترسیم شده است.

۱- نرخ دریافت بسته در واحد زمان

۲- درصد اشغال پهنای باند در واحد زمان

۳- زمان پاسخگویی در واحد زمان

۴- نرخ گم‌شدن بسته‌ها در ثانیه

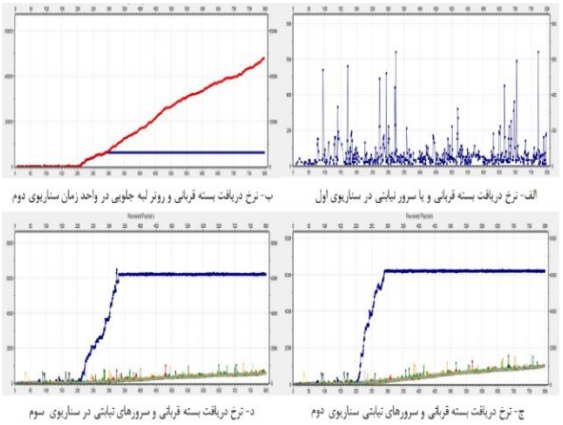
۵- متوسط تعداد بسته‌های دریافتی در کل زمان شبیه‌سازی

در ادامه هریک از سناریوها نسبت به پارامترهای فوق مقایسه و مورد بررسی قرار می‌گیرد.

۴-۲-۱ نرخ دریافت بسته

همان‌گونه که در شکل (۵) ملاحظه می‌شود، در سناریوی اول هنگامی‌که حمله‌ای صورت نگرفته باشد، نرخ دریافت بسته‌های سرور قربانی و یا سرور نیابتی دارای نرخ پایینی است (شکل ۵- الف). همچنین، با اجرای سناریوی دوم (که حمله صورت گرفته است) نرخ ترافیک هجوم تا مرز ۴۹۰۰۰ بسته در ثانیه در مسیریاب لبه جلویی قربانی ظاهر می‌گردد که درنتیجه،

سرور قربانی بعد از گذشت ۱۰۰ ثانیه به حالت اشباع (۵۰۰۰ بسته در ثانیه) می‌رسد و درنتیجه از خدمات‌دهی خارج می‌شود (شکل ۵- ب). در همین وضعیت، ترافیک سرور نیابتی حدود ۱۰۰۰ بسته در ثانیه را دریافت می‌کند (شکل ۵- ج).



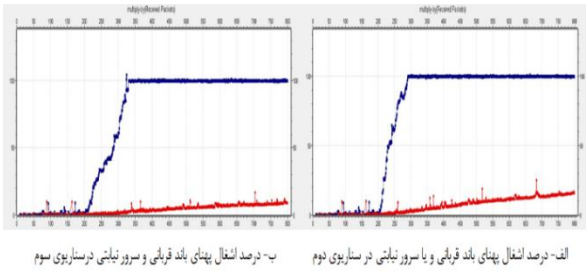
شکل (۵): نرخ دریافت بسته قربانی و نیابتی در سناریوهای مختلف

نتایج سناریوی سوم نیز شبیه سناریوی دوم است با این تفاوت که حمله قدری ضعیف‌تر بوده و قربانی دیرتر به حالت اشباع رفته است (شکل ۵- د).

۴-۲-۲- درصد اشغال پهنای باند قربانی و سرور نیابتی

نتایج شبیه‌سازی درخصوص اشغال پهنای باند در شکل (۶)، سناریوهای دوم (شکل ۶- الف) و سوم (شکل ۶- ب) نشان می‌دهد که پهنای باند سرور نیابتی در طول مدت حمله، اشباع نمی‌شود و توانسته است تا پایان آزمایش، کار را ادامه دهد اما پهنای باند سرور قربانی بعد از مدت‌زمان ۱۰۰ تا ۱۵۰ ثانیه اشباع شده است.

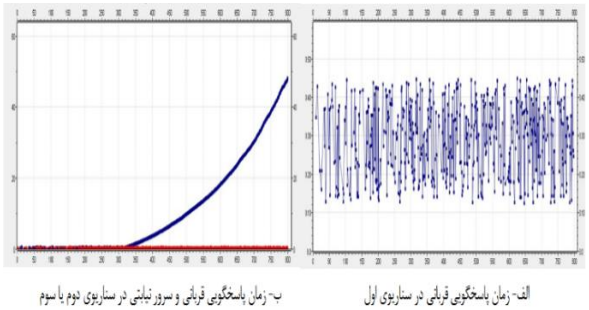
بنابراین، با انتخاب ضریب نمونه‌برداری مناسب می‌توان مطمئن شد که سرور نیابتی به‌علت اشباع پهنای باند از کار نمی‌افتد و می‌تواند به کار خود ادامه دهد.



شکل (۶): درصد اشغال پهنای باند قربانی و نیابتی در سناریوهای مختلف

۴-۲-۳- زمان پاسخگویی قربانی و سرور نیابتی

نتایج شبیه‌سازی درخصوص زمان پاسخ‌گویی ماشین‌های قربانی و نیابتی در شکل (۷- الف) نشان می‌دهد که ماشین قربانی در شرایط عادی (غیرحمله) پاسخ زمانی مطلوبی در حد ۳۰۰ میلی‌ثانیه دارد.

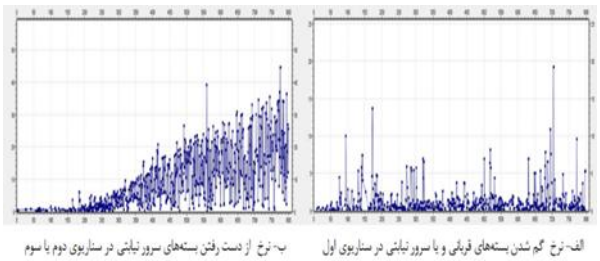


شکل (۷): زمان پاسخگویی قربانی و سرور نیابتی در سناریوها

اما در شرایط حمله، زمان پاسخ‌گویی قربانی از حد مجاز خود خارج شده و دیگر نمی‌تواند خدمات‌دهی داشته باشد، به‌طوری‌که هرقدر فشار حمله بیشتر می‌شود، زمان تأخیر پاسخ‌دهی طولانی می‌گردد. درنتیجه، از لحظه ۳۰۰ تا ۸۰۰ ثانیه، زمان پاسخ با سیر صعودی (نمایی) به حدود ۵۰ ثانیه می‌رسد (شکل ۷- ب).

۴-۲-۴- نرخ گم‌شدن بسته‌های قربانی و سرور نیابتی

نتایج شبیه‌سازی نشان می‌دهد که بسته‌ها همواره ممکن است با نرخ اندکی (۲ ٪) گم شوند (شکل ۸ - الف). همچنین، در زمان حمله تعداد بسته‌های گم‌شده در سرور نیابتی با افزایش نرخ بسته‌های حمله نسبت مستقیمی دارد (شکل ۸- ب).



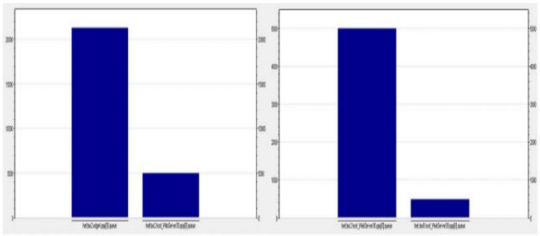
شکل (۸): نرخ گم‌شدن بسته‌های قربانی و سرور نیابتی در سناریوهای مختلف

بنابراین، می‌توان قبل از شروع حمله، نرخ گم‌شدن بسته‌ها را در مسیر سرور نیابتی اندازه‌گیری نمود و در بازسازی تخمین ترافیک واقعی، طبق رابطه (۱۰) آن‌را لحاظ کرد.

$$\text{تخمین ترافیک بات} = \frac{\text{بسته های دریافتی سرور نیابتی} * \text{ضریب نمونه برداری}}{1 - \text{نرخ گم شدن بسته}} \quad (۱)$$

۴-۲-۵- بسته‌های دریافتی قربانی و سرور نیابتی و مسیریاب لبه جلویی

در پایان آزمایش شبیه‌سازی، آماری از متوسط بسته‌های دریافتی توسط مسیریاب لبه جلویی (ترافیک واقعی بات)، قربانی و سرور نیابتی به‌صورت دوبه‌دو در شکل (۹) نشان داده شده است.



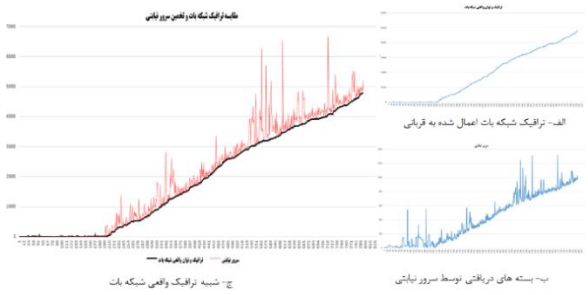
الف- بسته های دریافتی قربانی و سرور نیابتی در سناریوی دوم یا سوم ب- متوسط بسته های دریافتی قربانی و روتر لبه ای در سناریوی دوم یا سوم

شکل (۹): بسته‌های دریافتی قربانی، سرور نیابتی و مسیریاب لبه‌ای در سناریوهای مختلف

همان‌گونه که در این شکل ملاحظه می‌شود، نسبت بسته‌های دریافتی مسیریاب لبه جلویی و سرور نیابتی برابر ضریب نمونه‌برداری (حدود ۵۰ برابر) می‌باشد.

۴-۳- ارزیابی برآورد حسگر نیابتی و قدرت شبکه بات

همان‌گونه که انتظار می‌رفت حسگرهای نیابتی نشان دادند که در مقیاس کوچک ($\frac{1}{50}$) توانایی تخمین قدرت شبکه بات را دارند. شکل (۱۰)، این برآورد را به تصویر کشیده است. در شکل (۱۰- الف) منحنی ترافیک واقعی شبکه بات و در شکل (۱۰- ب) منحنی سرور نیابتی نشان داده شده است. همان‌گونه که مشاهده می‌شود سرور نیابتی توانسته است با دریافت ($\frac{1}{50}$) ترافیک واقعی شبکه بات، نمونه‌برداری قابل قبولی را انجام دهد، به‌طوری‌که با پنجاه برابرکردن این نرخ نمونه‌برداری، توانایی تخمین شبکه بات را کسب کرده است (شکل ۱۰- ج).



شکل (۱۰): مقایسه تخمین تک‌سرور نیابتی با ترافیک اعمال‌شده به قربانی

۴-۳-۱- نتایج ارزیابی تک‌حسگر نیابتی

شبیه‌سازی انجام‌شده در شرایطی انجام گرفت که عواملی همچون فیلترهای منطقه‌ای و خرابی سرور نیابتی وجود نداشتند. درصورتی‌که در واقعیت، این عوامل وجود دارند و موجب می‌گردند نتایج شبیه‌سازی تحت تأثیر آن قرار گیرد. به‌عبارتی، اگر هر لحظه خرابی در تک سرور نیابتی به‌وجود آید کار تخمین ترافیک عقیم می‌ماند و یا این‌که اگر فیلترینگ منطقه‌ای اعمال شود، نرخ بسته‌های دریافتی تک سرور نیابتی کاهش یافته و یا بسیار ناچیز می‌شود؛ بنابراین، تخمین ترافیک با بی‌دقتی زیادی مواجه بوده که برای رفع این مشکلات، استفاده از چند سرور نیابتی در نقاط جغرافیایی مختلف پیشنهاد می‌گردد که در اصطلاح به افزونگی[1] یا سرورهای اضافی معروف است.

۴-۳-۲- شبیه‌سازی و ارزیابی تلفیق اطلاعات شبکه حسگری نیابتی

در این مرحله با توجه به روش‌های پیشنهادی، مدنظر است با مفروضات بیان‌شده، روش‌های فوق را شبیه‌سازی کرد. لذا در سه آزمایش مجزا در ابتدا تأثیرات گم‌شدن بسته، فیلترینگ و خرابی حسگر سرور نیابتی مورد بررسی قرار می‌گیرند که نتایج آن‌ها در جدول (۳) نشان داده شده است. سپس، با نتایج به‌دست‌آمده، آزمایش ترکیبی شبیه‌سازی‌شده تا میزان دقت روش پیشنهادی اندازه‌گیری شود؛ بنابراین، تنظیمات شبیه‌ساز با توجه به جدول (۱) پیکربندی و اجرا می‌شود.

جدول (۳): مشخصات شبیه‌ساز در سناریوهای مختلف

تعداد بات	K	۲۳۸
نرخ بسته ارسالی بات به سرور نیابتی	1/N	۱/۵۰
درصد احتمال فیلترینگ	Pfil	۰ – ۵۰ - ۹۹
درصد احتمال گم‌شدن بسته	Pl	۰ – ۵ - ۱۰
درصد احتمال خرابی نیابتی	Pfail	۰
نرخ بسته‌های (بات ها) عبوری از فیلترینگ شبکه بات	N	۱۲۰ <= n <= ۱۷۰
نرخ بسته‌های عادی	M	۱۰ <= M <= ۱۱۲
نرخ بسته‌های عبوری از فیلترینگ کاربران عادی	M	۱ <= m <= ۱۱۲

1- Redundancy

۴-۳-۳- سناریو تأثیرات گم‌شدن بسته

هدف از این آزمایش، یافتن تأثیرات گم‌شدن بسته در مسیر سرورهای نیابتی است بنابراین، فرض می‌شود که هیچ‌گونه فیلتری و نیز خرابی در کار سرورهای نیابتی وجود ندارد. لذا، آزمایش در سه بخش با احتمال ۰، ۵ و ۱۰ ٪ گم‌شدن بسته انجام می‌گیرد (گم‌شدن بسته تا حد ۱ ٪ مقبول بوده و بیش از آن، موجب کاهش کیفیت سرویس شده و میزان نارضایتی کاربران شبکه را افزایش می‌دهد).

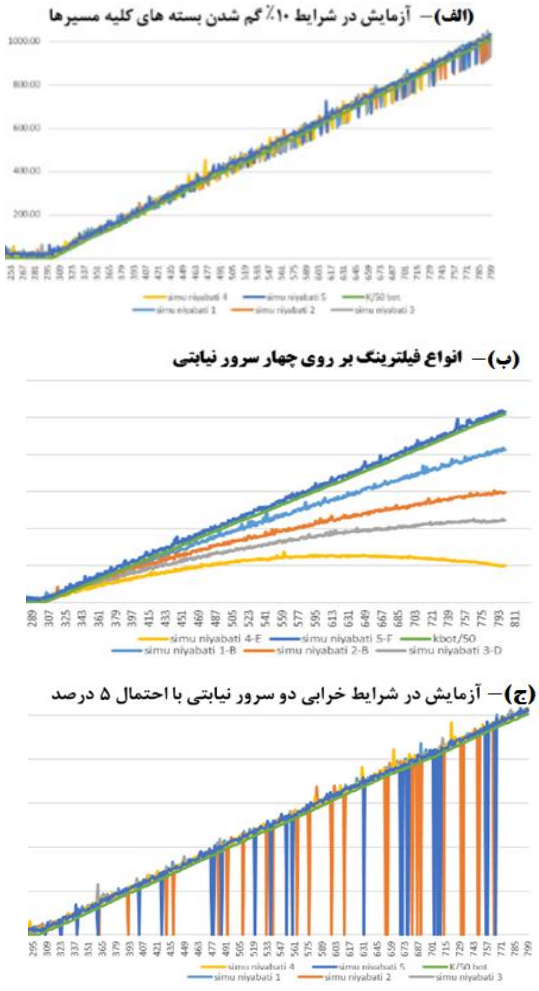
در بخش اول، هیچ‌یک از سرورهای نیابتی با گم‌شدن بسته مواجه نمی‌باشند. مشخص می‌شود که روش کمینه از شباهت بیشتری نسبت به بقیه برخوردار است. همچنین، پنج دسته آزمایش برای شرایطی که از یک تا پنج سرور نیابتی با احتمال ۵٪ گم‌شدن بسته، صورت گرفته است که بازهم نتایج نشان می‌دهد که روش کمینه شباهت بیشتری نسبت به بقیه دارد. آزمایش آخر نیز با پنج دسته فوق و با احتمال ۱۰ ٪ انجام شده است که شرایط را کمی متفاوت کرده است. به‌طوری‌که، نتایج نشان داد که روش مین ماکس از مقبولیت بیشتری نسبت به بقیه برخوردار است که می‌توان نتایج را در بخش فوقانی جدول (۴) ملاحظه نمود. سطر اول این بخش، بیانگر درصد گم‌شدن بسته‌های سرورهای نیابتی مورد آزمایش و سطر دوم نیز بیانگر تعداد سرورهای نیابتی مورد آزمایش می‌باشند. به عبارتی نماد $\binom{۳}{۵}$ نشان‌دهنده انتخاب سه سرور تصادفی از پنج سرور نیابتی (۳ از ۵) موجود در آزمایش می‌باشد. سه سطر بعدی به‌ترتیب بیانگر نتایج فاصله اقلیدسی روش‌های میانگین‌گیری سه‌تایی (انتخاب‌شده از پنج سرور)، کمینه و مین‌ماکس می‌باشند.

جدول (۴): تأثیرات گم‌شدن بسته، فیلترینگ بسته و خرابی حسگر در مسیر سرورهای نیابتی

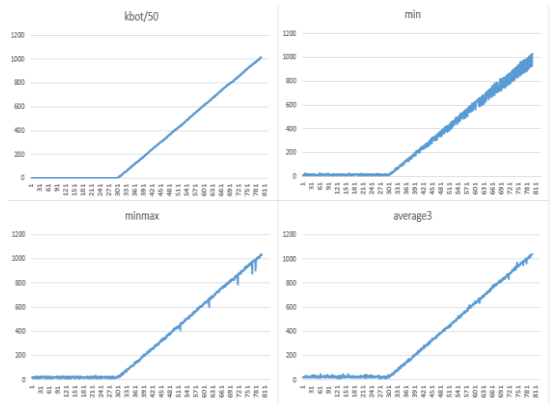
فاصله اقلیدسی مقادیر شبکه بات												
تأثیر گم‌شدن بسته	درصد گم‌شدن بسته	۰	۵					۱۰				
	تعداد سرورهای تحت آزمایش	$\binom{۰}{۵}$	$\binom{۱}{۵}$	$\binom{۲}{۵}$	$\binom{۳}{۵}$	$\binom{۴}{۵}$	$\binom{۵}{۵}$	$\binom{۱}{۵}$	$\binom{۲}{۵}$	$\binom{۳}{۵}$	$\binom{۴}{۵}$	$\binom{۵}{۵}$
	میانگین ۳ گزینه	۳۲/۵	۳۱/۸	۳۲/۳	۳۲/۵	۳۱/۹	۳۲/۰	۳۱/۸	۳۱/۸	۳۱/۷	۳۱/۷	۳۱/۹
	کمینه	۱۷/۳	۱۷/۳	۱۷/۴	۱۷/۴	۱۷/۵	۱۷/۸	۲۲/۷	۲۷/۰	۳۱/۵	۳۳/۳	۳۳/۵
	مین ماکس	۲۶/۴	۲۵/۹	۲۶/۰	۲۶/۱	۲۵/۶	۲۵/۹	۲۵/۸	۲۵/۷	۲۵/۴	۲۵/۸	۲۵/۵
تأثیر فیلترینگ بسته	درصد فیلترشدن	۵۰						۹۹				
	آزمایش	$\binom{۱}{۵}$	$\binom{۲}{۵}$	$\binom{۳}{۵}$	$\binom{۴}{۵}$	$\binom{۵}{۵}$		$\binom{۱}{۵}$	$\binom{۲}{۵}$	$\binom{۳}{۵}$	$\binom{۴}{۵}$	$\binom{۵}{۵}$
	میانگین ۳ گزینه	۳۰/۳	۲۷/۹	۷۰/۶	۱۷۱/۹	۲۵۲/۵		۳۰/۱	۲۷/۳	۱۴۷/۱	۳۱۸/۳	۴۸۶/۵
	کمینه	۲۸۵/۱	۲۷۳/۷	۲۶۷/۴	۲۷۷/۵	۲۶۷/۱		۴۹۱/۸	۵۰۳/۳	۴۸۶/۸	۴۹۷/۷	۴۹۴/۹
	مین ماکس	۲۳/۸	۲۰/۷	۲۴۲/۱	۲۶۸/۵	۲۵۷/۱		۲۳/۷	۲۰/۳	۴۷۷/۵	۴۹۰/۸	۴۸۸/۲
تأثیر خرابی حسگر	صحت سرور نیابتی	سالم	خراب									
	آزمایش	$\binom{۰}{۵}$	$\binom{۱}{۵}$		$\binom{۲}{۵}$			$\binom{۳}{۵}$		$\binom{۴}{۵}$		$\binom{۵}{۵}$
	میانگین ۳ گزینه	۳۲/۲	۳۰/۱		۲۷/۱			۲۰۴/۳		۴۲۲/۷		۶۵۱/۳
	کمینه	۱۷/۴	۶۴۹/۰		۶۵۰/۹			۶۵۳/۲		۶۴۴/۷		۶۵۱/۳
	مین ماکس	۲۶/۳	۲۳/۹		۱۹/۹			۶۵۳/۲		۶۴۴/۷		۶۵۱/۳

با توجه به نتایج حاصل از سه روش مذکور، روش مین ماکس در شرایط احتمال وقوع گم‌شدن بسته، از مقاومت بیشتری برخوردار است. البته گزینه روش مقدار کمینه نیز نتایج قابل قبولی را داشته است که در آزمایش‌های بعدی می‌توان قضاوت بهتری داشت. در شکل (۱۱- الف) نمودارهای پنج سرور نیابتی با شرایط ۱۰ ٪ گم‌شدن بسته نشان داده شده است. همان‌گونه که انتظار می‌رفت شرایط گم‌شدن بسته‌ها موجب کاهش میزان تخمین شده است.

همچنین به‌علت روی‌هم افتادگی نمودارها که وضعیت نمایشی مطلوبی به‌جا نمی‌گذارد، نمودار هریک از تخمین روش‌ها در شرایط ۱۰ ٪ گم‌شدن بسته‌ها برای تمامی پنج سرور به‌صورت مجزا در شکل (۱۲) نشان داده شده است.



شکل (۱۱): نمودارهای پنج سرور نیابتی با شرایط: الف) ۱۰ ٪ گم‌شدن بسته، ب) اعمال انواع فیلترینگ بر روی چهار سرور و ج) خرابی دو سرور نیابتی با احتمال ۵ ٪

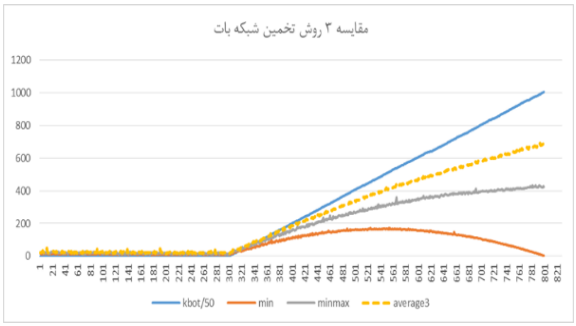


شکل (۱۲): تخمین روش‌ها در شرایط ۱۰ ٪ گم‌شدن بسته‌ها

همان‌گونه که در شکل (۱۲) ملاحظه می‌شود تخمین‌های مین ماکس و میانگین ۳ نسبت به تخمین کمینه شباهت بیشتری به نمودار شبکه بات (kbot/s) دارد. لیکن آنچه محاسبات فاصله اقلیدسی در جدول (۱) نشان داد، تخمین مین‌ماکس شباهت بیشتری نسبت به بقیه دارد.

۴-۳-۴- سناریوی تأثیرات فیلترینگ

در این مرحله از آزمایش، روش‌های ادغام نسبت به فیلترشدن مسیر سرورهای نیابتی مورد ارزیابی قرار می‌گیرند. به‌طوری‌که دو احتمال فیلترینگ ۵۰ ٪ (حد میانه) و ۹۹ ٪ (حداکثر آستانه) به‌صورت مجزا آزمایش شده است که نتایج آن در بخش میانی جدول (۴) نشان داده شده است. نتایج آزمایش نشان می‌دهد که اگر کمتر از سه سرور در معرض فیلترینگ قرار گیرد روش مین ماکس از مقبولیت بیشتری نسبت به بقیه برخوردار است و اگر بیش از ۴ سرور فیلتر شود روش میانگین نسبت به بقیه بهتر است. نکته قابل توجه این‌که در تمامی این مرحله از آزمایش روش کمینه بدترین وضعیت را داشته است که می‌توان علت آن‌را بدین گونه تفسیر کرد که سرورهای فیلترشده دارای کمترین شباهت به ترافیک اصلی شبکه بات هستند. از این‌رو، روش کمینه فقط سرورهای فیلترشده بیشتر را گزینش می‌کند و بدین ترتیب، نتیجه کارش مطلوب نمی‌باشد. در شکل (۱۱- ب) اعمال انواع فیلترینگ بر روی چهار سرور نیابتی نشان داده شده است. سرور نیابتی پنجم که در معرض فیلترینگ قرار نداشته است، نزدیک‌ترین شباهت را نسبت به ترافیک شبکه بات از خود نشان داده است. به عبارتی، در چنین شرایطی، روش بیشینه می‌تواند بهترین گزینه باشد که بسیار مورد خاصی است. در شکل (۱۳) نتایج سه روش تخمین نسبت به ترافیک شبکه بات قابل ملاحظه است که روش میانگین ۳ به ترافیک شبکه بات نزدیک‌تر است.

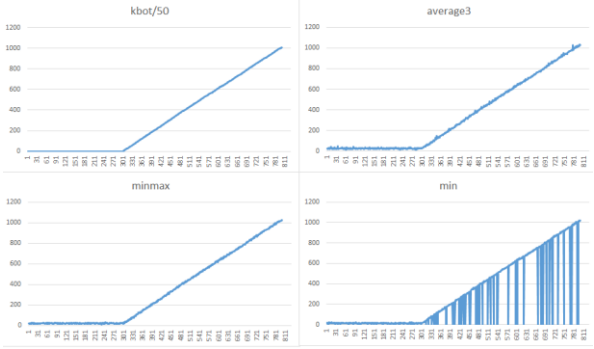


شکل (۱۳): مقایسه سه روش تخمین شبکه بات در وضعیت فیلترینگ

۴-۳-۵- سناریوی تأثیرات خرابی

این آزمایش به دنبال یافتن تأثیرات خراب‌شدن سرورهای نیابتی و از دسترس خارج‌شدن آن‌ها می‌باشد. از این‌رو، آزمایش با شرایط این‌که خرابی وجود نداشته باشد یا این‌که از یک تا پنج سرور خراب شوند که نتایج در بخش تحتانی جدول (۴) نشان داده شده است.

همان‌گونه که ملاحظه می‌شود اگر خرابی سرورها کمتر از سه سرور باشد، نتایج روش مین‌ماکس از بقیه مطلوب‌تر است و اگر بیش از سه سرور باشد روش میانگین‌گیری بهتر بوده و اگر هر پنج سرور خراب شود هیچ‌کدام مطلوب نمی‌باشند. در شکل (۱۱- ج) نمودار خرابی دو سرور نیابتی با احتمال ۵ ٪ نشان داده شده است. هم‌چنین، می‌توان نتایج سه روش تخمین را در شکل (۱۴) ملاحظه کرد. بدترین تخمین مربوط به روش کمینه است و بهترین آن مربوط به مین‌ماکس می‌باشد. حال با توجه به سه آزمایش مستقل انجام‌گرفته، به‌نظر می‌رسد در شرایط خاصی روش مین‌ماکس گزینه مطلوب‌تری باشد. از این‌رو، یک آزمایش ترکیبی با شرایط ویژه انجام می‌شود. با توجه به تشابه نتایج خرابی حسگرها و فیلترشدن مسیرها، آزمایش ترکیبی صرفاً از فیلترشدن مسیرها و گم‌شدن بسته‌ها انجام می‌گیرد

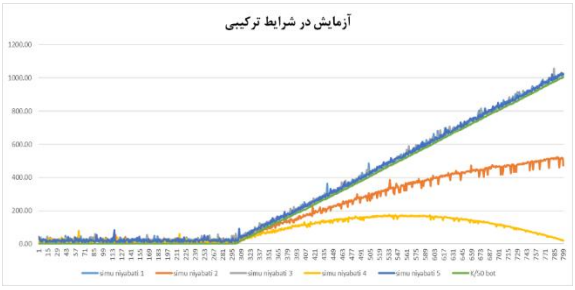


شکل (۱۴): سه روش تخمین در شرایط خرابی دو سرور نیابتی

به‌طوری‌که سه تا از سرور نیابتی در مسیرهای مطمئنی قرار گیرند که فیلتر نشده باشند. همچنین، سه تا از سرورهای نیابتی در مسیرهای قابل اطمینان بیشتری قرار گرفته باشند که بسته‌هایشان کمتر گم شوند. در بخش بعد به این آزمایش ترکیبی پرداخته می‌شود.

۴-۳-۶- سناریوی ترکیبی

در این مرحله سه روش ادغام در شرایط گم‌شدن بسته با دو احتمال ۵ ٪ و ۱۰ ٪ و فیلترشدن با دو احتمال ۵۰ ٪ و ۹۹ ٪ انجام می‌گیرد تا مشخص شود کدام روش از مقبولیت بهتری برخوردار است. نتایج آزمایش در جدول (۵) نشان داده شده است. همان‌گونه که در جدول (۵) ملاحظه می‌شود، روش کمینه بدترین نتایج را به‌دنبال دارد و همچنین روش میانگین‌گیری رتبه نزدیک‌تری به روش مین‌ماکس دارد؛ بنابراین، می‌توان ادعا کرد که روش مین‌ماکس در شرایط مفروض دارای مقبولیت بیشتری نسبت به سایر روش‌ها می‌باشد. در شکل (۱۵) نمودار ترکیبی برای فیلترشدن ۵۰ ٪ و ۱۰۰ ٪ روی دو سرور نیابتی و همچنین گم‌شدن بسته‌ها با نرخ ۱۰ ٪ روی همان دو سرور نیابتی نشان داده است.



شکل (۱۵): نمودار نتایج آزمایش ترکیبی برای فیلتر شدن ۵۰ ٪ و ۱۰۰ ٪ و گم‌شدن بسته ۱۰ ٪ روی دو سرور نیابتی

همان‌طور که ملاحظه می‌شود وجود فیلترینگ در مسیر سرورهای نیابتی دو و چهار موجب شده است تا تخمین ترافیک شبکه بات در حداکثر بی‌دقتی قرار گیرد. لذا دو منحنی مربوطه نسبت به منحنی ترافیک اصلی شبکه بات زاویه پیدا کرده است. همچنین، وجود نرخ ۱۰ درصدی ازدست‌رفتن بسته‌ها در دو سرور نیابتی دوم و چهارم باعث ایجاد اعوجاج در آن‌ها شده است. از طرفی سایر سرورهای نیابتی که معرض فیلترینگ و گم‌شدن بسته نیستند دارای منحنی قابل قبولی نسبت به منحنی ترافیک اصلی شبکه بات هستند.

جدول (۵): نتایج سه روش تخمین در شرایط ترکیب

آزمایش برای گم‌شدن بسته و فیلترینگ با درصدهای مختلف																		
آزمایش	فیلترینگ	۰ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵	۱ از ۵	۲ از ۵
	گم‌شدن بسته	۰ از ۵	۰/۰۵	۰/۰۵	۰/۰۵	۰/۰۵	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱	۰/۱
		۰ از ۵	۱ از ۵	۱ از ۵	۲ از ۵	۲ از ۵	۲ از ۵	۲ از ۵	۱ از ۵	۱ از ۵	۱ از ۵	۱ از ۵	۲ از ۵	۲ از ۵	۲ از ۵	۲ از ۵	۱ از ۵	۲ از ۵
فاصله اقلیدسی با تخمین	میانگین ۳ گزینه	۳۱/۸۲	۲۹/۶۳	۲۶/۵۰	۲۹/۶۹	۲۶/۹۲	۳۰/۴۴	۲۶/۰۸	۲۹/۷۶	۲۵/۵۵	۲۹/۲۳	۲۶/۸۲	۲۹/۹۴	۲۹/۷۶	۳۰/۳۰	۲۶/۳۸	۲۹/۶۰	۲۵/۷۵
	کمینه	۱۷/۵۱	۲۶۹/۰۴	۲۷۵/۸۷	۲۷۸/۷۳	۲۷۱/۴۶	۲۵۳/۳۷	۲۷۹/۵۸	۲۷۰/۱۰	۲۸۳/۷۲	۵۵۸/۹۸	۵۵۴/۶۶	۵۵۴/۰۲	۵۵۶/۲۵	۵۵۳/۸۸	۵۵۸/۳۰	۵۵۴/۰۶	۵۵۷/۶۶
	مین ماکس	۲۶/۰۷	۲۳/۰۷	۱۹/۳۱	۲۳/۵۲	۲۰/۳۸	۲۳/۳۹	۲۵/۳۲	۲۳/۵۵	۲۹/۲۰	۲۳/۱۴	۲۰/۲۵	۲۳/۳۳	۱۹/۹۶	۲۳/۶۶	۲۴/۷۶	۲۳/۴۹	۲۷/۴۸
نسبت مساحت	میانگین ۳ گزینه	۱/۰۵۲	۱/۰۴۸	۱/۰۴۳	۱/۰۴۸	۱/۰۴۳	۱/۰۴۹	۱/۰۴	۱/۰۴۸	۱/۰۳۸	۱/۰۴۸	۱/۰۴۳	۱/۰۴۸	۱/۰۴۳	۱/۰۴۹	۱/۰۴۱	۱/۰۴۸	۱/۰۳۸
	کمینه	۱/۰۲۸	۰/۶۶	۰/۶۴۹	۰/۶۴۸	۰/۶۵۳	۰/۶۸۳	۰/۶۴۶	۰/۶۵۷	۰/۶۳۷	۰/۲۷۵	۰/۲۷۹	۰/۲۸۲	۰/۲۷۷	۰/۲۸۲	۰/۲۷۵	۰/۲۸۱	۰/۲۷۵
	مین ماکس	۱/۰۴۳	۱/۰۳۷	۱/۰۲۹	۱/۰۳۸	۱/۰۲۹	۱/۰۳۸	۱/۰۲۲	۱/۰۳۶	۱/۰۱۴	۱/۰۳۷	۱/۰۲۹	۱/۰۳۷	۱/۰۲۸	۱/۰۳۸	۱/۰۲۲	۱/۰۳۶	۱/۰۱۷
دقت روش منتخب		۰/۹۷۲	۰/۹۶۳	۰/۹۷۱	۰/۹۶۲	۰/۹۷۱	۰/۹۶۲	۰/۹۷۸	۰/۹۶۴	۰/۹۸۶	۰/۹۶۳	۰/۹۷۱	۰/۹۶۳	۰/۹۷۲	۰/۹۶۲	۰/۹۷۸	۰/۹۶۴	۰/۹۸۳

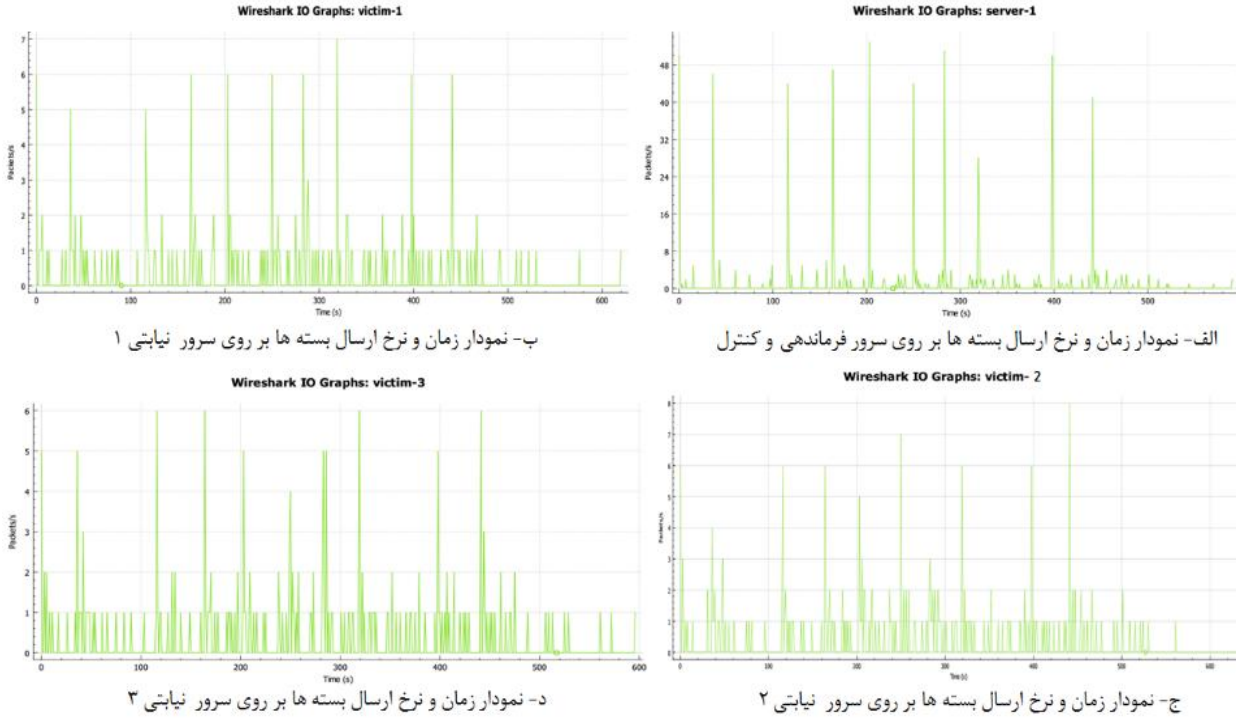
۴-۴- نتایج ارزیابی تلفیق اطلاعات شبکه حسگری نیابتی

با توجه به وجود فیلترینگ و خرابی حسگر، بهره‌گیری از یک حسگر نیابتی موجب کم‌شدن قابلیت اطمینان خواهد بود. از این‌رو، با افزونگی حسگرها و ادغام اطلاعات آن‌ها، قابلیت اطمینان بیشتر می‌شود. حال با توجه به نتایج حاصل از سه روش مذکور ادغام، در بخش فوقانی جدول (۴) نشان داده شد که روش مین‌ماکس در شرایط احتمال وقوع گم‌شدن بسته، از مقاومت بیشتری برخوردار است. همچنین، با توجه به بخش میانی و تحتانی جدول، درخصوص اعمال انواع فیلترینگ و خرابی سرورهای نیابتی، مشخص شد که هرقدر میزان فیلترینگ و خرابی بر تعداد مسیرهای سرور نیابتی بیشتر شود، مطلوبیت از روش مین‌ماکس به روش میانگین سه‌تایی میل می‌کند؛ بنابراین، می‌توان روش مطلوب را در گزینه مین‌ماکس جستجو کرد، به‌شرط آن‌که حداقل m تا از سرورهای نیابتی با احتمال کمی در معرض خرابی یا فیلترینگ قرار داشته باشند. لذا با چنین شرایط مفروضی، آزمایش‌های جدول (۵) نشان داد که گزینه مین‌ماکس از مقبولیت بهتری نسبت به روش‌ها برخوردار است به‌طوری‌که دقت آن را می‌توان بالای ۹۶ ٪ درنظر گرفت. از طرفی اگر اعمال فیلترینگ در مسیرهای بیشتری از سرورهای نیابتی رؤیت شود (درست تشخیص داده شود) می‌توان گزینه مطلوب را روش میانگین‌گیری ۳ تایی یا گزینه مقدار بیشینه درنظر گرفت.

۵- آزمایش حسگرهای نیابتی در محیط اینترنت

به‌منظور ارزیابی دقیق‌تر، آزمایش سرورهای نیابتی در محیط اینترنت انجام شد. در این آزمایش از سه سرور نیابتی در کشورهای آلمان، فرانسه و کانادا استفاده شد و با استفاده از یک سرور فرماندهی و کنترل که به ۲۴ بات مجهز بود، عمل ارسال بسته‌های علامت‌دار[1] به سرورهای نیابتی انجام گرفت. در این آزمایش، حمله‌ای در کار نبود (قربانی وجود نداشت) تنها شبکه بات به ازای هر یک دقیقه، یک بسته به سمت هریک از سه سرور نیابتی ارسال می‌کرد که این عمل ۱۰ بار تکرار شده است؛ بنابراین، هر سرور نیابتی باید از هر بات ۱۰ بسته دریافت کرده باشد و درمجموع، ۲۴۰ بسته در مدت ۱۰ دقیقه (به تعداد کلیه بات‌ها) گرفته باشد. در این آزمایش، کلیه بسته‌ها توسط نرم‌افزار تحلیل‌گر بسته وایرشارک[2] دریافت شده و مورد تجزیه و تحلیل قرار گرفت که در شکل (۱۶) نمودارهای زمانی و نرخ ارسال بسته‌های سرور فرماندهی و کنترل و سه سرور نیابتی نشان داده شده است.

1- Singed Packet
2- Wireshark Packet Analyzer



شکل (۱۶): نمودارهای زمانی و نرخ ارسال بسته‌ها در محیط وایرشارک

همچنین IP آدرس‌های مورد استفاده در جدول (۶) و نیز نتایج این آزمایش در جدول (۷) نشان داده شده است.

همان‌گونه که در جدول (۷) مشاهده می‌گردد، سرورهای نیابتی درمجموع به‌ترتیب ۲۲۳، ۲۱۴ و ۲۰۳ بسته دریافت کرده‌اند که این اختلاف بیانگر گم‌شدن بسته و فیلترینگ منطقه‌ای می‌باشد. بسته‌های گم‌شده به‌ترتیب ۷، ۱۶ و ۷ بسته (با نرخ ۳ ٪، ۷ ٪ و ۳٪) و فیلترینگ به‌ترتیب ۱، ۳ و ۱ تعداد برای هر سرور نیابتی بوده است. با توجه به نتایج حاصل‌شده (سرورهای نیابتی)، اگر مدنظر باشد که تخمینی از شبکه بات به‌دست آید لازم است ادغام داده صورت پذیرد که در بخش بعد به آن پرداخته می‌شود.

۵-۱- ادغام داده برای سرورهای نیابتی

در این مرحله با توجه به جدول (۸) لازم است با استفاده از روش‌های تلفیق برآورد نزدیکی از شبکه بات به‌دست آید. همان‌گونه که در شکل (۱۷- الف) ملاحظه می‌شود نمودار هیچ یک از سرورهای نیابتی شبیه به شبکه بات نمی‌باشد؛ بنابراین، نیاز به تلفیق داده دارد. با توجه به این‌که داده‌های دریافتی علامت‌دار بوده‌اند از این‌رو، با ترافیک کاربران عادی روبرو نبوده و در کار تأثیری ندارند. بنابراین، روش میانگین‌گیری، مقدار بیشینه و مقدار کمینه می‌تواند برای ادغام مورد آزمایش قرار گیرند. بعد از انجام آزمایش، نتایج حاصل از ادغام در سه سطر قسمت تحتانی جدول (۸) آمده است. همچنین برای ارزیابی تعیین درجه نزدیکی روش‌های ادغام از روش‌های فاصله اقلیدسی و نسبت مساحت‌ها استفاده شده است که نتایج حاصل در جدول (۹) آمده است.

جدول (۶): IP آدرس‌های مورد استفاده در محیط اینترنت

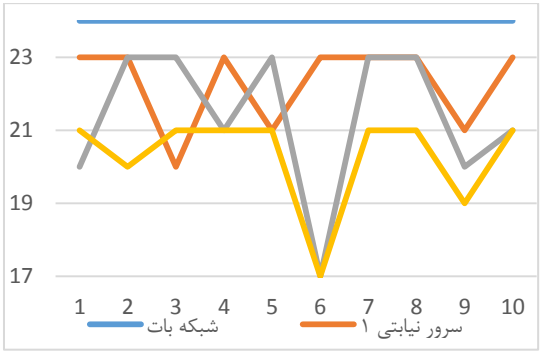
IP 1	45.40.143.57	IP 5	54.235.240.140	IP 9	69.164.212.64	IP 13	107.17.92.18	IP 17	198.56.238.128	IP 21	209.41.67.169
IP 2	52.91.132.109	IP 6	64.26.95.14	IP 10	70.254.226.206	IP 14	158.69.237.1	IP 18	199.227.40.31	IP 22	107.151.142.122
IP 3	54.67.52.36	IP 7	65.19.183.159	IP 11	76.72.124.100	IP 15	162.144.94.184	IP 19	207.5.112.114	IP 23	208.105.242.155
IP 4	54.200.51.124	IP 8	68.106.30.108	IP 12	104.239.228.149	IP 16	173.243.119.232	IP 20	207.91.10.234	IP 24	52.90.76.70

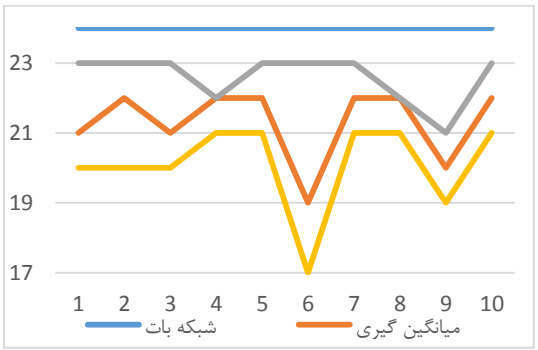
جدول (۷): نتایج آزمایش سرورهای نیابتی در محیط اینترنت

تعداد بسته‌های دریافتی توسط سرورهای نیابتی به ازای IP آدرس هر بات																								
IP	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵	۱۶	۱۷	۱۸	۱۹	۲۰	۲۱	۲۲	۲۳	۲۴
نیابتی ۱	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۵	۱۰	۱۰	۱۰	۱۰	۱۰	۸	۱۰	۱۰	۱۰	۱۰	۰
نیابتی ۲	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۷	۱۰	۶	۱۰	۱۰	۱۰	۱۰	۱۰	۸	۱۰	۱۰	۱۰	۳	۰
نیابتی ۳	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۱۰	۹	۱۰	۶	۱۰	۱۰	۱۰	۱۰	۱۰	۸	۱۰	۱۰	۰	۰	۰

جدول (۸): نتایج ادغام داده سرورهای نیابتی در محیط اینترنت

نتایج آزمایش بسته‌های دریافتی توسط سرورهای نیابتی	زمان (دقیقه)	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰
	شبکه بات	۲۴	۲۴	۲۴	۲۴	۲۴	۲۴	۲۴	۲۴	۲۴	۲۴
	سرور نیابتی ۱	۲۳	۲۳	۲۰	۲۳	۲۱	۲۳	۲۳	۲۳	۲۱	۲۳
	سرور نیابتی ۲	۲۰	۲۳	۲۳	۲۱	۲۳	۱۷	۲۳	۲۳	۲۰	۲۱
	سرور نیابتی ۳	۲۱	۲۰	۲۱	۲۱	۲۱	۱۷	۲۱	۲۱	۱۹	۲۱
روش‌های ادغام	میانگین‌گیری	۲۱	۲۲	۲۱	۲۲	۲۲	۱۹	۲۲	۲۲	۲۰	۲۲
	تخمین بیشینه	۲۳	۲۳	۲۳	۲۲	۲۳	۲۳	۲۳	۲۲	۲۱	۲۳
	تخمین کمینه	۲۰	۲۰	۲۰	۲۱	۲۱	۱۷	۲۱	۲۱	۱۹	۲۱





شکل (۱۷): الف) مقایسه داده سرورهای نیابتی با شبکه بات و ب) مقایسه تخمین‌های پیشنهادی با شبکه بات

بنابراین روش میانگین‌گیری، مقدار بیشینه و مقدار کمینه می‌تواند برای ادغام مورد آزمایش قرار گیرند. بعد از انجام آزمایش، نتایج حاصل از ادغام در سه سطر قسمت تحتانی جدول (۸) آمده است. همچنین، برای ارزیابی تعیین درجه نزدیکی روش‌های ادغام از روش‌های فاصله اقلیدسی و نسبت مساحت‌ها استفاده شده است که نتایج حاصل در جدول (۹) آمده است. همان‌گونه که ملاحظه می‌شود مقدار فاصله اقلیدسی تخمین بیشینه نسبت به سایر روش‌ها، کمتر بوده و نشان‌دهنده این است که شباهت بیشتری به ترافیک واقعی دارد. همچنین، نسبت مساحت‌ها نیز گویای دقت ۹۵ درصدی شباهت روش بیشینه نسبت به سایر روش‌ها می‌باشد.

جدول (۹): ارزیابی تعیین درجه نزدیکی روش‌های ادغام با نسبت مساحت

نسبت مساحت‌ها (درجه نزدیکی)			فاصله اقلیدسی		
مساحت کمینه	مساحت بیشینه	مساحت میانگین‌گیری	تخمین کمینه	تخمین بیشینه	میانگین‌گیری
۰/۸۵	۰/۹۵	۰/۸۹	۱۲	۴	۸/۵۴

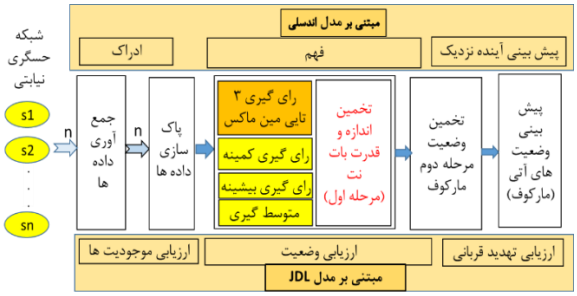
۵-۲- نتایج ارزیابی حسگرهای نیابتی

همان‌گونه که در بخش کارهای مرتبط اشاره شد، هیچ طرحی برای اندازه‌گیری عملکرد شبکه بات در حین حمله منع خدمت توزیع‌شده، ارائه نگردیده است. از این‌رو، نمی‌توان نتایج طرح پیشنهادی را با سایر طرح‌ها مورد مقایسه قرار داد. لذا تلاش شد با استفاده از سناریوهای مختلف (اعم از محیط شبیه‌ساز و محیط واقعی اینترنت)، صحت طرح پیشنهادی مورد ارزیابی قرار گیرد. بنابراین، با توجه به نتایج حاصل‌شده، روش‌های ادغام پیشنهادی در محیط اینترنت، توانستند درجه دقتی از ۸۵ ٪ تا ۹۵ ٪ را تخمین بزنند. از طرفی، وجود داده‌های علامت‌گذاری‌شده موجب حذف داده‌های ترافیک ناخواسته گردید و دقت اندازه‌گیری را افزایش داد. همچنین، به‌منظور بالابردن امنیت سرورهای نیابتی مناسب است درخصوص محل استقرار آن‌ها ملاحظاتی درنظر گرفته شود. این تمهیدات از قبیل این‌که به‌سختی مورد رصد قرار گیرند (به‌عنوان‌مثال از ماشین‌هایی که در کشورهای دیگر هستند

و نیز همکاری بین‌المللی ندارند، استفاده شوند) و احتمال ازکارافتادن آن‌ها بسیار کم باشد (قابلیت اطمینان زیادی داشته باشند) و درنهایت حافظه هارددیسک حس‌گرهای نیابتی را بلافاصله پس از بهره‌برداری، پاک کرد.

۶- نتیجه‌گیری

در بخش اول برای ارزیابی صحنه نبرد حملات منع خدمت، چارچوب در قالب شکل (۱) ارائه گردید. در این مرحله می‌توان ارزیابی صحنه نبرد مهاجم را در شکل (۱۸) پیشنهاد کرد. در این چارچوب، جمع‌آوری داده‌ها از شبکه حسگری نیابتی صورت می‌گیرد و سپس با پاک‌سازی داده‌ها (از بسته‌های ناخواسته) شرایط برای تلفیق اطلاعات برای تخمین اندازه و قدرت بات مهیا شود و با توجه به روند حمله می‌توان وضعیت‌های آتی (مانند تداوم حمله با توجه به ازدست‌رفتن بات‌ها) را تخمین زد. این چارچوب با مدل‌های اندسلی و JDL دارای سازگاری می‌باشد (شکل ۱۸).



شکل (۱۸): چارچوب ارزیابی صحنه نبرد حملات منع خدمت توزیع‌شده

تخمین قدرت شبکه بات در حین حمله برای مهاجم همواره یک چالش اساسی بوده و طرح‌های فعلی، اندازه‌گیری این تخمین را قبل یا بعد از حمله انجام می‌دهند که نمی‌تواند برای هدایت حمله مورد استفاده قرار گیرد. لذا طرح پیشنهادی درصدد رفع این چالش بوده است؛ بنابراین، نوآوری طرح شامل موارد ذیل است:

۱- امکان تخمین قدرت شبکه بات را در حین حمله را میسر می‌کند.

۲- حداقل سربار را برای شبکه بات و بخش C2 در بردارد.

۳- دقت تخمین آن بیشتر از ۹۵ ٪ می‌باشد.

۴- نتایج تخمین پیشنهادی نسبت به گزارش‌های رسیده از شبکه بات (در روش‌های موجود) واقعی و قابل اطمینان‌تر است.

۵- یک چارچوب برای ارزیابی صحنه نبرد حملات منع خدمت توزیع‌شده ارائه گردیده است.

ایده به‌کارگیری سرورهای نیابتی نشان داد که می‌توان تخمین مناسبی از قدرت شبکه بات را تا بیش از ۹۵ ٪ به‌دست آورد. درصورتی‌که بتوان از بسته‌های علامت‌دار در طرح سرورهای نیابتی استفاده نمود، روش مقدار بیشینه می‌تواند در روش رأی‌گیری گزینه مناسبی برای تخمین قدرت شبکه بات باشد. درصورتی‌که بسته‌ها علامت‌دار نباشند، با شرط این‌که حداقل m تا از سرورهای نیابتی با احتمال کمتر از ۱ ٪ در معرض خرابی یا فیلترینگ قرار داشته باشند، گزینه مین‌ماکس می‌تواند در روش رأی‌گیری انتخاب بهتری برای تخمین قدرت شبکه بات باشد. در غیر این صورت، اگر مدافعین شبکه قربانی با اعمال فیلترینگ بسته (دفاعی) در مسیرهای بیشتری از سرورهای نیابتی رؤیت شود (درست تشخیص داده شود)، روش رأی‌گیری به‌صورت میانگین‌گیری kتایی یا گزینه مقدار بیشینه می‌تواند نتیجه مطلوب‌تری را در تخمین قدرت شبکه بات دربر داشته باشد.

۷- مراجع

[1] M. R. Hasani Ahangar, and R. Jalaei, “A Analytical Survey on Botnet and Detection Methods,” Journal of Electronical & Cyber Defence, vol. 4, no. 4, Serial no. 16, IHU. AC. IR, 2017. (In Persian)

[2] B. Arne Welzel, “On Measuring the Impact of DDoS Botnets,” in EuroSec’14, Amsterdam, Netherlands, April 2014.

[3] S. Savage, “The Heisenbot Uncertainty Problem: Challenges in Separating Bots from Chaff,” in University of California, San Diego, 2008.

[4] C. Nordlohne, “Measuring Botnet Prevalence: Malice Value,” in University of Applied Sciences Gelsenkirchen, Germany, January 2015.

[5] S. Igor kotenko, “Agent Based Modeling & Simulation of Botnets and Botnet Defense,” in academic of sciences, conference of cyber conflict proceeding, Petersburg, Russia, 2010.

[6] I. Kotenko, “Agent-Based Modeling And Simulation Of Cyber-Warfare Between Malefactors And Security Agents In Internet,” St. Petersburg, Russia, 2005.

[7] C. Bannwart, “Predicting the Impact of Denial of Service Attacks,” August 2012.

[8] A. Terzis, “My Botnet is Bigger than Yours (Maybe, Better than Yours): why size estimates emain challenging,” in Computer Science Department Johns Hopkins University, 2008.

[9] C. Ping wang, “AN Advanced Hybrid Peer-to-peer Botnet,” in IEEE Transactions on dependable and secure computing, 2010.

[10] C. Wentao, "Measuring Botnets in the Wild: Some New Trends," in George Mason University, 2015.

[11] B. Gupta, "Estimating Strength of Ddos Attack Using Variou Regression Models," in springer, 2011.

[12] Y. Zhitang Li, "Measuring the botnet using the second character of bots," in Journal of Networks, vol. 5, no. 1, January 2010.

[13] L. McGuinness, "Ontology Development 101: A Guide to Creating Your First Ontology," in Stanford University, CA, 94305 , [http://protege.stanford.edu], Stanford, 2000.

[14] L. A. Klein, "Sensor and Data Fusion: A Tool for Information Assessment and Decision Making," in p. 53, SPIE Press, 2004.

[15] I. Christopher and D. Wickens Champaign, "Situation Awareness: Review of Mica Endsley's 1995 Articles on Situation Awareness Theory and Measurement," In Golden Anniversary Special Issue, University of Illinois, June 2008.

[16] N. Shouwan Gao, "Stability Analysis of Multi-Sensor Kalman Filtering over Lossy Networks," in Sensors (Basel, Switzerland), PMCID: PMC4851080, Apr. 2016.

[17] B. J. Norman, "A Study of Peer-To-Peer Botnets," in Master of Science in computer science, Utah State University, Major Professor: Dr. Chad D. Mano Department, 2008.

[18] E. M. M. Deza, "Encyclopedia of Distances," in Springer. p. 94, Cluster analysis, 2011.

Journal of Electronical & Cyber Defence
Vol. 6, No. 1, 2017, Serial No. 21

Estimation of a Botnet Using Vicarious Servers in Distributed Denial of Service Attacks

H. Akbari*, S. M. Safavi Hemami

*Imam Hossein University

(Received: 15/11/2016, Accepted: 01/05/2017)

ABSTRACT

Monitoring of attacks carried out by botnets still has challenges of uncertainty during the attack. In this study, we have proposed a methodology in which a Botnet sends some number of packets towards the hosts under its control (vicarious) across their network. Then, we can estimate the power of a botnet by data fusion. The existence of defensive filtering (local and regional), failure of sensors and packet loss cause faulty estimation. Thus, using the OMNET simulator, the proposed,model was tested with three scenarios and maximum-minimum and average voting procedures were used for data fusion. And the results were compared and evaluated using the Euclidean method which they showed that the Min-Max method is 95% accurate in such conditions. The above-mentioned experiment on the Internet environment showed that by utilizing labeled packets, the accuracy of 96 % is obtained.

Keywords: Botnet, Data Fusion, Cyber Sensors Network, Filtering, Uncertainty, Ddos, Shadow Host

* Corresponding Author Email: kphakbari@ihu.ac.ir