Supreme National Defense University Quarterly Journal of Defense Logistics and Technology

https://amfad.sndu.ac.ir E-ISSN: 2980-8073

Vol. 8, No. 4, Issue. 28, Winter 2025 **Received:** 2025/01/19 **Accepted:** 2025/02/15

Research paper

Early Detection of Botnet Attacks Using Network Traffic Analysis and Anomaly Detection

Maryam Rahimipour
M.Sc. in Software Engineering, Department of Software Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran (Corresponding Author)
Email: rahimipour.m@gmail.com
Afshin Firouzi
Ph.D. Candidate in Strategic Cyber Management, Department of Cybersecurity, Faculty of National Security, Supreme National Defense University, Tehran, Iran
Email: firouzy.af@gmail.com

Abstract
Internet malware has significantly increased its penetration capability and destructive potential through the use of distributed algorithms and computations. Among various types of malware, botnets are currently considered one of the most serious threats to Internet users worldwide. In a botnet architecture, the botmaster compromises vulnerable hosts and remotely controls them to launch a variety of large-scale attacks, including Distributed Denial of Service (DDoS) attacks, spam dissemination, identity theft, and other malicious activities against target victims. Botnets are resistant to detection mechanisms for several reasons, including traffic encryption, the use of standard communication protocols, and continuous code updates. Furthermore, most existing detection approaches identify botnets only during the final stages or attack phase. Early detection and identification of botnet traffic flows during the initial stages of botnet formation can play an important role in preventing the final attack phase and reducing the impact of botnet-related cybercriminal activities on cyber services. This paper proposes a novel architecture and algorithm for detecting botnets in the early stages of botnet network formation through the identification and adaptation of botnet traffic characteristics. To achieve this goal, network flows are first classified using the Levenshtein algorithm, and then anomalies in Command-and-Control (C&C) channel traffic are detected through analysis and matching with the composite indicators of botnet traffic flows. The proposed algorithm was evaluated under two scenarios in a real network environment and compared with existing botnet detection methods. The experimental results, including high detection rates of botnet traffic flows (92.60% in the first scenario and 90.57% in the second scenario) as well as 100% detection of infected systems within the network, demonstrate the effectiveness of the proposed algorithm in detecting botnet networks.

Keywords: Botnet, Early Detection, Command and Control, Traffic Analysis, Anomaly Detection

سال هشتم، شماره چهارم (پیاپی ۲۸)، زمستان ۱۴۰۴، صص. ۱۱- ۴۲
تاریخ دریافت: ۱۴۰۳/۱۰/۳۰ ـ تاریخ پذیرش: ۱۴۰۳/۱۱/۲۷

مقاله پژوهشی

تشخیص زودهنگام حملات بات‌نت با استفاده از تحلیل ترافیک شبکه و تشخیص ناهنجاری

مریم رحیمی‌پور
کارشناس ارشد مهندسی نرم‌افزار، گروه نرم‌افزار واحد علوم تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول)
Email: rahimipour.m@gmail.com

افشین فیروزی
دانشجوی دکتری مدیریت راهبردی فضای سایبر، گروه امنیت سایبری، دانشکده امنیت ملی، دانشگاه عالی دفاع ملی، تهران، ایران
Email: firouzy.af@gmail.com

چکیده

بدافزارهای اینترنت با استفاده از الگوریتم‌ها و محاسبات توزیع شده ضریب نفوذ و تخریب خود را افزایش داده‌اند. بات‌نت‌ها اکنون به‌عنوان گونه‌ای از بدافزارها، مهم‌ترین تهدید برای کاربران اینترنت در سراسر جهان محسوب می‌شوند. در ساختار بات‌نت، مدیر بات با تصرف میزبان‌های آسیب‌پذیر و کنترل آن‌ها از راه دور حملات مختلفی را در سطوح گسترده از قبیل حملات جلوگیری از سرویس توزیع شده، ارسال هرزنامه، سرقت هویت و سایر فعالیت‌های مجرمانه را بر روی قربانیان اصلی اجرا می‌نمایند. بات‌نت‌ها به دلایلی مانند رمزکردن ترافیک خود و استفاده از پروتکل‌های ارتباطی استاندارد و همچنین به‌روزرسانی مداوم کدها در مقابل روش‌های تشخیص مقاوم هستند و اکثر روش‌های ارائه‌شده برای تشخیص با توجه به رویکرد آن‌ها، بات‌نت‌ها را در مراحل نهایی و فاز حمله شناسایی می‌کنند. تشخیص و شناسایی جریان‌های بات نتی در مراحل نخست و شکل گیری آن می‌تواند کمک موثری به ممانعت از وقوع مرحله نهایی و تأثیرپذیری خدمات سایبری از فعالیت مجرمانه بات‌نت‌ها گردد. این مقاله با شناسایی و انطباق شاخصه‌های ترافیک بات‌نت، ساختار و الگوریتم جدیدی برای تشخیص بات‌نت در مراحل ابتدایی تشکیل شبکه بات ارائه می‌کند. برای این منظور پس از دسته‌بندی جریان شبکه با استفاده از الگوریتم لوناشتاین و تحلیل و انطباق آن با شاخص‌های ترکیبی جریان‌های بات نتی، به کشف ناهنجاری‌های جریان‌های کانال فرمان و کنترل می‌پردازد. الگوریتم پیشنهادی تحت دو سناریو در شبکه واقعی آزمایش و با روش‌های مطرح شناسایی بات‌نت‌ها مقایسه شده است. تحلیل نتایج آزمایشات و نرخ بالای تشخیص درست جریان‌های بات نتی (۹۲/۶۰٪ در سناریو نخست و ۹۰/۵۷٪ در سناریو دوم) و ۱۰۰٪ سیستم‌های آلوده در شبکه، حاکی از موفقیت الگوریتم پیشنهادی در تشخیص شبکه بات دارد.

کلیدواژه‌ها: بات‌نت، تشخیص زودهنگام، فرمان و کنترل، تحلیل ترافیک، ناهنجاری

20.1001.1.28212606.1404.8.4.1.2 https://amfad.sndu.ac.ir/ E-ISSN: 2980-8073

مقدمه

امروزه اینترنت به یک شبکه بسیار بزرگ، توزیع شده و ناهمگن تبدیل شده و تقریباً نقش عمده‌ای در زندگی روزمره افراد در سرزمین‌های مختلف و همچنین تداوم حیات سیاسی و اقتصادی دولت‌ها و سازمان‌ها دارد. وجود اطلاعات مهم و لزوم برقرار بودن ارتباط اینترنتی برای سازمان‌ها، زمینه و انگیزه به وجود آمدن تهدیدات و حملاتی را در اینترنت فراهم نموده است که به‌طورکلی با هدف کسب منافع و یا ضربه به دولت‌ها و یا سازمان‌ها صورت می‌گیرد (Sadeghi & Jin, 2018). با پیشرفت فناوری و استفاده از ساختارهای هوشمندانه و محاسبات توزیع شده، قدرت و دامنه حملات اینترنتی به‌صورت قابل ملاحظه‌ای افزایش یافته است و برقراری امنیت و حفاظت از اطلاعات سازمان‌ها به یک چالش بزرگ تبدیل شده است. تحقیقات نشان داده است بدافزارها مهم‌ترین عوامل حملات در فضای اینترنت هستند که در سال‌های اخیر به سمت سازمان‌دهی بهتر و سودمحوری بیشتر حرکت کرده‌اند (Wazzan et al., 2021). در مرکز بیشتر این حملات، گروهی از سیستم‌ها قرار دارند که تحت کنترل مهاجم درآمده و توسط وی از راه دور هدایت می‌شوند. این گروه از میزبان‌های آسیب‌پذیر تحت کنترل و مهاجم یک بات‌نت را تشکیل می‌دهند. بات‌نت در واقع به معنی شبکه‌ای از میزبان‌های آلوده به کدهای دودویی بات و ابزاری برای ترتیب دادن انواع حملات با وسعت زیاد در شبکه‌های کامپیوتری است (Koroniotis et al., 2018). زمانی که یک کامپیوتر به بات آلوده می‌شود، دیگر قادر به مقاومت در برابر دستورات مدیر بات و مهاجم نیست. در نتیجه مهاجم می‌تواند از امکانات و توان پردازشی میزبان‌های اشغال شده، به‌صورت توزیعی، بهره‌برداری کرده و انواع مختلفی از حملات را به‌صورت هماهنگ و با قدرت تخریبی بسیار بالا بر روی قربانی سازمان‌دهی و اجرا کند (Nguyen et al., 2020). برخلاف دیگر بدافزارها که به‌طور مستقل قادر به انجام مأموریت‌های بدخواهانه هستند، بات‌نت به یک زیرساخت ارتباطی نیاز دارد تا مدیر بات بتواند از طریق آن، دستورات و فرامین خود را برای بات‌ها ارسال کرده و پاسخ آن‌ها را دریافت کند. این زیرساخت ارتباطی کانال فرمان و کنترل نام دارد. در واقع بات‌نت، یک گروه هماهنگ از بات‌هایی است که از طریق کانال فرمان و کنترل

تحت مدیریت مهاجم، فعالیت‌های بدخواهانه‌ای را انجام می‌دهند. چرخه حیات بات‌نت‌ها از سه مرحله اصلی شکل‌گیری، فرمان-کنترل و حمله تشکیل شده است و در هر یک از این مراحل نوع فعالیت بات‌نت متفاوت است (Wazzan et al., 2021). در مرحله شکل‌گیری، میزبان‌های آسیب‌پذیر توسط فایل‌های آلوده‌سازی که از طرق و مکانیسم‌های مختلف انتشار به آن‌ها منتقل شده است به تصرف مهاجم درمی‌آیند. میزبان‌ها با اجرا شدن فایل آلوده به بات تبدیل و با استفاده از کانال‌های ارتباطی موجود و در نظر گرفته‌شده به بات‌نت ملحق می‌شوند. در مرحله فرمان و کنترل، مدیر بات دستورات خود را از طریق کانال‌های فرمان و کنترل به بات‌های تحت کنترل ارسال می‌کند. همچنین بات‌ها جهت اعلام زنده‌بودن، به‌روزرسانی و دریافت دستورات، به‌صورت دوره‌ای و منظم از طریق کانال‌های فرمان و کنترل با مدیر بات و یا سایر بات‌ها ارتباط برقرار می‌کنند (Meidan et al., 2018). مراحل شکل‌گیری و فرمان-کنترل، مراحل آغازین از چرخه حیات بات‌نت‌ها هستند و رفتار بدخواهانه‌ای از بات‌ها در این مراحل مشاهده نمی‌شود. در مرحله حمله سیستم‌های قربانی با توجه به آخرین دستورات دریافتی از مهاجم، فعالیت‌های بدخواهانه موردنظر مهاجم را انجام می‌دهند. عمده حملات صورت گرفته در این مرحله حملات انکار سرویس توزیع شده، سرقت هویت دسته‌جمعی، ارسال هرزنامه و سایر فعالیت‌های مجرمانه است (Nguyen et al., 2020). روش‌های مختلفی برای تشخیص بات‌نت‌ها پیشنهاد شده است که اکثر آن‌ها بات‌نت‌ها را در مرحله حمله و پس از اقدام به فعالیت بدخواهانه تشخیص می‌دهند همچنین بیشتر تحقیقات ارائه شده قابلیت پیاده‌سازی در شبکه واقعی را ندارند (Wazzan et al., 2021). با توجه به بررسی نتیجه مطالعات مرتبط که در بخش بعد ارائه می‌شود در حال حاضر، بیشتر روش‌های موجود برای تشخیص بات‌نت‌ها معمولاً در مرحله‌ای از چرخه حیات بات‌نت عمل می‌کنند که حملات مخرب به قربانیان آغاز شده‌اند. این مدل‌های تشخیص عمدتاً قادر به شناسایی حملات پس از وقوع آن‌ها هستند و این امر باعث می‌شود که پیشگیری از تهدیدات و حمله نهایی فراهم نباشد ازآنجایی‌که در بسیاری از موارد، فعالیت‌های مخرب بات‌نت‌ها از مرحله فرمان و کنترل آغاز می‌شود، شناسایی ناهنجاری‌ها در این مرحله می‌تواند

راه‌حلی کارآمد برای جلوگیری از حملات مبتنی بر بات‌نت باشد. در این مرحله، مهاجم به میزبان‌های آلوده دستورات خود را ارسال کرده و از طریق کانال‌های فرمان و کنترل ارتباط برقرار می‌کند؛ اما هنوز حملات مخرب شروع نشده‌اند. بنابراین، مسئله اصلی این است که نیاز به یک رویکرد پیشگیرانه برای شناسایی بات‌نت‌ها قبل از شروع حملات واقعی احساس می‌شود. در این مقاله برای حل مشکلات فوق یک ساختار و الگوریتم تشخیص بات‌نت مبتنی بر تحلیل آماری ترافیک شبکه و تشخیص ناهنجاری در مجموعه‌ای از جریان‌ها ارائه می‌شود که بات‌نت‌ها را با توجه به ناهنجاری‌های ترافیکی مرحله فرمان و کنترل و قبل از وقوع حمله به قربانی اصلی تشخیص می‌دهد. نوآوری این پژوهش مرتبط به رویکرد آن در خصوص مرحله مورد تحلیل جهت شناسایی شبکه بات و تشخیص پیشگیرانه پیش از وقوع حمله برخلاف روش‌های پیشین است. روش پیشنهادی ابتدا شامل دسته‌بندی جریان‌های شبکه با استفاده از الگوریتم لون‌شاتین است که به شناسایی شباهت‌ها بین جریان‌های شبکه کمک می‌کند. پس از دسته‌بندی، الگوریتم به تحلیل و انطباق این جریان‌ها با شاخص‌های ترکیبی جریان‌های بات‌نت پرداخته و ناهنجاری‌های موجود در کانال فرمان و کنترل را شناسایی می‌کند. این فرایند به شناسایی رفتار غیرعادی ارتباطات بین میزبان‌های آلوده و مدیر بات پرداخته و فعالیت‌های مشکوک را شناسایی می‌کند. الگوریتم پیشنهادی تحت دو سناریو مختلف در شبکه واقعی آزمایش شده است و نتایج نشان می‌دهد که این الگوریتم با دقت بالای ۹۲/۶۰٪ در سناریو اول و ۹۰/۵۷٪ در سناریو دوم، قادر به شناسایی بات‌نت‌ها و ۱۰۰٪ سیستم‌های آلوده است. این الگوریتم با موفقیت توانسته است بات‌نت‌ها را پیش از وقوع حملات در مراحل ابتدایی شناسایی کند، که این امر نسبت به روش‌های موجود که عمدتاً در مراحل نهایی حملات عمل می‌کنند، یک پیشرفت مهم در تشخیص زودهنگام تهدیدات محسوب می‌شود. در ادامه در بخش دوم، انواع بات‌نت و ویژگی‌های آن شرح و کارهای مرتبط در زمینه تشخیص بات‌نت به‌صورت مختصر معرفی می‌شود. در بخش سوم، ساختار و الگوریتم پیشنهادی معرفی می‌شود و در بخش چهارم، نتایج حاصل از آزمایشات

و پیاده‌سازی برای ارزیابی کارایی الگوریتم پیشنهادی ارائه شده و در بخش پنجم، نتیجه‌گیری به عمل می‌آید.

۱. پیشینهٔ پژوهش و کارهای مرتبط

۱-۱. انواع بات‌نت

بات‌نت‌ها براساس ساختار کانال‌های فرمان-کنترل به دو دسته متمرکز و غیرمتمرکز دسته‌بندی می‌شوند. در بات‌نت‌های متمرکز، یک یا چند میزبان با پهنای باند بالا، نقطه مرکزی و سرویس‌دهنده فرمان و کنترل برای همه بات‌ها هستند. بر روی این میزبان، سرویس‌های شبکه‌ای خاصی (از قبیل IRC یا HTTP) برای برقراری ارتباط با بات‌ها اجرا می‌شوند و از این طریق بات‌نت مرحله ارتباطات و هدایت توسط مدیر بات را سپری می‌کند (Manos et al., 2017; Paganini, 2017). علی‌رغم اینکه این ساختار یک ضعف اساسی دارد و با حذف این سرویس‌دهنده مدیر بات ارتباط خود با همه بات‌ها را از دست خواهد داد، اما این ساختار به دلیل راه‌اندازی سریع و آسان در اغلب بات‌نت‌ها استفاده می‌شود و اکثر بات‌نت‌ها با استفاده از این ساختار بات‌های خود را مدیریت می‌کنند (Manos et al., 2017; Paganini, 2017). در بات‌نت‌های غیرمتمرکز، زیرساخت ارتباطی به‌طور کامل بر روی تنها یک و یا چند سرویس‌دهنده فرمان و کنترل استوار نیست. در این نوع بات‌نت با شناسایی چند میزبان آلوده، کل بات‌نت در معرض خطر نابودی قرار نمی‌گیرد (Nguyen et al., 2020).

۱-۲. ویژگی‌های بات‌نت

- تمام بات‌نت‌ها از ساختار فرمان و کنترل برای ارتباط با مدیر بات استفاده می‌کنند. کانال‌های فرمان و کنترل عموماً برای سه هدف مورد استفاده بات‌نت‌ها قرار می‌گیرد. اعلام زنده بودن بات‌نت‌ها یکی از دلایل بهره‌گیری از این ساختار است که در آن بات‌ها در دوره‌های زمانی منظم با توجه به تنظیمات اعمالی مدیر بات شروع به ارسال

پیام‌هایی به مدیر بات می‌نمایند. دریافت تنظیمات و به‌روزرسانی بات‌نت از اهداف دیگر مرحله ارتباطات است (Wazzan et al., 2021).

- ❖ بهره‌گیری بات‌نت‌ها از پروتکل‌های ارتباطی موجود و استاندارد ویژگی دیگر بات‌نت‌ها است. بات‌نت‌ها در ساختار فرمان و کنترل خود و همچنین حملات صورت گرفته صرفاً از پروتکل‌های ارتباطی استاندارد مانند HTTP و IRC استفاده می‌کنند (Koroniotis et al., 2019).
- ❖ حجم ترافیک بات‌نت‌ها زیاد نبوده و تقریباً مشخصات جریان‌های عادی شبکه را دارند (McDermott et al., 2018).
- ❖ بات‌نت‌های جدید دارای خاصیت خود حفاظت‌کنندگی هستند. به‌این‌ترتیب که در مقابل روش‌های تشخیص بات‌نت به‌سرعت تغییر حالت می‌دهند و برای مدتی عملکرد و وظایف خود را متوقف کرده و با به‌روزرسانی کدهای خود مجدداً فعالیت خود را از سر می‌گیرند (Wazzan et al., 2021).
- ❖ یکی دیگر از ویژگی‌های بات‌نت‌ها استفاده از الگوریتم‌های پیچیده برای رمزنگاری محتوای ترافیک خود است. این الگوریتم‌ها در تمام ارتباطات مربوط به بات‌نت ازجمله بات‌ها با یکدیگر و مدیر بات مورد استفاده قرار می‌گیرد (Yin et al., 2019).
- ❖ بات‌های عضو یک بات‌نت معمولاً کدها، تنظیمات و دستورات یکسانی را اجرا می‌کنند و این موضوع باعث پیدایش رفتار گروهی هماهنگ و مشابهی در مراحل مختلف از چرخه حیات بات‌نت می‌شود. این فعالیت گروهی اختصاص به فعالیت‌های بدخواهانه بات‌نت ندارد و در مراحل آغازین چرخه حیات بات‌نت که هنوز بات در حمله‌ای شرکت نکرده است نیز مشاهده می‌شود (Meidan et al., 2018).

۱-۳. کارهای مرتبط

تحقیقات گسترده‌ای برای شناسایی و مقابله با بات‌نت‌ها انجام شده است که در این بخش به مهم‌ترین روش‌های ارائه‌شده پرداخته می‌شود.

«بات‌گاد»[1]: چوی و همکاران (۲۰۱۱) یک روش برخط و غیر نظارتی برای تشخیص بات‌نت‌ها پیشنهاد کردند که فعالیت‌های گروهی در ترافیک DNS را مانیتور می‌کند. این روش در شناسایی بات‌نت‌هایی که از آدرس‌های IP به‌جای نام‌های دامنه یا فقط در مرحله شکل‌گیری از DNS استفاده می‌کنند، محدودیت دارد (Choi et al., 2011).

روش «بات‌اونوس»[2]: یحیی‌زاده و همکاران (۲۰۱۲) با استفاده از بردارهای جریان ترافیک شبکه و الگوریتم خوشه‌بندی شعاع ثابت، روش بات‌اونوس را توسعه دادند. این روش به دلیل شباهت بالای بردارهای جریان تولیدشده توسط بات‌های یک بات‌نت، آن‌ها را شناسایی می‌کند (Yahyazadeh et al., 2012).

روش مبتنی بر رفتار: وانگ و همکاران (۲۰۱۳) سیستمی مبتنی بر بازشناسی الگوی فازی برای تشخیص بات‌نت‌ها ارائه کردند که با تحلیل رفتارهای فردی، نام‌های دامنه و آدرس‌های IP مخرب را شناسایی می‌کند (Wang et al., 2013).

روش «بات‌اسنیفر»[3]: زو و همکاران (۲۰۱۴) با تمرکز بر هماهنگی رفتارهای بات‌ها، الگوریتمی برای شناسایی کانال‌های فرمان و کنترل بات‌نت‌ها ارائه دادند. این روش از تحلیل همبستگی و شباهت در فعالیت بات‌ها برای شناسایی استفاده می‌کند (Zhou et al., 2014).

روش مبتنی بر خوشه‌بندی و تطبیق ترافیک: لو و همکاران (۲۰۱۵) با بهره‌گیری از مدل درخت تصمیم‌گیری، ترافیک بات‌نت‌ها را با ترافیک شناخته‌شده تطبیق داده و موارد نامطابق را خوشه‌بندی می‌کنند. این روش برای شبکه‌های بزرگ که دارای حجم بالای ترافیک هستند، چالش‌هایی در تطبیق ترافیک دارد (Lu et al., 2015).

روش‌های مبتنی بر یادگیری ماشین: استفاده از یادگیری ماشین، به‌ویژه الگوریتم‌های درخت تصمیم، کای نزدیک‌ترین همسایه و شبکه‌های عصبی، در سال‌های اخیر مورد توجه قرار گرفته است. اسمیت و همکاران (۲۰۲۰) با ترکیب این الگوریتم‌ها روشی ارائه دادند که دقت بالایی در شناسایی حملات بات‌نت نشان داد (Smith et al., 2020).

1. BotGAD
2. BotOnus
3. BotSniffer

روش‌های مبتنی بر شبکه‌های عصبی عمیق: جانسون و همکاران (۲۰۲۱) با استفاده از شبکه‌های عصبی عمیق (Deep Neural Networks) روشی برای شناسایی الگوهای پیچیده در ترافیک شبکه ارائه کردند. این روش قادر به شناسایی بات‌نت‌ها در مراحل اولیه چرخه حیات آن‌هاست (Johnson et al., 2021).

روش‌های مبتنی بر تحلیل گراف: کیم و همکاران (۲۰۲۲) از تحلیل گراف برای مدل‌سازی روابط بین گره‌های شبکه و شناسایی خوشه‌هایی که رفتار مشابهی دارند، استفاده کردند. این روش قابلیت تشخیص بات‌نت‌ها در شبکه‌های بزرگ و توزیع‌شده را افزایش می‌دهد (Kim et al., 2022).

روش‌های مرور شده، علی‌رغم تفاوت در الگوریتم‌ها و ویژگی‌های استخراج‌شده، بر تشخیص بات‌نت‌ها در مرحله نهایی حمله تمرکز دارند. این بدان معناست که این روش‌ها زمانی بات‌نت‌ها را شناسایی می‌کنند که فعالیت مخرب آن‌ها در جریان است. درحالی‌که این رویکردها برای کاهش اثرات بات‌نت‌ها مفید هستند؛ اما توانایی پیش‌بینی و جلوگیری از تشکیل بات‌نت‌ها یا شناسایی آن‌ها در مراحل اولیه را ندارند.

روش‌های مرور شده در پژوهش‌ها و مطالعات مربوط به تشخیص بات‌نت‌ها، علی‌رغم تفاوت‌های قابل‌توجه در الگوریتم‌ها، تکنیک‌های مورد استفاده و ویژگی‌های استخراج‌شده از داده‌ها، عمدتاً بر تشخیص بات‌نت‌ها در مرحله نهایی حمله تمرکز دارند. این بدان معناست که این روش‌ها معمولاً در مرحله‌ای از چرخه عمر بات‌نت‌ها وارد عمل می‌شوند که فعالیت‌های مخرب آن‌ها، مانند حملات گسترده یا سرقت اطلاعات، در حال انجام یا آشکار شده است. در چنین شرایطی، سیستم‌های تشخیصی می‌توانند اقدامات مفیدی برای کاهش اثرات مخرب بات‌نت‌ها و محدود کردن خسارات ناشی از آن‌ها انجام دهند.

بااین‌حال، این رویکردها از یک نقطه‌نظر استراتژیک، محدودیت‌هایی دارند. این روش‌ها معمولاً فاقد توانایی پیش‌بینی وقوع تهدیدهای ناشی از بات‌نت‌ها هستند و نمی‌توانند پیش از تشکیل کامل یا فعال‌سازی آن‌ها، این شبکه‌های مخرب را شناسایی کنند. به‌عبارت‌دیگر،

سیستم‌های فعلی در زمینه تشخیص بات‌نت‌ها در مراحل اولیه چرخه حیات آن‌ها، که شامل مراحل آماده‌سازی، گسترش و سازمان‌دهی است، کارایی کمتری دارند.

این مسئله از دو جهت حائز اهمیت است: نخست، تشخیص زودهنگام می‌تواند فرصت‌های بیشتری برای مداخله فعال و جلوگیری از پیشروی بات‌نت‌ها ایجاد کند و از تبدیل شدن آن‌ها به تهدیدات بزرگ‌تر جلوگیری کند. دوم، شناسایی بات‌نت‌ها در مراحل اولیه می‌تواند به سازمان‌ها کمک کند تا منابع و زیرساخت‌های خود را برای مقابله با این تهدیدات بهینه‌تر مدیریت کنند و از تحمیل هزینه‌های اضافی مرتبط با خسارات گسترده یا بازیابی سیستم‌ها پیشگیری کنند.

درمجموع، علی‌رغم مفید بودن این رویکردهای موجود در کاهش تأثیرات مخرب بات‌نت‌ها، نیاز به توسعه روش‌های پیشرفته‌تر و جامع‌تر احساس می‌شود. این روش‌ها باید قابلیت پیش‌بینی، شناسایی و مهار تهدیدات ناشی از بات‌نت‌ها را در مراحل اولیه چرخه عمر آن‌ها داشته باشند تا بتوانند به‌طور مؤثرتری امنیت سیستم‌ها و شبکه‌ها را تضمین کنند.

۲. تشخیص بات‌نت با استفاده از تحلیل ترافیک شبکه و تشخیص ناهنجاری

۲-۱. معماری سیستم پیشنهادی

در این بخش، معماری سیستم پیشنهادی برای تشخیص بات‌نت‌ها معرفی و توضیح داده می‌شود. با توجه به ماهیت ساختاری و چرخه حیات بات‌نت‌ها، می‌توان نتیجه گرفت که تشخیص و مقابله با بات‌نت‌ها در مرحله ارتباطات یا (C&C) یکی از مؤثرترین و کاربردی‌ترین راهکارها برای کنترل و مهار آن‌ها به شمار می‌رود. دلیل این امر، دو ویژگی مهم این مرحله از چرخه حیات بات‌نت است: نخست، مدت زمان طولانی که مرحله فرمان و کنترل معمولاً در آن جریان دارد و دوم، مشهود بودن نشانه‌های ناهنجاری و رفتارهای غیرعادی در این مرحله که آن را برای تحلیل و شناسایی مناسب‌تر می‌کند.

راهکار پیشنهادی بر پایه تحلیل ترافیک شبکه و بهره‌گیری از تکنیک‌های تشخیص ناهنجاری طراحی شده است. این روش به‌گونه‌ای عمل می‌کند که ابتدا جریان‌های شبکه

به‌دقت مورد تحلیل و پردازش قرار می‌گیرند. سپس در بازه‌های زمانی مشخص، این جریان‌ها با استفاده از الگوریتم‌های تشخیص ناهنجاری بررسی می‌شوند تا جریان‌هایی که رفتارهای غیرعادی و مشابه بات‌نت دارند شناسایی شوند. یکی از جنبه‌های کلیدی این روش، برخط بودن فرایند تشخیص است. برای دستیابی به این هدف، باید بازه‌های زمانی برای تحلیل جریان‌ها تا حد ممکن کوتاه و نزدیک به یکدیگر در نظر گرفته شوند، به‌طوری که تحلیل داده‌ها به‌صورت تقریباً آنی یا در زمان واقعی انجام شود. این امر اهمیت ویژه‌ای دارد زیرا بات‌نت‌ها می‌توانند در مدت زمان کوتاهی تغییر رفتار داده یا فعالیت خود را متوقف کنند و شناسایی دقیق و سریع در این شرایط حیاتی است.

شکل (۱)، ساختار معماری سیستم پیشنهادی را به تصویر می‌کشد و نحوه عملکرد اجزای مختلف آن را نشان می‌دهد. این معماری شامل ماژول‌های کلیدی برای جمع‌آوری و پردازش ترافیک شبکه، استخراج ویژگی‌های مرتبط و تشخیص ناهنجاری‌های مربوط به جریان‌های مشکوک است. چنین سیستمی نه‌تنها قادر است در مقابله با تهدیدات بات‌نت‌ها کارآمد باشد، بلکه می‌تواند به‌عنوان یک ابزار انعطاف‌پذیر و قابل گسترش برای تحلیل و شناسایی سایر تهدیدات سایبری نیز مورد استفاده قرار گیرد.

در مجموع، تمرکز این معماری بر تحلیل دقیق، بهینه‌سازی فرایندهای تشخیص و اطمینان از سرعت و دقت در شناسایی تهدیدات است که می‌تواند امنیت شبکه را به‌طور قابل ملاحظه‌ای ارتقا دهد.

الف) مدیر ترافیک: در ساختار پیشنهادی برای شناسایی و مدیریت جریان‌های شبکه، از سیستمی تحت عنوان «مدیر ترافیک» در نقطه‌ای استراتژیک از شبکه استفاده شده است. این نقطه استقرار، محل تلاقی و ارتباط بین شبکه داخلی و شبکه‌های خارجی است، که یکی از حیاتی‌ترین بخش‌های زیرساخت شبکه محسوب می‌شود. مدیر ترافیک به‌عنوان یک گلوگاه برای تمامی جریان‌های ورودی و خروجی به شبکه داخلی عمل می‌کند و به همین دلیل نقش کلیدی در نظارت و مدیریت ترافیک شبکه ایفا می‌کند.

با استفاده از این سیستم، تمامی جریان‌های داده‌ای که به شبکه داخلی وارد یا از آن خارج می‌شوند، از طریق مدیر ترافیک عبور می‌کنند. این ویژگی به مدیر ترافیک اجازه می‌دهد که اطلاعات کاملی از جریان‌های مختلف شبکه، ازجمله حجم داده‌ها، مقصد، مبدأ، پروتکل‌های مورد استفاده و سایر ویژگی‌های مرتبط را رصد و تحلیل کند. این قابلیت نه‌تنها امکان نظارت جامع و متمرکز بر جریان‌های شبکه را فراهم می‌کند، بلکه زیرساختی مناسب برای پیاده‌سازی سیستم‌های تشخیص ناهنجاری و شناسایی تهدیدات امنیتی نیز ایجاد می‌کند.

علاوه بر نقش اساسی خود در مدیریت ترافیک، این سیستم معمولاً به‌عنوان یک دیواره آتش نیز عمل می‌کند. به‌عبارت‌دیگر، مدیر ترافیک وظیفه کنترل دسترسی‌ها و اجرای سیاست‌های امنیتی شبکه را بر عهده دارد. این سیستم می‌تواند از ورود جریان‌های مخرب یا غیرمجاز به شبکه داخلی جلوگیری کرده و ارتباطات شبکه را مطابق با قوانین و پروتکل‌های تعیین‌شده تنظیم کند. یکی دیگر از مزایای استفاده از مدیر ترافیک، قابلیت آن در ثبت و ذخیره‌سازی اطلاعات جریان‌های شبکه است. این اطلاعات می‌توانند برای تحلیل‌های آتی، شناسایی الگوهای ناهنجار و حتی تحقیقات قانونی در صورت وقوع حملات سایبری مورد استفاده قرار گیرند. علاوه بر این، توانایی مدیر ترافیک در کنترل و مدیریت جریان‌ها، شبکه را در برابر تهدیدات خارجی مقاوم‌تر کرده و از اختلالات داخلی جلوگیری می‌کند. به‌طورکلی، سیستم مدیریت ترافیک نه‌تنها به‌عنوان یک نقطه حیاتی برای نظارت و مدیریت جریان‌های شبکه، بلکه به‌عنوان یک لایه محافظتی چندمنظوره عمل می‌کند. این سیستم با ترکیب قابلیت‌های دیواره آتش و ابزارهای نظارتی، نقش حیاتی در افزایش امنیت و بهره‌وری شبکه ایفا می‌کند و به‌طور مستقیم در ارتقای سطح کلی ایمنی سایبری شبکه نقش دارد.

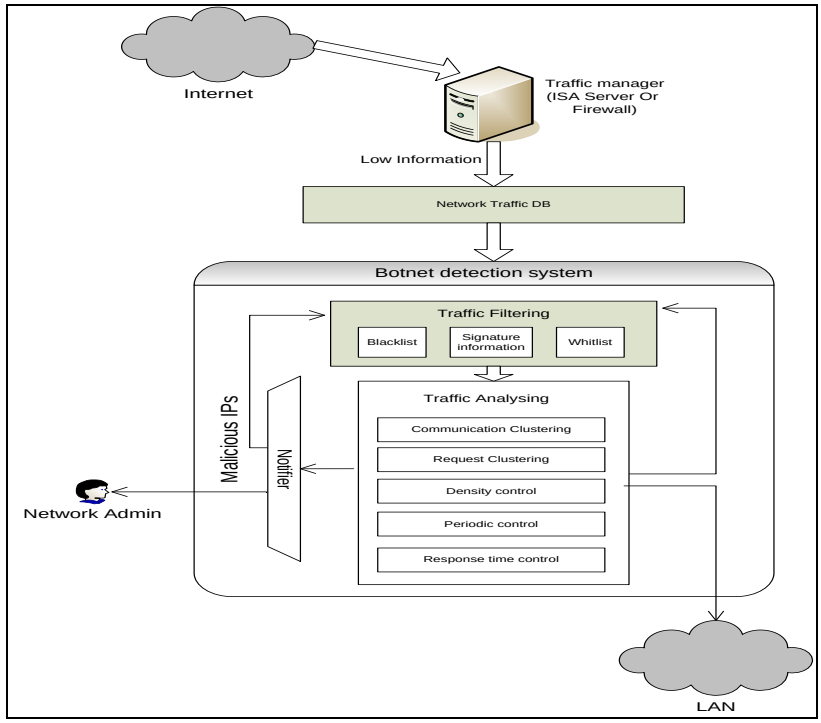
ب) بانک اطلاعاتی ترافیک شبکه: بانک اطلاعاتی ترافیک شبکه در معماری پیشنهادی به‌عنوان یک زیرساخت کلیدی برای نظارت، تحلیل و مدیریت جریان‌های داده طراحی شده است. این بانک اطلاعاتی به‌صورت برخط عمل می‌کند و اطلاعات تمام جریان‌هایی که از طریق مدیر ترافیک بین شبکه داخلی و شبکه‌های خارجی در حال عبور هستند، پیش از تحویل به مقصد نهایی در شبکه ثبت و ذخیره می‌کند. این ویژگی به سیستم امکان می‌دهد

تا یک دید جامع و دقیق از تمامی جریان‌های داده‌ای که وارد شبکه یا از آن خارج می‌شوند داشته باشد و به شناسایی سریع رفتارهای غیرعادی کمک کند.

اطلاعات ذخیره‌شده در این بانک شامل خلاصه‌ای از ویژگی‌های مهم هر جریان شبکه است که ازجمله آن‌ها می‌توان به آدرس مبدأ و مقصد، پروتکل مورد استفاده، حجم بسته‌های داده، زمان وقوع جریان و سایر خصوصیات مرتبط اشاره کرد. آدرس مبدأ و مقصد اطلاعات کلیدی‌ای را ارائه می‌دهند که به کمک آن‌ها می‌توان مسیر جریان‌ها و منشأ آن‌ها را شناسایی کرد. پروتکل مورد استفاده، نشان‌دهنده نوع ارتباط است و در تحلیل رفتار جریان‌ها و تشخیص ناهنجاری‌ها نقش مهمی دارد. حجم بسته‌های داده نیز می‌تواند سرنخ‌هایی درباره میزان فعالیت یا وجود رفتارهای مشکوک ارائه دهد. علاوه بر این، ثبت دقیق زمان شروع و پایان جریان‌ها به تحلیل‌های زمانی و شناسایی الگوهای مشکوک کمک شایانی می‌کند.

این بانک اطلاعاتی به دلیل برخط بودن، امکان نظارت و تحلیل آنی جریان‌های داده را فراهم می‌آورد. این ویژگی به‌خصوص در شرایطی که نیاز به پاسخ سریع به تهدیدات امنیتی وجود دارد، بسیار حیاتی است. به‌عنوان مثال، در صورت وقوع رفتارهای غیرعادی مانند حملات DDoS یا نفوذ به شبکه، اطلاعات موجود در این بانک می‌تواند برای شناسایی و مقابله فوری استفاده شود.

بانک اطلاعاتی ترافیک شبکه نه‌تنها برای شناسایی تهدیدات و نظارت امنیتی کاربرد دارد، بلکه ابزاری ارزشمند برای تحلیل عملکرد شبکه و بهینه‌سازی آن نیز محسوب می‌شود. این داده‌ها می‌توانند برای شناسایی گلوگاه‌ها، بهبود کارایی زیرساخت‌ها و حتی پیش‌بینی مشکلات احتمالی در آینده استفاده شوند. به‌طورکلی، این بانک اطلاعاتی به‌عنوان قلب سیستم نظارتی عمل می‌کند و با ثبت دقیق و ساختاریافته اطلاعات جریان‌های شبکه، امنیت و کارایی را به‌طور هم‌زمان بهبود می‌بخشد.



شکل ۱: معماری سیستم پیشنهادی تشخیص

ج) زیرسیستم فیلترینگ ترافیک: در ساختار پیشنهادی برای مدیریت و تحلیل ترافیک شبکه، مرحله فیلتر کردن جریان‌ها نقشی کلیدی در فرایند شناسایی و برخورد با تهدیدات ایفا می‌کند. اطلاعات تمامی جریان‌هایی که در بانک اطلاعاتی ذخیره شده‌اند و در رکوردهای مرتبط با خود جای گرفته‌اند، در این مرحله مورد بررسی دقیق قرار می‌گیرند. هدف اصلی این مرحله، دسته‌بندی جریان‌های شبکه براساس سطح اعتماد، تطابق با الگوهای بدخواهانه و ارتباط آن‌ها با حملات پیشین است.

در این فرایند، ابتدا اطلاعات جریان‌ها با دو مجموعه داده مهم مقایسه می‌شود :لیست آدرس‌های مطمئن و لیست آدرس‌های بدخواه که در طول دوره‌های قبلی تحلیل، شناسایی، ثبت و به‌روزرسانی شده‌اند. علاوه بر این، امضای جریان نیز که نمایانگر ویژگی‌های منحصربه‌فرد آن است، با الگوهای شناخته‌شده حملات قبلی مقایسه می‌شود. این مرحله سه حالت ممکن را برای تصمیم‌گیری در مورد جریان ایجاد می‌کند:

۱. حالت اول: جریان‌های مطمئن: اگر جریان مورد بررسی از یک مبدأ معتبر (مطابق با لیست آدرس‌های مطمئن) به مقصد یکی از سیستم‌های داخلی شبکه حرکت کند و هیچ تطابقی با الگوهای شناخته‌شده حملات قبلی نداشته باشد، این جریان به‌عنوان یک جریان مطمئن شناسایی می‌شود. در این حالت، بدون انجام مراحل آنالیز ترافیک، جریان به مقصد نهایی خود منتقل خواهد شد. این روش باعث کاهش بار پردازشی سیستم و تسریع در مدیریت جریان‌های سالم می‌شود.

۲. حالت دوم: جریان‌های بدخواه یا مشکوک به حمله: درصورتی‌که اطلاعات جریان با آدرس‌های موجود در لیست آدرس‌های بدخواه تطابق داشته باشد یا امضای آن با یکی از الگوهای حملات بات‌نت‌های شناسایی‌شده در گذشته هم‌خوانی داشته باشد، جریان به‌عنوان یک تهدید شناسایی می‌شود. در این حالت، سیستم به‌طور خودکار از ورود این جریان به شبکه داخلی جلوگیری می‌کند. این اقدام پیشگیرانه به حفظ امنیت شبکه کمک شایانی می‌کند و مانع از گسترش یا موفقیت حملات می‌شود.

۳. حالت سوم: جریان‌های ناشناخته: در برخی موارد، ممکن است جریان در هیچ‌یک از دسته‌بندی‌های فوق قرار نگیرد. به‌عبارت‌دیگر، آدرس مبدأ یا مقصد جریان در لیست آدرس‌های مطمئن یا بدخواه وجود ندارد و همچنین امضای جریان با الگوهای حملات قبلی مطابقت نمی‌کند. در چنین شرایطی، جریان به‌عنوان ناشناخته دسته‌بندی شده و برای بررسی بیشتر به مرحله تحلیل ترافیک منتقل می‌شود. در این مرحله، سیستم از تکنیک‌های پیشرفته مانند یادگیری ماشینی یا تحلیل ناهنجاری برای شناسایی رفتارهای مشکوک استفاده می‌کند. این مرحله از فرایند مدیریت ترافیک شبکه، تأثیر قابل‌توجهی بر امنیت و کارایی سیستم دارد. با دسته‌بندی جریان‌ها و تصمیم‌گیری سریع در مورد آن‌ها، سیستم می‌تواند منابع پردازشی خود را بر جریان‌های مشکوک متمرکز کند. همچنین، جلوگیری از ورود جریان‌های بدخواهانه در مراحل اولیه، ریسک حملات سایبری را به حداقل می‌رساند. علاوه بر این، انتقال جریان‌های ناشناخته به مرحله تحلیل پیشرفته، امکان شناسایی تهدیدات جدید و

به‌روزرسانی مداوم لیست‌های مطمئن و بدخواه را فراهم می‌کند. به‌طورکلی، مرحله فیلتر کردن جریان‌ها، ترکیبی از تحلیل سریع و مؤثر است که ضمن افزایش امنیت شبکه، به بهینه‌سازی عملکرد سیستم نیز کمک می‌کند. این فرایند نه‌تنها برای حفاظت از زیرساخت‌های شبکه در برابر تهدیدات شناخته‌شده مفید است، بلکه قابلیت شناسایی و مقابله با تهدیدات ناشناخته و نوظهور را نیز دارد.

۴. زیرسیستم تحلیل ترافیک: در مرحله تحلیل ترافیک، جریان‌ها براساس الگوریتمی که در بخش‌های بعدی به‌طور کامل در مورد آن بحث می‌شود مورد تحلیل و آنالیز قرار می‌گیرند. در این زیرسیستم که بخش اصلی و پردازشگر سیستم تشخیص پیشنهادی است ابتدا ارتباطات و درخواست‌ها بر طبق الگوریتم خاصی خوشه‌بندی می‌شوند، این خوشه‌بندی باعث به وجود آمدن گروه‌هایی از ارتباطات و جریان‌ها و اطلاعات آماری در خصوص هر گروه از ارتباطات و جریان‌ها می‌شود. سپس برای هر خوشه پارامترهایی مورد محاسبه قرار می‌گیرد و با توجه به مقادیر به دست آمده از این محاسبات و مقایسه آن‌ها با آستانه‌های تعیین شده جریان‌های بات‌نتی و بات‌ها شناسایی می‌شوند.

۵. زیرسیستم هشداردهنده: درصورتی‌که سیستم قادر باشد یک جریان خاص را به‌عنوان جریان بات‌نت‌ها شناسایی کند، به‌صورت خودکار از طریق سیستم هشداردهنده به مدیر امنیت شبکه اطلاع‌رسانی خواهد کرد. این اطلاع‌رسانی به مدیر امنیت کمک می‌کند تا هرگونه تهدید احتمالی یا حمله مرتبط با بات‌نت‌ها را به‌سرعت شناسایی و اقدامات لازم را برای مقابله با آن انجام دهد. علاوه بر این، سیستم به‌طور هم‌زمان آدرس مبدأ جریان را شناسایی کرده و آن را به لیست آدرس‌های بدخواه یا لیست سیاه اضافه می‌کند تا ازاین‌پس ارتباطات مرتبط با آن آدرس‌ها مسدود و کنترل شوند. این هشدار می‌تواند از طریق روش‌های مختلف به مدیر امنیت منتقل شود تا اطمینان حاصل شود که هشدار به‌موقع به دست وی خواهد رسید. یکی از روش‌های رایج برای اطلاع‌رسانی ارسال پیام الکترونیکی است که در آن تمامی جزئیات مرتبط با

جریان مشکوک و آدرس‌های شناسایی‌شده ارسال می‌شود. همچنین، امکان ارسال پیام کوتاه (SMS) به مدیران مربوطه نیز وجود دارد تا در صورت نیاز، هشدار به‌سرعت به دست آنان برسد.

در کنار این موارد، سیستم‌های مانیتورینگ شبکه که به‌طور مداوم وضعیت شبکه را پایش می‌کنند، می‌توانند آلارم‌های ویژه‌ای برای شناسایی و هشدار نسبت به فعالیت‌های غیرعادی مانند بات نت‌ها ایجاد کنند. این آلارم‌ها معمولاً به‌صورت گرافیکی در پنل‌های نظارتی نمایش داده می‌شوند تا مدیران امنیتی به‌راحتی بتوانند تهدیدات را شناسایی کنند. همچنین، این هشدارها می‌توانند شامل اطلاعات دقیق‌تری باشند، مانند نوع پروتکل مورد استفاده در جریان، پورت‌های مورد استفاده، حجم داده‌های ارسال‌شده، زمان وقوع رویداد و سایر جزئیات فنی که می‌تواند به تشخیص دقیق‌تر تهدید کمک کند. این فرایند به مدیر امنیت این امکان را می‌دهد که به‌صورت دقیق‌تری تهدیدها را تحلیل کرده و در صورت لزوم، اقدامات پیشگیرانه یا مداخله‌ای را در جهت مقابله با حملات انجام دهد.

به‌طورکلی، سیستم هشداردهنده نقش کلیدی در شناسایی و مدیریت تهدیدات ناشی از بات‌نت‌ها ایفا می‌کند و به مدیران امنیت این امکان را می‌دهد که سریعاً واکنش نشان دهند و از بروز آسیب‌های بیشتر جلوگیری کنند.

۲-۲. مراحل الگوریتم پیشنهادی برای تشخیص بات‌نت

۲-۲-۱. خوشه‌بندی ارتباطات

در این مرحله ابتدا براساس آدرس‌های مبدأ و مقصد خوشه‌هایی از ارتباطات تعریف می‌شوند. منظور از یک خوشه، ارتباطاتی است که بین دو آدرس IP مبدأ و مقصد برقرار هستند. بدیهی است تمام جریان‌هایی که از یک مبدأ خاص به یک مقصد خاص در حال حرکت باشند در یک خوشه و گروه قرار خواهند گرفت.

۲-۲-۲. خوشه‌بندی درخواست‌ها

پس از خوشه‌بندی ارتباطات در داخل هر seed یا خوشه اقدام به خوشه‌بندی درخواست‌ها می‌کنیم. منظور از خوشه‌بندی درخواست‌ها قرار دادن درخواست‌های مشابه هم که از یک مبدأ به یک مقصد جاری هستند در یک گروه است. در این مرحله درخواست‌هایی که از یک مبدأ به مقصدی خاص ارسال می‌شوند با استفاده از الگوریتم لون‌اشتاین (از الگوریتم‌های تطابق رشته) مورد بررسی قرار گرفته و پس از تعیین میزان مشابهت با توجه به آستانه‌ای که برای میزان مشابهت درخواست‌ها تعیین شده است در یک گروه قرار می‌گیرند. رابطه (۱)، میزان مشابهت درخواست‌ها را محاسبه می‌کند.

$$\text{ReqDist\_value(req1,req2)}=\frac{\text{Levenshttein Distance(req1,req2)}}{\text{Max(Len[req1],Len[req2])}} \qquad (۱)$$

که Levenshttein Distance(req1, req2) فاصله بین درخواست‌ها و به عبارت بهتر، کمترین تعداد جایگزینی‌های لازم جهت تبدیل رشته مربوط به یک درخواست به رشته درخواست دیگر را محاسبه می‌کند. (فاصله لون‌اشتاین، حداقل برابر تفاوت اندازه‌های دو رشته، حداکثر برابر اندازه طول رشته بلندتر و نیز برابر صفر است اگر و تنها اگر رشته‌ها یکسان باشند) سپس در مخرج کسر ابتدا Len[req1] و Len[req2] طول هر درخواست را محاسبه کرده و با استفاده از تابع Max نیز مقداری که بین Len[req1] و Len[req2] بزرگ‌تر باشد، برگردانده می‌شود. بدیهی است که هرچه مقدار ReqDist_value(req1,req2) نزدیک‌تر به صفر باشد دو درخواست، میزان مشابهت بیشتری باهم خواهند داشت و زمانی که ReqDist_value(req1,req2) مساوی صفر باشد دو درخواست کاملاً برابر خواهند بود. همچنین هرچه ReqDist_value(req1,req2) به یک نزدیک‌تر باشد درخواست‌ها مشابهت کمتری باهم خواهند داشت و زمانی که مقدار آن مساوی یک باشد، درخواست‌ها کاملاً متفاوت خواهند بود. پس می‌توان گفت کران بالا و کران پایین برای ReqDist_value به ترتیب یک و صفر خواهد بود. بررسی درخواست‌های ارسال شده در انواع بات‌نت‌ها نشان داده است که میزان ReqDist_value در بسیاری از بات‌نت‌ها برابر صفر است و اندکی از آن‌ها مقداری بیش از

صفر و کمتر از ۰/۳ خواهند داشت. این مقدار برای درخواست‌های مربوط به جریان نرمال همواره بالا و نزدیک به یک است [۱۴].

۲-۲-۳. محاسبه و کنترل میزان تراکم ارتباطات

در این بخش از الگوریتم با توجه به میزان ارتباطات قرارگرفته در هر گروه با توجه به مدت زمان مانیتور کردن ارتباطات تراکم ارتباطات محاسبه می‌شود. برای این منظور ابتدا تعداد پیشامد یا وقوع هر ارتباط با توجه به آمار ارتباطات مشابه در هر خوشه به‌دست‌آمده و سپس با تقسیم بر واحد زمان، تراکم ارتباطات از یک مبدأ به یک مقصد محاسبه می‌شود.

$$D = \frac{Fci}{\Delta t} \qquad (۲)$$

در رابطه (۲)، Fci فراوانی هر ارتباط و Δt برابر با مدت زمان مانیتور کردن ترافیک شبکه است. مقدار به دست آمده از رابطه (۲)، هرچه بزرگ‌تر باشد مسلماً تعداد ارتباطات برای ارتباط خاص مورد بررسی بالا خواهد بود. در الگوریتم پیشنهادی یک مقدار آستانه برای ارتباطات و تراکم آن تعیین می‌شود چنانچه مقدار D از مقدار آستانه در نظر گرفته شده بیشتر باشد، الگوریتم پیشنهادی این ارتباطات را به‌عنوان ارتباط مشکوک، جهت بررسی به مرحله بعد یعنی بررسی تراکم درخواست هدایت خواهد کرد در غیر این صورت به‌عنوان ترافیک نرمال به مقصد هدایت خواهد شد.

۲-۲-۴. محاسبه و کنترل میزان تراکم درخواست‌ها

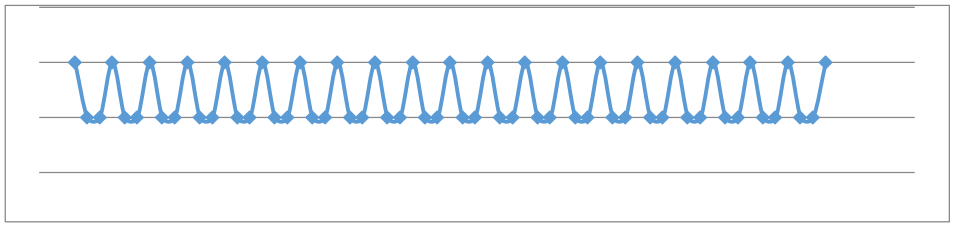
ارتباطات مشکوک در محاسبه و کنترل مرحله تراکم ارتباطات شناسایی شده و به این مرحله هدایت شده‌اند؛ همچنین جریان‌هایی که در خوشه‌بندی درخواست‌ها در یک گروه قرارگرفته بودند نیز مانند مرحله قبل از نظر میزان تراکم مورد بررسی قرار گرفته و چنانچه تراکم آن‌ها از مقدار آستانه تعیین‌شده برای درخواست‌های مشابه موجود در یک خوشه بیشتر باشد به‌عنوان درخواست‌های مشکوک به مرحله کنترل دوره‌ای بودن درخواست‌ها منتقل می‌شوند.

در این بخش نیز چنانچه تراکم به‌دست‌آمده برای درخواست‌های مشابه کمتر از حد آستانه تعیین شده باشد به مقصد هدایت می‌شوند.

۲-۲-۵. بررسی دوره‌ای بودن درخواست‌ها

درخواست‌های مشکوک که تراکم آن‌ها از حد آستانه تعیین شده بیشتر باشد جهت بررسی دوره‌ای بودن به این مرحله منتقل می‌شوند. منظور از دوره‌ای بودن ترافیک و درخواست‌ها به این معنی است که فاصله زمانی بین دو درخواست مشابه از یک مبدأ به یک مقصد مشخص در دفعات مختلف تکرار یکسان باشد. برای بررسی این موضوع درخواست‌های مشابه که در یک خوشه قرار گرفته و تراکم آن‌ها در مدت مانیتورینگ بیشتر از آستانه تعیین شده باشد به ترتیب زمان وقوع درخواست مرتب می‌شوند و سپس فاصله زمانی وقوع دو درخواست مشابه متوالی محاسبه می‌شود. چنانچه مقدار به دست آمده برای تعدادی از درخواست‌ها یکسان باشد این درخواست‌ها دوره‌ای خواهند بود. تعداد دفعات تکرار این فاصله و معیار تشخیص آن نیز براساس آستانه‌ای مشخص خواهد شد. البته ممکن است برخی از بات‌نت‌ها به دلایل مختلفی مثلاً عدم برخط بودن بات در طول دوره مانیتورینگ یا قطع بودن جریان شبکه و نهایتاً عدم ارسال و دریافت درخواست بات‌نتی در طول این مدت، فاقد جریان متناوب و دوره‌ای باشند که الگوریتم پیشنهادی برای پی بردن به این موضوع نیز راهکاری ارائه می‌کند. الگوریتم پیشنهادی برای بررسی دوره‌ای بودن درخواست‌ها از قوانین و روابط ریاضی تصاعد عددی یا حسابی بهره می‌برد. فاصله زمانی بین درخواست‌هایی که سیستم آلوده به بات آن در طول دوره مانیتور شبکه به‌طور کامل و منظم ارسال و دریافت درخواست داشته است می‌تواند قدرنسبتی برای واحد زمان باشد و با اضافه کردن این مقدار قدرنسبت، زمان بعدی وقوع درخواست مشابه را پیش‌بینی کرد. الگوریتم ما درخواست‌های مشابهی را که تراکم آن‌ها در مرحله کنترل تراکم بیش از حد آستانه مشخص باشد به ترتیب زمان وقوع درخواست مرتب می‌کند و از تفاضل زمان وقوع‌های متوالی یک مقدار تقریباً

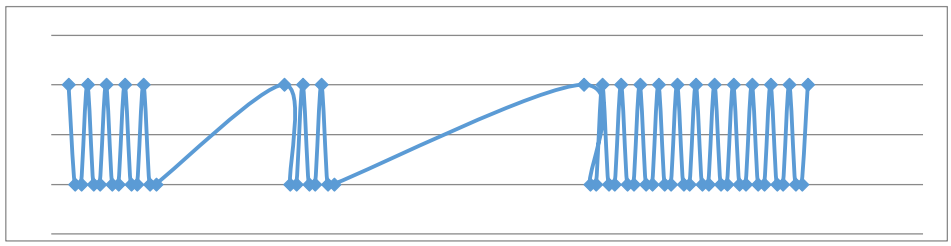
ثابت به دست می‌آید. این مقدار در جریان‌های منظم بات‌نتی دقیقاً ثابت و تکرارپذیر هستند. نمودار زمان وقوع درخواست‌های مشابه بات‌نتی در شکل (۲)، نمایش داده شده است.



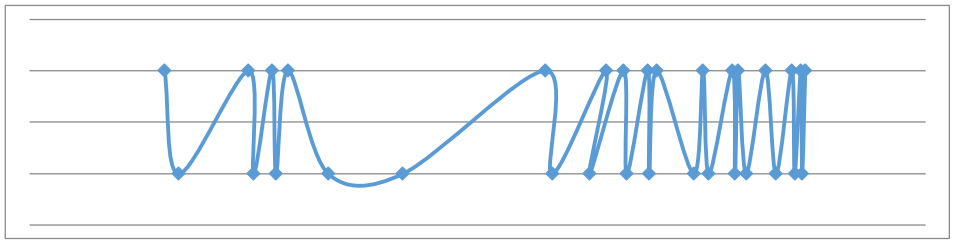
شکل ۲: نمودار زمان وقوع درخواست‌های مشابه در ترافیک بات‌نتی منظم

اما در بات‌نت‌هایی که ارسال و یا دریافت درخواست‌های بات‌نتی آن‌ها با وقفه مواجه شده است ممکن است فاصله زمانی ارتباطات متوالی ثابت نباشد و نهایتاً نتوان قدرنسبت ثابتی برای آن‌ها به دست آورد. برای حل این مشکل مانند جریان‌های منظم بات‌نتی، درخواست‌های مشابه حاصل از مرحله محاسبه تراکم درخواست‌ها را براساس زمان وقوع درخواست‌ها به‌صورت صعودی مرتب می‌کنیم. در لیست مرتب‌شده تمام حالت‌های ممکن تفاضل بین زمان‌های وقوع جریان‌ها محاسبه می‌شود، برای جریان‌های بات‌نتی حاصل این تفاضل‌ها باید تناسبی از یکدیگر باشند.

شکل (۳) و (۴) به ترتیب زمان وقوع درخواست‌های مشابه بات‌نتی نامنظم و ترافیک نرمال را نشان می‌دهند.



شکل ۳: نمودار زمان وقوع درخواست مشابه در ترافیک بات‌نتی نامنظم



شکل۴: نمودار زمان وقوع جریان نرمال

۲-۲-۶. کنترل زمان پاسخ‌گویی

جهت افزایش کارایی و دقت الگوریتم، لازم است زمان پاسخ‌گویی جریان‌ها نیز بررسی شوند. منظور از زمان پاسخ‌گویی مدت‌زمانی است که طول می‌کشد تا بات به جریانی که از بات‌سرور برایش ارسال می‌شود پاسخ دهد. در سیستم‌هایی که تحت مدیریت انسان قرار دارند مدت زمان پاسخ‌گویی بسیار بالا است. این زمان در سیستم‌هایی که تحت مدیریت یک کد دودویی قرار دارند در حد زمان واقعی و نزدیک به صفر بوده و مانند درخواست‌های دوره‌ای که فاصله بین جریان‌ها یکسان بود مقدار این زمان تقریباً در تمام جریان‌های بات‌نتی مقداری ثابت است. الگوریتم پیشنهادی ما پس از بررسی این موضوع جریان‌ها و درخواست‌های بات‌نتی و همچنین سیستم‌های آلوده به بات و بات‌سرور را شناسایی و معرفی می‌کند.

۲-۲-۷. پیاده‌سازی و بررسی نتایج

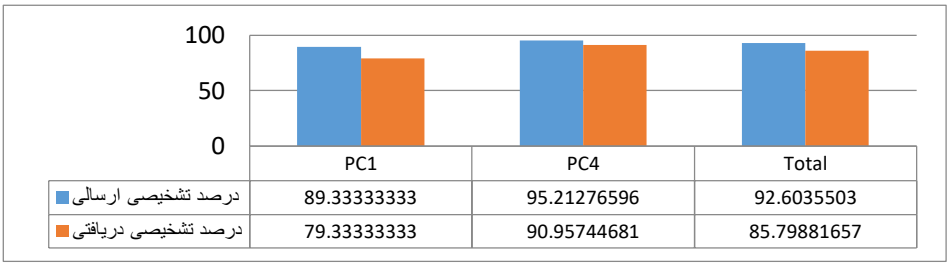
برای پیاده‌سازی الگوریتم پیشنهادی، تحلیل و آنالیز ترافیک و انجام آزمایشات و ارزیابی کارایی الگوریتم در تشخیص بات‌نت‌ها، در طول انجام تحقیق با چالش‌ها و محدودیت‌های مختلفی روبه‌رو بودیم. چالش اول راه‌اندازی زیرساخت لازم و به‌خصوص سیستم ایجاد شبکه بات به‌نحوی‌که ارتباطات و ترافیک بات‌نت را ایجاد نماید به همین دلیل صرفاً با دسترسی و بهره‌گیری از یک الگوی بات نتی توانستیم آزمایشات عملیاتی مربوطه را انجام

دهیم. چالش و محدودیت بعدی به فراهم آوردن شبکه‌ای واقعی از کامپیوترها که بتوان آزمایشات مختلف را بر روی آن پیاده‌سازی نمود، مربوط بود. دلیل این موضوع عدم امکان پیش‌بینی رفتار بات‌ها پس از آلوده‌سازی سیستم‌های رایانه‌ای در یک شبکه واقعی و احتمال عدم امکان قلع و قمع و پاک‌سازی سیستم‌های مذکور از فایل‌های آلوده و اکسپلویت‌ها بود. چالش نهایی تبدیل الگوریتم تحلیل ترافیک و تشخیص ناهنجاری پیشنهادی به یک برنامه قابل ارزیابی و دارای واسط کاربری مناسب جهت تشخیص زودهنگام بات‌نت‌ها و ارتباطات آن‌ها بود که با بهره‌گیری از برای پیاده‌سازی شبکه مورد آزمایش از ابزار مجازی‌سازی VMware استفاده کرده و در دو سناریو مختلف (۲ کامپیوتر آلوده در یک شبکه با ۴ کامپیوتر، ۴ کامپیوتر آلوده در یک شبکه با ۷ کامپیوتر) ترافیک نرمال را از طریق تزریق ترافیک مطمئن اینترنت به سیستم‌های مجازی و ترافیک آلوده را از طریق سیستم تولید بات‌نت zeus وارد شبکه نمودیم. برای ثبت ترافیک شبکه از نرم‌افزار wireshark استفاده کردیم. برای نگهداری اطلاعات ترافیک ثبت شده و تحلیل آن‌ها از بانک اطلاعاتی SQL Server 2019و نهایتاً برای تبدیل الگوریتم به برنامه نهایی از نرم‌افزارهای ساخت‌یافته برنامه‌نویسی زبان برنامه‌نویسی php استفاده کرده‌ایم.

با توجه به نتایج الگوریتم، میزان و درصد تشخیص بات در هر دو سناریو در جدول (۱)، آورده شده است. همچنین آمار مربوط به تشخیص جریان بات‌نتی در سناریوی اول و دوم در شکل (۵) و (۶) مشاهده می‌شود.

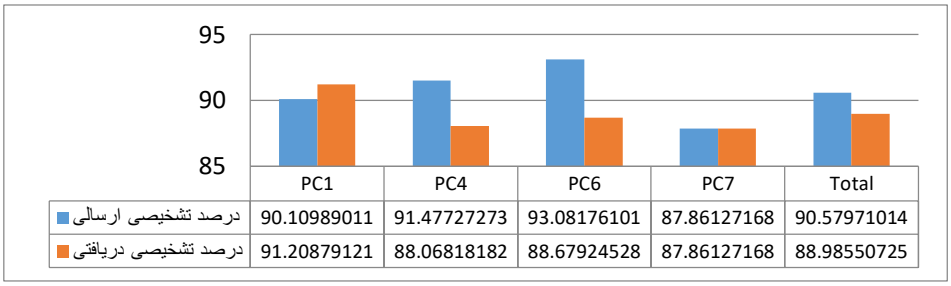
جدول ۱: میزان تشخیص بات توسط الگوریتم در سناریوهای مورد بررسی

	تعداد بات	تعداد بات شناسایی شده	درصد موفقیت الگوریتم پیشنهادی
سناریو اول	۲	۲	۱۰۰
سناریو دوم	۴	۴	۱۰۰



	PC1	PC4	Total
درصد تشخیصی ارسالی	89.33333333	95.21276596	92.6035503
درصد تشخیصی دریافتی	79.33333333	90.95744681	85.79881657

شکل ۵: میزان تشخیص جریان‌های بات نتی سناریوی اول



	PC1	PC4	PC6	PC7	Total
درصد تشخیصی ارسالی	90.10989011	91.47727273	93.08176101	87.86127168	90.57971014
درصد تشخیصی دریافتی	91.20879121	88.06818182	88.67924528	87.86127168	88.98550725

شکل ۶: میزان تشخیص جریان‌های بات نتی سناریوی دوم

نتایج به‌دست‌آمده در هر دو سناریو نشان داد که الگوریتم پیشنهادی قادر به شناسایی همه سیستم‌های آلوده و تشخیص بیش از ۹۰٪ جریان‌های بات‌نتی بوده است. برای غنی‌سازی تحلیل، چندین شاخص اضافی مانند نرخ هشدار نادرست، دقت و زمان پردازش مورد بررسی قرار می‌گیرند.

نرخ هشدار نادرست و تأثیر آن بر عملکرد الگوریتم: در آزمایشات، مشاهده شد که سیستم پیشنهادی نرخ هشدار نادرست بسیار پایینی دارد، که یک مزیت بزرگ نسبت به روش‌های مشابه است. نرخ هشدار نادرست به کمتر از ۲٪ کاهش یافت که نشان می‌دهد الگوریتم پیشنهادی به‌درستی ارتباطات مشکوک را از جریان‌های نرمال شبکه تفکیک کرده است. دلیل این موفقیت را می‌توان در بهره‌گیری از الگوریتم خوشه‌بندی لوناشتاین برای شناسایی جریان‌های مشابه و حذف داده‌های نرمال دانست.

تحلیل دقت الگوریتم پیشنهادی: دقت الگوریتم پیشنهادی نشان می‌دهد که چه تعداد از سیستم‌هایی که به‌عنوان آلوده تشخیص داده شده‌اند واقعاً آلوده بوده‌اند. براساس آزمایشات،

در سناریوی اول دقت ۹۶/۵٪ اندازه‌گیری شد و در سناریوی دوم دقت ۹۴/۸٪ بود. این ارقام بیانگر این است که الگوریتم پیشنهادی به‌خوبی از هشدارهای نادرست جلوگیری کرده و دقت بالایی در تشخیص باتنت‌ها دارد.

زمان پردازش و مقایسه با روش‌های موجود: یکی از مهم‌ترین عوامل در کاربردی بودن یک روش، زمان پردازش آن در محیط‌های عملیاتی است. نتایج بررسی‌ها نشان داد که در سناریوی اول، میانگین زمان پردازش هر جریان باتنتی ۱/۲ ثانیه و در سناریوی دوم، میانگین زمان پردازش هر جریان برابر ۱/۵ثانیه بوده است. این نتایج نشان می‌دهد که الگوریتم پیشنهادی به‌طور قابل‌ملاحظه‌ای سریع‌تر از بسیاری از روش‌های سنتی است که معمولاً به بیش از ۲/۵ تا ۳ ثانیه زمان پردازش برای هر جریان نیاز دارند.

تأثیر تحلیل دوره‌ای بودن و فاصله پاسخ‌گویی بر دقت شناسایی: در بررسی‌های انجام‌شده، تحلیل دوره‌ای بودن درخواست‌ها نقش مهمی در افزایش دقت الگوریتم داشت. مشاهده شد که ۸۰ درصد از باتنت‌های تحت بررسی، الگوی ارتباطی دوره‌ای داشتند. ۱۵ درصد دیگر دارای دوره‌های نامنظم بودند؛ اما همچنان الگوهای تکراری در فاصله‌های ارتباطی مشاهده شد. تنها ۵ درصد از جریان‌های مشکوک نامنظم بودند و نیاز به تحلیل‌های عمیق‌تر داشتند. این امر تأیید می‌کند که تحلیل دوره‌ای بودن درخواست‌ها و کنترل زمان پاسخ‌گویی یک معیار مؤثر برای تشخیص باتنت‌ها، حتی در شبکه‌های رمزگذاری شده است.

در ادامه مقایسه‌ای بین الگوریتم و ساختار پیشنهادی با سایر روش‌ها انجام پذیرفته است. با توجه به تنوع زیاد در شبکه‌های مورد ارزیابی، تفاوت در حجم و محتوای ترافیک شبکه، استفاده از باتنت‌های مختلف با ویژگی‌ها و رفتارهای متنوع و همچنین عدم وجود یک مجموعه داده استاندارد و مشترک برای ارزیابی الگوریتم‌ها، مقایسه مستقیم و عادلانه بین سیستم‌ها و الگوریتم‌های مختلف تشخیص باتنت به چالش کشیده می‌شود. این عوامل باعث می‌شوند که ارزیابی عملکرد دقیق و معتبر الگوریتم‌ها در شرایط مختلف دشوار باشد، چراکه عملکرد هر الگوریتم ممکن است بسته به شرایط شبکه، نوع حمله و ویژگی‌های باتنت‌ها متفاوت باشد. به همین دلیل، امکان ارائه یک مقایسه جامع و کلی برای تمامی

الگوریتم‌ها و سیستم‌ها غیرممکن است. ازاین‌رو، به‌جای مقایسه مستقیم کارایی سیستم‌ها، پیشنهاد می‌شود که ویژگی‌های مؤثر و مهم که در تشخیص بات‌نت‌ها در سیستم‌های مختلف تأثیرگذار هستند، مورد بررسی و تحلیل قرار گیرند. این ویژگی‌ها می‌توانند شامل دقت تشخیص، توانایی شناسایی حملات به‌صورت برخط و در مراحل اولیه، مقیاس‌پذیری الگوریتم‌ها و قابلیت انطباق با انواع مختلف حملات و پیکربندی‌های شبکه بر مبنای اعلام رسمی آن تحقیقات باشند.

با بررسی این ویژگی‌ها و تحلیل چگونگی عملکرد الگوریتم‌ها در شرایط مختلف، می‌توان نقاط قوت و ضعف هر سیستم را شناسایی کرده و درک بهتری از موفقیت یا محدودیت‌های آن‌ها در سناریوهای مختلف به‌دست آورد. این رویکرد به‌جای تمرکز صرف بر مقایسه کارایی، امکان ارزیابی دقیق‌تر و جامع‌تری را فراهم می‌آورد که در نهایت می‌تواند به بهبود طراحی و توسعه الگوریتم‌های تشخیص بات‌نت در شرایط متنوع کمک کند. جدول (۲)، این مقایسه را نشان می‌دهد.

جدول ۲: مقایسه ساختار پیشنهادی با الگوریتم‌های مطرح تشخیص بات‌نت

روش تشخیص	تشخیص بات‌نت ناشناخته	تشخیص برخط	نرخ هشدار نادرست پایین	تشخیص بات نت رمز شده
Botgad	✓	✓	✓	✓
Botminer	-	-	✓	✓
Dataadaptive	✓	✓	✓	-
Rishi	-	✓	-	-
Botprobe	-	✓	✓	-
Botsniffer	✓	-	✓	✓
ساختار پیشنهادی	✓	✓	✓	✓

ساختار پیشنهادی ارائه‌شده به دلیل تحلیل مشخصه‌های جریان کانال کنترل و فرمان و همچنین توجه به رفتار سیستم‌های شبکه، قادر به شناسایی بات‌نت‌های ناشناخته است. این قابلیت به‌ویژه ازآن‌جهت اهمیت دارد که بسیاری از روش‌های تشخیص قبلی به‌دلیل وابستگی به امضای شناخته‌شده یا ویژگی‌های ثابت، قادر به شناسایی تهدیدات جدید یا مبتنی بر تکنیک‌های نوین تغییر مسیر داده‌شده نیستند. در این راستا، روش پیشنهادی با تمرکز بر بررسی مجموعه‌ای از جریان‌های شبکه‌ای و تحلیل ویژگی‌های دینامیک آن‌ها، با در نظر گرفتن تغییرات رفتار سیستم در طول زمان، می‌تواند به‌طور مؤثر به شناسایی تهدیدات جدید پردازد.

این روش بر مبنای مقایسه میزان مشابهت جریان‌ها در شبکه، آن‌ها را در خوشه‌های مختلف طبقه‌بندی می‌کند. سپس با بررسی دقیق تراکم این خوشه‌ها و تحلیل رفتار دوره‌ای آن‌ها، قادر به شناسایی جریان‌های بات‌نتی و شبیه‌سازی‌های رفتاری خاص بات‌نت‌ها می‌شود. یکی از ویژگی‌های برجسته این الگوریتم، توانایی شناسایی بات‌نت‌های رمزنگاری‌شده است که در آن ارتباطات بین گره‌های بات‌نت به‌طور پنهانی و با استفاده از پروتکل‌های رمزنگاری انجام می‌شود. این ویژگی به‌ویژه در شرایطی که مهاجمان از روش‌های پیچیده برای پنهان‌سازی فعالیت‌های خود استفاده می‌کنند، اهمیت بسیاری پیدا می‌کند. الگوریتم پیشنهادی، جریان‌های شبکه را براساس میزان مشابهت، بدون وابستگی به الگوهای خاص داده‌کاوی یا تحلیل محتوای بسته‌ها، خوشه‌بندی کرده و سپس با بررسی ویژگی‌های رفتاری نظیر تراکم و دوره‌ای بودن ارتباطات، به شناسایی جریان‌های مرتبط با بات‌نت‌ها می‌پردازد. این رویکرد، برخلاف روش‌های متکی بر تحلیل محتوا وابستگی به رمزگشایی محتوای ترافیک ندارد و از ویژگی‌های رفتاری ارتباطات برای شناسایی الگوهای مخفی و ناهنجاری‌های ترافیکی استفاده می‌کند. بسیاری از روش‌های سنتی تشخیص بات‌نت، برای شناسایی حملات نیاز به دسترسی به محتوای بسته‌های شبکه دارند. این روش‌ها در مواجهه با ترافیک رمزگذاری شده دچار ضعف می‌شوند، زیرا نمی‌توانند محتوای پیام‌های ردوبدل شده را تحلیل کنند؛ اما در الگوریتم پیشنهادی، تمرکز بر تحلیل ویژگی‌های متادیتا و رفتار

ارتباطی بات‌نت‌ها است که مستقل از محتوای بسته‌ها عمل می‌کند. در واقع روش پیشنهادی حتی در صورت رمزنگاری کامل محتوا، همچنان می‌تواند بات‌نت‌ها را شناسایی کند، چراکه رمزنگاری تغییری در الگوی رفتاری ارتباطات ایجاد نمی‌کند. بر همین اساس می‌توان گفت قابلیت شناسایی بات‌نت‌های رمزگذاری شده را نیز دارا است.

علاوه بر این، روش پیشنهادی دارای نرخ تشخیص درست بسیار بالا و نرخ تشخیص نادرست نزدیک به صفر است. این به‌معنای دقت بالا در شناسایی تهدیدات واقعی و جلوگیری از هشدارهای غلط است. با استفاده از مانیتورینگ ترافیک شبکه و تحلیل لحظه‌ای جریان‌های داده، این روش قادر است ارتباطات مشکوک را شناسایی کرده و به‌طور سریع و مؤثر بر آن‌ها الگوریتم‌های تشخیص اعمال کند. ازآنجاکه این فرایند در زمان‌های نزدیک به زمان واقعی صورت می‌گیرد، می‌توان از آن برای شناسایی و مقابله با بات‌نت‌ها در محیط‌های برخط و پویا بهره گرفت.

در نهایت، این ساختار به دلیل توانایی در شناسایی سریع تهدیدات، تطبیق‌پذیری بالا با شرایط مختلف شبکه‌ای و توانمندی در شناسایی بات‌نت‌های ناشناخته و رمزنگاری‌شده، به‌عنوان یک ابزار کارآمد در امنیت شبکه‌های پیچیده و در حال تغییر مطرح است. این رویکرد می‌تواند به‌طور مؤثر در سیستم‌های مانیتورینگ و پیشگیری از حملات سایبری به‌ویژه در شبکه‌های حساس و با سطح امنیت بالا مورد استفاده قرار گیرد.

۳. نتیجه‌گیری و پیشنهاد

بات‌نت ساختاری برای اجرای حملات مخرب در گستره وسیع است. علی‌رغم اینکه آمار حمله‌های صورت گرفته با استفاده از بات‌نت بسیار بالا است، روش‌های تشخیص و مقابله با حملات مبتنی بر بات‌نت علاوه بر محدودیت‌ها و تشخیص دیرهنگام بات‌نت، اغلب قابل پیاده‌سازی نبوده و در حد نظریه و شبیه‌سازی ارائه شده‌اند. در این مقاله یک ساختار و الگوریتم تشخیص بات نت معرفی شد که با توجه به مشخصه‌های ترافیکی و ناهنجاری حاصل از ارتباطات مرحله فرمان–کنترل قادر به تشخیص بات نت قبل از مرحله حمله اصلی است. سیستم پیشنهادی به دنبال ناهنجاری در مجموعه‌ای از ترافیک بوده و براساس

ویژگی‌های اختصاصی ترافیک بات‌نتی، ترافیک مورد رصد را آنالیز می‌کند. الگوریتم پیشنهادی در یک شبکه واقعی پیاده‌سازی و مورد آزمایش قرار گرفت. نقطه قوت سیستم پیشنهادی توانایی تشخیص کامل بات‌ها و همچنین تشخیص بات نت در مراحل آغازین چرخه حیات آن است. برای تحقیقات آینده، پیشنهاد می‌شود الگوریتم‌های خوشه‌بندی با کاهش پیچیدگی و استفاده از یادگیری عمیق بهبود یابند. شناسایی باتنت‌ها در محیط‌های رمزنگاری‌شده با تحلیل متادیتا و بررسی رفتار شبکه، آزمایش الگوریتم‌ها در شبکه‌های بزرگ مانند اینترنت اشیا و ترکیب با روش‌های یادگیری، از اولویت‌های تحقیقاتی در این حوزه است. همچنین توسعه روش‌هایی برای شناسایی بات‌نت‌های ترکیبی و چندلایه و یکپارچه‌سازی الگوریتم‌ها با سیستم‌های امنیتی موجود مانند سامانه‌های تشخیص و پاسخ در نقاط انتهایی و تشخیص و پاسخ گسترده، می‌تواند کارایی سیستم‌ها و الگوریتم‌های تشخیص و مقابله با بات نت‌ها را افزایش دهد. این اقدامات می‌توانند راهکارهای مؤثرتری برای مقابله با باتنت‌ها ارائه دهند.

Referencds

- Koroniotis, N., Moustafa, N., Sitnikova, E., & Slay, J. (2018). Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques. Computers & Security, 88, 101668.
- Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17(3), 48-60.
- Nguyen, H. T., Ngo, Q. D., & Le, V. H. (2020). PSI-rooted subgraph: A novel feature for IoT botnet detection using classifier algorithms. Computers & Security, 99, 102036.
- Wazzan, M., Algazzawi, D., Bamasaq, O., Albeshri, A., & Cheng, L. (2021). Internet of Things Botnet Detection Approaches: Analysis and Recommendations for Future Research. Applied Sciences, 11(5713).
- Manos, A., et al. (2017). Understanding the Mirai botnet. In Proceedings of the 26th USENIX Security Symposium. Vancouver, BC, Canada: USENIX Association. Retrieved from
- Paganini, P. (2017). The Hajime Botnet Continues to Grow and Implements a New Attack Technique. Security Affairs.
- Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Science Direct.
- McDermott, C. D., Majdani, F., & Petrovski, A. V. (2018). Botnet detection in the Internet of Things using deep learning approaches. IEEE.
- Yin, L., Luo, X., Zhu, C., Wang, L., Xu, Z., & Lu, H. (2019). ConnSpoiler: Disrupting C&C Communication of IoT-Based Botnet through Fast Detection of Anomalous Domain Queries. IEEE.
- Choi, H., Lee, H., Lee, H., & Kim, H. (2011). BotGAD: Detecting botnets by capturing group activities in DNS traffic. Computer Networks, 56(1), 20–33.
- Yahyazadeh, M., Azgomi, M. A., & Hashemi, H. (2012). BotOnus: An online unsupervised framework for detecting botnets. Journal of Computer Virology and Hacking Techniques, 8(3), 165–176.
- Wang, P., Sparks, J., & Zou, C. C. (2013). An advanced hybrid peer-to-peer botnet. IEEE Transactions on Dependable and Secure Computing, 10(2), 86–99.
- Zhou, X., Wang, Y., & Li, J. (2014). BotSniffer: Detecting botnet command and control channels. IEEE Transactions on Parallel and Distributed Systems, 25(3), 690–703.
- Lu, W., Tavallaee, M., & Ghorbani, A. A. (2015). Detecting botnets through network behavior analysis and anomaly detection. Journal of Network and Computer Applications, 36(2), 276–285.
- Smith, J., Johnson, R., & Lee, T. (2020). Machine learning for botnet detection: A hybrid approach using decision trees and KNN. Journal of Cybersecurity, 12(4), 345–362.
- Johnson, R., & Kim, S. (2021). Deep learning approaches for botnet detection in large-scale networks. IEEE Transactions on Information Forensics and Security, 16, 1574–1586.

- Kim, S., Park, H., & Lee, J. (2022). Graph-based analysis for botnet detection in distributed environments. Journal of Network and Systems Management, 30(2), 245–268.
- Sadeghi, A. R., & Jin, Y. (2018). Security challenges in the internet of things. Proceedings of the 55th Annual Design Automation Conference (DAC), 1-6.