Journal of New Technologies in Distributed Systems and Algorithmic Computing
Islamic Azad University of Sabzevar
E-ISSN: 3115-705X
https://sanad.iau.ir/journal/ntds

Review Article

Challenges and Solutions for Detecting and Preventing SYN Attacks in the Internet of Things

Vesal Firoozi [1] | Hassan Shakeri [2] | Hassan Raei Sani *[3]

[1]Department of Computer Engineerin, Ma.C., Islamic Azad University, Mashhad, Iran, V.firoozi@iau.ac.ir

[2]Department of Computer Engineerin, Ma.C., Islamic Azad University, Mashhad, Iran, Hassanshakeri@iau.ac.ir

[3]Department of Computer Engineerin, Ma.C., Islamic Azad University, Mashhad, Iran, H.raei@iau.ac.ir

Corresponding Author
*Hassan Shakeri, Associate Professor, Department of Computer Engineerin, Ma.C., Islamic Azad University, Mashhad, Iran, Hassanshakeri@iau.ac.ir

Main Subjects: Detecting and Preventing SYN Attacks
Received: 16 November 2024
Revised: 10 April 2025
Accepted: 29 April 2025

https://doi.org/10.82195/ntds.2025.1190576

Abstract

The number and applications of IoT devices have increased dramatically in recent years. This issue has caused a continuous increase in security risks and vulnerabilities associated with these devices. One of the main challenges in the Internet of things environment is the threat of distributed denial of service (DDoS) attacks. The SYN attack is one of the most important attacks of this type that has spread in recent years. Despite a lot of research in the field of detection and prevention of SYN attacks, attackers can easily evade detection mechanisms using advanced tools and techniques. This issue causes several problems in real-time detection of such deadly attacks. In this article, after the description of the SYN attack, the detection and prevention methods of this attack have been investigated in two groups of end host strategies and network based strategies. Finally, open issues and challenges that need the attention of researchers in this field are introduced. This research sheds light on the significant potential of various SYN attack methods in IoT and thus provides valuable insights to IoT security researchers.

Keywords: Internet of Things, Intrusion Detection, Distributed Denial of Service Attacks, SYN Attack.

فناوری های نوین در سیستم های توزیع شده و محاسبات الگوریتمی
دانشگاه آزاد اسلامی واحد سبزوار
E-ISSN: 3115-705X
https://sanad.iau.ir/journal/ntds

مروری

چالش‌ها و راهکارهای شناسایی و پیشگیری از حملات SYN در اینترنت اشیا

وصال فیروزی[1] | حسن شاکری*[2] | حسن راعی ثانی[3]

[1]گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران،
V.firoozi@iau.ac.ir

[2]گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران ،
Hassanshakeri@iau.ac.ir

[3]گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران ،
H.raei@iau.ac.ir

نویسنده مسئول
*حسن شاکری، دانشیار، گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران،
Hassanshakeri@iau.ac.ir

موضوع اصلی: شناسایی و پیشگیری از حملات SYN
تاریخ دریافت: ۱۴۰۳/۸/۲۶
تاریخ بازنگری: ۱۴۰۴/۱/۲۱
تاریخ پذیرش: ۱۴۰۴/۲/۹

چکیده:

تعداد و کاربردهای دستگاه‌های اینترنت اشیا در سال‌های اخیر به طور چشمگیری افزایش‌یافته است. این موضوع باعث افزایش مداوم خطرات و آسیب‌پذیری‌های امنیتی مرتبط با این دستگاه‌ها شده است. یکی از چالش‌های اصلی در محیط اینترنت اشیا، تهدید حملات انکار سرویس توزیع‌شده است. حمله SYN یکی از حملات مهم این‌گونه است که در سال‌های اخیر گسترش‌یافته است. باوجود تحقیقات فراوان در زمینه تشخیص و پیشگیری از حملات SYN، مهاجمان با استفاده از ابزارها و تکنیک‌های پیشرفته به‌راحتی می‌توانند از سازوکارهای تشخیص، فرار کنند. این موضوع باعث مشکلات متعددی در تشخیص بلادرنگ چنین حملات مهلکی می‌شود. در این مقاله، پس از شرح حمله SYN، روش‌های تشخیص و پیشگیری از این حمله در دو گروه راهبردهای میزبان پایانی و راهبردهای مبتنی بر شبکه، موردبررسی قرار گرفته است. در نهایت، موضوعات باز و چالش‌هایی که نیاز به توجه محققان این حوزه دارند، معرفی شده است. این تحقیق، پتانسیل قابل‌توجه روش‌های مختلف حملات SYN در اینترنت اشیا را روشن می‌کند و بینش‌های ارزشمندی را به محققان حوزه امنیت اینترنت اشیا ارائه می‌دهد.

https://doi.org/10.82195/ntds.2025.1190576

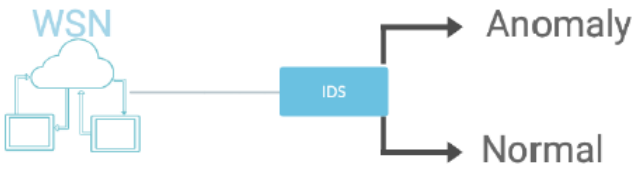
کلیدواژه‌ها: اینترنت اشیا، تشخیص نفوذ، حملات انکار سرویس توزیع‌شده، حمله SYN.

۱- مقدمه

با ظهور اینترنت اشیا[1] انتظار می‌رود تعداد و تنوع دستگاه‌های متصل به طور تصاعدی افزایش یابد. درحالی‌که این فناوری، نوید مزایای قابل‌توجهی را به کاربران می‌دهد که به طیف گسترده‌ای از برنامه‌های کاربردی جدید دسترسی خواهند داشت، درها را برای تعدادی از چالش‌های امنیتی، حریم خصوصی و ایمنی جدید باز می‌کند[۱]. تهدیدات، از جمله ایمنی فیزیکی و تهدیدات امنیتی شخصی، محدودیت‌های شدیدی در هزینه‌های سخت‌افزاری، استفاده از حافظه و مصرف انرژی دستگاه‌های اینترنت اشیا ایجاد کرده‌اند. این محدودیت‌ها منجر به بروز آسیب‌پذیری‌های امنیتی شده است که می‌توان با آن‌ها مقابله کرد [۲].

حفاظت از مجموعه‌های دستگاه‌های هوشمند، چالش‌های جدیدی را ایجاد می‌کند که بسیار فراتر از ایمن کردن هر یک از دستگاه‌های منفرد است. این چالش‌های جدید تا حدی از توانایی دستگاه‌های هوشمند برای کنترل جنبه‌های فیزیکی محیط خود و تا حدودی از تعامل آنها با یکدیگر و با شبکه ابری و مه ناشی می‌شود [۳]. در نتیجه، اجماع گسترده‌ای وجود دارد که امنیت یکی از چالش‌برانگیزترین الزامات برای سیستم‌های اینترنت اشیا آینده است [۴].

قطعاً باید از مجموعه دستگاه‌های هوشمند در برابر مشکلات امنیتی و حملات محافظت کرد و از یکپارچگی و محرمانه بودن داده‌های ذخیره‌شده حفاظت نمود. برای این منظور از سیستم‌های تشخیص نفوذ استفاده می‌شود. این سیستم‌ها قادرند هر حمله‌ای را از ترافیک عادی متمایز کرده و در صورت وقوع حمله، به کاربر هشدار دهند. یک سیستم تشخیص نفوذ که سازوکار کلی عملکرد آن در شکل ۱ ارائه شده است، تمامی فعالیت‌هایی را که با ترافیک عادی متفاوت هستند به عنوان ناهنجاری ثبت می‌کند. البته این سیستم‌ها ممکن است مستعد هشدارهای کاذب باشند. بنابراین، بسیار مهم است که سیستمی که توسعه می‌یابد، از دقت بالایی برخوردار باشد.



شکل ۱: سیستم‌های تشخیص نفوذ
Figure 1: Intrusion Detection Systems (IDS)

رایج‌ترین حملات در فضای اینترنت اشیا، حملات انکار سرویس[2] است. این حملات هیچ داده مرتبط با کاربر را تغییر نمی‌دهند و دسترسی غیرقانونی به آن‌ها نمی‌دهند، اما متکی به تعداد زیاد درخواست هستند تا ارتباط عادی کاربران قانونی را مختل کنند. حمله توزیع‌شده انکار سرویس[3] نوع جدیدی از حملات انکار سرویس است که به‌صورت توزیع‌شده اتفاق می‌افتد. حمله توزیع‌شده انکار سرویس یک تلاش مخرب برای ایجاد اختلال در ترافیک عادی سیستم قربانی است. هدف این نوع از حملات، ایجاد اختلال در سرویس، با ارسال بسته‌هایی بیش از ظرفیت ماشین‌های هدف است. مهاجمان از کامپیوترهای قربانیان با بدافزارها به سیستم‌های اینترنت اشیا نفوذ کرده و از آنها برای ارسال مقادیر زیادی بسته به سمت اهداف حمله استفاده می‌کنند. حملات توزیع‌شده انکار سرویس باعث ترافیک بالای شبکه با بسته‌های ارسال شده از طریق شبکه می‌شود و باعث می‌شود که سیستم به درخواست‌های کاربران عادی که می‌خواهند سرویس دریافت کنند پاسخ ندهد [۵]. حمله توزیع‌شده انکار سرویس یکی از بزرگ‌ترین تهدیدها برای برنامه‌های کاربردی مبتنی بر اینترنت و منابع آنهاست. هدف از این حمله ناتوان‌بودن خدمات مبتنی

[1] Internet of Things (IoT)
[2] Denial of Service (DoS)
[3] Distributed Denial of Service (DDoS)

بر اینترنت با انتقال حجم قابل‌توجهی از ترافیک است [۶]. در سال‌های اخیر حمله UDP[1]، حمله SYN[2] و حمله تقویتی[3]، سه نوع اصلی حملات توزیع‌شده انکار سرویس بوده‌اند [۷].

حمله SYN یکی از انواع حملات توزیع‌شده انکار سرویس است. در یک حمله SYN، مهاجم منابع دستگاه‌های اینترنت اشیا را با ارسال مکرر بسته‌های همگام‌سازی نیمه‌باز برای درخواست اتصال TCP پر می‌کند. این اتصالات برای ارتباط بیشتر باز می‌مانند. ماشین قربانی، با استفاده از تمام پورت‌های موجود، ممکن است به‌آرامی پاسخ دهد یا اصلاً به ترافیک قانونی پاسخ ندهد. یک حمله SYN از نقص‌های دست‌دادن سه‌طرفه TCP سوءاستفاده می‌کند. در اصل، مهاجم چندین درخواست SYN ارسال می‌کند؛ بنابراین سرور تمام منابع موردنیاز را بدون دریافت هیچ‌گونه ACK از مهاجم تخصیص می‌دهد. دست‌دادن سه‌طرفه TCP شامل سه بسته است که دارای پرچم‌های SYN و یا ACK تنظیم شده است. بسته اول فقط حاوی پرچم SYN است و از مشتری ارسال می‌شود. بسته دوم حاوی پرچم‌های SYN و ACK است و به‌عنوان تأیید شروع اتصال TCP از سرور ارسال می‌شود. بسته سوم فقط حاوی پرچم ACK است و از طرف مشتری ارسال می‌شود. حمله SYN به معنای تولید بسته‌های SYN متعدد است، ازاین‌رو سرور یک پورت را برای آن اتصال باز می‌کند؛ اما هرگز ACK را از مهاجم دریافت نمی‌کند. هنگامی‌که تمام پورت‌های سرور استفاده می‌شود، سرور از سرویس‌دهی به هرگونه کلاینت قانونی دیگر خودداری می‌کند [۸].

با توجه به اهمیت حمله SYN در اینترنت اشیا، در ادامه مقاله در بخش ۲، ضمن معرفی بدافزاهای حمله SYN، تحقیق‌های انجام شده در زمینه حمله SYN در اینترنت اشیا را دسته بندی و مرور می‌کنیم. چالش‌های پیش‌رو و همچنین فرصت‌های مطالعاتی آینده، در بخش ۳ بیان می‌شود و در بخش ۴ مقاله جمع‌بندی می‌شود.

۲- مرور کارهای پیشین

برای مرور کارهای انجام شده دررابطه‌با حمله‌های SYN در اینترنت اشیا، ابتدا بدافزارهای اینترنت اشیا باقابلیت حمله SYN را بررسی می‌کنیم، در ادامه روش‌های حمله SYN را در دو گروه دسته‌بندی می‌کنیم و راه‌حل‌های مقابله با حمله SYN را بررسی می‌کنیم.

در اینترنت اشیا، بدافزارهایی باقابلیت حمله SYN وجود دارند. در مورد بدافزارهای برجسته اینترنت اشیا باقابلیت حملات DDoS و حمله SYN در چند سال گذشته می‌توان به BASHLITE و Linux.Hydra اشاره کرد. Linux.Hydra یک ابزار منبع‌باز است که در سال ۲۰۰۸ به طور خاص با هدف‌قراردادن دستگاه‌های مسیریابی با استفاده از معماری MIPS معرفی شد. Linux.Hydra بر اساس فرهنگ لغت، حمله را انجام می‌دهد و اسامی و پسوردها را برای نفوذ ایجاد می‌کند. Linux.Hydra در مورد مسیریاب‌های D-Link، از یک آسیب‌پذیری شناخته‌شده احراز هویت سوء استفاده می‌کند. هنگامی‌که یک دستگاه در معرض خطر قرار می‌گیرد، به عنوان بخشی از یک شبکه مبتنی بر چت اینترنتی[4] یکپارچه می‌شود و می‌تواند یک حمله SYN را اجرا کند. اسناد بدافزار به توانایی Linux.Hydra برای راه اندازی یک حمله سیل UDP اشاره می‌کند، اما این قابلیت در منابع آنلاین مشهود نیست. اگرچه این بدافزار نسبتاً ساده است، اما پایه و اساس بدافزارهای بعدی MIPS را ایجاد کرده است [۹]. در سال ۲۰۱۴، بدافزار رایج BASHLITE از یک پروتکل ارتباطی ساده چت اینترنتی استفاده کرد که به طور گسترده برای ایجاد یک معماری بات نت مستقل از سرورهای چت اینترنتی، تغییر یافته و آن را به عنوان بدافزار مبتنی بر عامل[5] و نه مبتنی بر چت اینترنتی طبقه بندی کرد و طیف قابل توجهی از معماری‌های آسیب‌پذیر از جمله حملات توزیع‌شده انکار سرویس که شامل حملات سنتی سیل ACK، UDP و SYN را روی دستگاه‌های SPARC را به نمایش گذاشت [۱۰]. علاوه بر تحقیقات علمی در مورد دفاع در برابر حملات SYN، برخی از محصولات تجاری مبتنی بر ابر مانند Prolexic، CloudFlare، Cisco، Akamai و Arbor هم وجود دارند که در برابر انواع حملات انکار سرویس، دفاع می‌کنند.

---

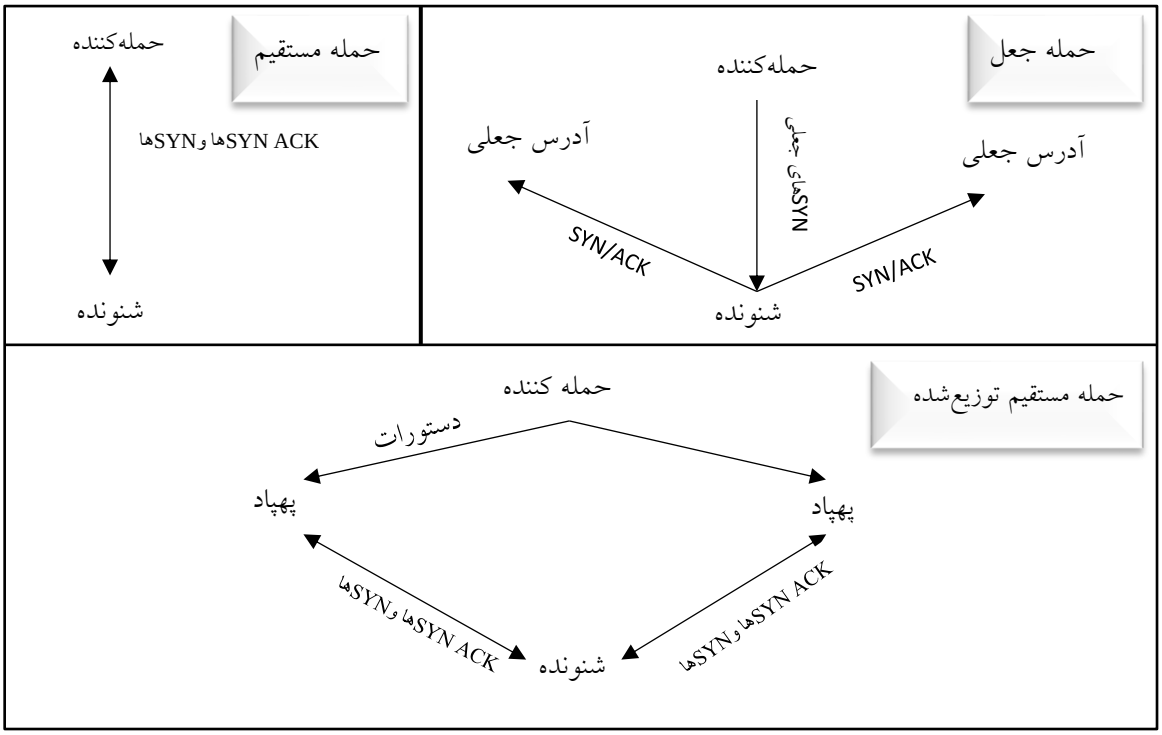
[1] UDP flooding

[2] SYN flooding

[3] Amplification

[4] Internet Relay Chat (IRC)

[5] Agent-Handlerbased



شکل ۲: انواع حمله‌های SYN [7].
Figure 2: Types of SYN Attacks

حملات SYN از نظر ساختار به سه دسته حمله مستقیم، حمله جعل و حمله مستقیم توزیع‌شده تقسیم می‌شوند که در شکل ۲ نشان داده شده است [۷]. حمله مستقیم شامل جعل یا تزریق بسته‌ها نیست، بلکه ایجاد چندین اتصال TCP با تماس[1] و جلوگیری از ارسال هرگونه پیام ACK، RST یا پروتکل پیام کنترل اینترنت ICMP توسط سیستم عامل است. این کار را می‌توان با ایجاد قوانین فایروال انجام داد که بسته‌های خروجی را فیلتر می‌کند و فقط SYNها را مجاز می‌کند یا بسته‌های ورودی را فیلتر می‌کند که اجازه SYN/ACK را نمی‌دهد. حمله جعل[2] شامل استفاده از آدرس‌های IP جعلی است. مهاجم باید هدر IP و TCP معتبر را در بسته‌ها تزریق کند. وقتی نوبت به انتخاب آدرس می‌رسد، مهاجم باید بداند که دستگاهی که آدرس IP جعلی دارد به هیچ پیام SYN/ACK پاسخ نمی‌دهد. در حمله مستقیم توزیع‌شده[3] که متوقف نمودن آن بسیار دشوار است، مهاجم از پهپادهای موجود در اینترنت استفاده می‌کند که حملات مستقیم یا حملات جعلی را انجام می‌دهند. از آنجایی که ماشین‌های پهپاد دائماً اضافه یا حذف می‌شوند، جلوگیری از حمله مستقیم توزیع‌شده بسیار چالش‌برانگیز است.

برای تشخیص حملات SYN، طبق گفته وانگ و همکاران [۱۱]، دو راهبرد وجود دارد: راهبرد میزبان پایانی[4] و راهبرد مبتنی بر شبکه. رویکرد میزبان پایانی شامل اجرای سخت‌افزاری TCP برای جستجو و ایجاد اتصال است. رویکرد مبتنی بر شبکه شامل استفاده از سخت‌افزار شبکه به‌گونه‌ای است که سرورها از شبکه‌هایی که اتصالات TCP غیرقانونی ارائه می‌کنند، جدا می‌شوند. راهبردهای میزبان پایانی معمولا کم هزینه‌تر از راهبردهای مبتنی بر شبکه هستند [۷].

در هر دو راهبرد اغلب از روش‌های مبتنی بر هوش مصنوعی و زیرشاخه‌های آن مانند یادگیری ماشین و الگوریتم‌های ابتکاری و فراابتکاری برای تشخیص نفوذ استفاده می‌شود. هوش مصنوعی به‌عنوان یک حوزه علمی و فناوری، توانایی شبیه‌سازی فرایندهای شناختی انسان را در ماشین‌ها فراهم می‌کند و در سال‌های اخیر به طور خاص در زمینه‌های امنیت سایبری و تشخیص نفوذ در اینترنت اشیا موردتوجه قرار گرفته است. زیرشاخه‌های هوش مصنوعی، از جمله الگوریتم‌های یادگیری ماشین،

[1] Connect
[2] Spoofing attack
[3] Distributed direct attack
[4] End-Host

به سیستم‌ها این امکان را می‌دهند که از داده‌ها یاد بگیرند و الگوهای پیچیده حملات را شناسایی کنند. الگوریتم‌های یادگیری ماشین با تجزیه‌وتحلیل داده‌های ترافیک شبکه، می‌توانند حملات را به‌صورت خودکار شناسایی کنند و بهبود دهند. از سوی دیگر، الگوریتم‌های ابتکاری و فراابتکاری نیز در این زمینه کاربرد دارند؛ این الگوریتم‌ها با استفاده از روش‌های جستجوی هوشمند و بهینه‌سازی، به شناسایی الگوهای غیرمعمول و رفتارهای مشکوک در شبکه‌های IoT کمک می‌کنند. ترکیب این تکنیک‌ها می‌تواند به ایجاد سیستم‌های تشخیص نفوذ مؤثرتر و کارآمدتر منجر شود که قادر به مقابله با تهدیدات پیچیده دنیای دیجیتال هستند.

۲-۱- راهبرد میزبان پایانی

در یک حمله SYN، راهبرد میزبان پایانی به تکنیک‌هایی اشاره دارد که توسط سرور موردنظر برای دفاع در برابر چنین حملاتی استفاده می‌شود که ازجمله می‌توان به راهکارهای معرفی‌شده در [۷] [۱۲] [۱۳] اشاره کرد. اوزچلیک و همکاران [۱۲]، با استفاده از الگوی محاسباتی مه، معماری دفاعی اینترنت اشیا نرم‌افزاری تعریف‌شده لبه‌مرکز[1] (ECESID) را پیشنهاد می‌کنند. این تکنیک از یک پیاده‌روی تصادفی آستانه با الگوریتم محدودکننده نرخ مبتنی بر اعتبار[2] (TRW-CB) استفاده می‌کند. این الگوریتم سعی می‌کند با تکیه بر احتمال تلاش‌های موفقیت آمیز اتصال، مرحله اسکن حملات در میزبان را شناسایی کند. این سازوکار از یک صف SYN برای هر دستگاه اینترنت اشیا برای شناسایی فعالیت‌های مخرب استفاده می‌کند. اگرچه مرجع مذکور به طور مستقیم از الگوریتم‌های یادگیری ماشین یا هوش مصنوعی نام نمی‌برد، اما رویکرد آن را می‌توان نوعی روش ابتکاری در نظر گرفت که از مزایای SDN و محاسبات مه برای بهبود تشخیص و کاهش حملات در شبکه‌های اینترنت اشیا استفاده می‌کند. نویسندگان در [7]، رویکردی برای تشخیص و پیشگیری از حمله SYN برای داده‌های بزرگ در فضای ابری با توجه به قرارداد سطح سرویس پیشنهاد می‌کنند. الگوریتم پیشنهادی، پرچم SYN، تعداد Hop-Count و آدرس IP هر درخواست را در نظر می‌گیرد. همچنین برای هر اتصال یک سن تعریف می‌کند. اگر تمام ورودی‌های جدول درهم‌سازی پر شده باشد و درخواست جدیدی در سرور وجود داشته باشد، جدیدترین اتصال در جدول را حذف کرده و از پورت مرتبط آن مجددا استفاده می‌کنند. به این ترتیب سرور قادر خواهد بود بدون اینکه تحت فشار قرار گیرد، به هر کاربر پاسخ دهد. این الگوریتم نیاز به نظارت بر هر درخواست در داخل هر ماشین مجازی در حال اجرا بر روی ابر دارد.

باتوجه‌به محدودیت منابع ابزارهای اینترنت اشیا، در مرجع [13]، حملات انکار سرویس با بررسی وضعیت دستگاه‌ها در طول حمله SYN بررسی شده است. هدف نویسندگان، اندازه‌گیری مصرف انرژی در هنگام حمله است. آنها برای این کار، یک پلتفرم بستر آزمایشی آماده کردند و میزان استفاده از پردازنده یک دستگاه را در هنگام حمله SYN و حمله پروتکل پیام کنترل اینترنتی(ICMP)[3] بررسی کردند. آزمایشها در مورد نظارت بر بار پردازنده، در محیط ویندوز نشان داد که در هنگام شروع حمله SYN، بار پردازنده به طور قابل توجهی به حدود ۸۵٪ افزایش می‌یابد. SYN از پهنای باند یکسانی برای انتقال و دریافت داده استفاده می‌کند که حدود ۲۰۰ مگابیت بر ثانیه است. همچنین در حمله SYN مصرف انرژی بطور قابل توجهی در ابزار اینترنت اشیا افزایش می‌یابد و به این ترتیب نویسندگان توانستند با راهکار پیشنهادی حمله SYN را با توجه به مصرف انرژی در میزبان پایانی تشخیص دهند.

گالین و همکاران [14]، الگوریتم آنتروپی را برای تشخیص حمله توزیع شده انکار سرویس با استفاده از معماری شبکه نرم ابزارمحور پیشنهاد کردند. در روش پیشنهادی آنها، حمله‌ای که در سطح کاربردی رخ می‌دهد با استفاده از مقادیر آنتروپی شناسایی می‌شود. الگوریتم آنتروپی از نوع الگوریتم‌های یادگیری ماشین است که در دسته الگوریتم‌های درخت تصمیم قرار می‌گیرد. این الگوریتم به طور خاص در ساخت درخت‌های تصمیم‌گیری استفاده می‌شود و هدف آن کاهش عدم قطعیت در داده‌ها است. در این کار اندازه پنجره بسیار کوچک تعیین شد و دقت بالایی داشت. در روش آنها حمله TCP SYN و UDP با

[1] Edge-centric software-defined IoT defense

[2] Threshold random walk with a credit-based rate limiting

[3] Internet Control Message Protocol (ICMP)

نرخ مثبت کاذب ۲۰٪، نرخ تشخیص ۸۰٪ و میانگین زمان ۲۶/۹۸ میلی‌ثانیه در بدترین حالت برای اندازه پنجره ۳ تا ۲۰ شناسایی می‌شود. مشکل این کار این است که در صورت افزایش اندازه پنجره، دقت تشخیص کاهش می‌یابد.

در سال‌های اخیر، بسیاری از روش‌های دفاعی یادگیری ماشین برای رسیدگی به رشد همه‌گیر حملات توزیع‌شده انکار سرویس به اینترنت اشیا توسعه یافته‌اند و اکثر آنها از مشکلات تأخیر زمانی تشخیص رنج می‌برند؛ بنابراین، در [15]، رویکردی با تمرکز بر کاهش ابعاد و تکنیک‌های انتخاب ویژگی برای به حداقل رساندن تشخیص طولانی‌مدت بدون به خطر انداختن دقت ارائه شد. رویکرد پیشنهادی از تجزیه و تحلیل مؤلفه اصلی(PCA)[1]، تجزیه و تحلیل تمایز خطی(LDA)[2]، تحلیل عاملی و حذف ویژگی بازگشتی با اعتبارسنجی متقاطع (RFECV)[3] به عنوان تکنیک‌های کاهش ابعاد و انتخاب ویژگی و گاوسی نایو بیز(GNB)[4]، درخت تصمیم، جنگل تصادفی، AdaBoost و رگرسیون لجستیک به عنوان مدل‌های یادگیری ماشین برای طبقه بندی ترافیک مخرب استفاده می‌کند. این رویکرد یک مدل تشخیص حمله توزیع‌شده انکار سرویس قابل اعتماد ارائه می‌دهد که به طور موثر تاخیر زمانی تشخیص را با ترکیب GNB با LDA بهبود می‌دهد و دقت ۹۹.۹۸٪ را در ۰.۵۸۲ ثانیه زمان تشخیص به دست می‌آورد.

شبکه‌های SDN به دلیل معماری متمرکز خود در برابر حملات سیلابی TCP-SYN آسیب‌پذیر هستند. این حملات با تولید بسته‌های جعلی بیش از حد، کنترل‌کننده را تحت‌فشار قرار می‌دهند که منجر به کاهش عملکرد و افزایش مصرف انرژی می‌شود. راه‌حل‌های موجود معمولاً بر بهبود امنیت تمرکز دارند؛ اما تأثیرات انرژی را نادیده می‌گیرند. سینها و همکاران در [16] الگوهای مصرف انرژی کنترل‌کننده‌ها و سوئیچ‌های SDN را در حین حملات تحلیل می‌کنند. آنها SYN-Monitor را پیشنهاد می‌دهند که یک رویکرد انرژی کارآمد برای کاهش حملات سیلابی TCP-SYN با استفاده از پردازش انتخابی ترافیک سالم در سطح کنترل‌کننده است. SYN-Monitor با استفاده از یک تکنیک نگاشت آدرس، پورت‌های سوئیچ آسیب‌دیده را شناسایی کرده و از رویکرد SYN-proxy در این پورت‌ها استفاده می‌کند و بسته‌های جعلی SYN را بدون بارگذاری بر روی کنترل‌کننده فیلتر می‌کند، درحالی‌که ترافیک مجاز را نیز تشخیص می‌دهد. بسته‌های SYN مجاز از پورت‌های معتبر به طور عادی پردازش می‌شوند. رویکرد پیشنهادی مصرف انرژی کنترل‌کننده را ۲۰ تا ۵۰ درصد و مصرف انرژی سوئیچ‌های OpenFlow را ۶۰ تا ۷۰ درصد در مقایسه با SDN بدون راه‌حل امنیتی تحت حمله کاهش می‌دهد. علاوه بر این، SYN-Monitor به طور قابل‌توجهی نرخ مثبت کاذب را کاهش داده و زمان پاسخگویی برای ترافیک مشروع را نسبت به راه‌حل‌های موجود بهبود می‌بخشد. نویسندگان SYN-Monitor را در کنترل‌کننده Floodlight پیاده‌سازی کرده و اثربخشی روش پیشنهادی خود را در زمینه‌های امنیت و کارایی انرژی نشان داده‌اند.

۲-۲- راهبرد مبتنی بر شبکه

راهبردهای مبتنی بر شبکه برای کاهش حملات SYN بر حفاظت از زیرساخت شبکه و اطمینان از دردسترس بودن خدمات از داده‌های شبکه برای تشخیص حمله کمک می‌گیرند. تحقیق‌هایی همچون [2]، [6] و [17] بر این اساس حملات SYN را تشخیص می‌دهند.

در مرجع [17] یک سیستم مبتنی بر سیستم ایمنی مصنوعی برای تشخیص بلادرنگ حملات SYN به نام AISD[5] معرفی شده است. این سیستم از الگوریتم سلول دندریک[6] برای شناسایی و پاسخ به حملات SYN استفاده می‌کند. سیستم AISD ترافیک شبکه را رصد می‌کند، الگوهای سیل SYN را شناسایی می‌کند و به مهاجم پاسخ می‌دهد و یک مکانیسم دفاعی موثر در برابر حملات SYN فراهم می‌کند. الگوریتم سلول دندریک به طور مداوم ترافیک شبکه را نظارت می‌کند و نسبت تعداد بسته‌های SYN به تعداد بسته‌های SYN-ACK را محاسبه می‌کند. نسبت بالاتر از آستانه به این معنی است که بسیاری از بسته‌های SYN

---

[1] Principal Component Analysis

[2] Linear Discriminant Analysis

[3] Recursive Feature Elimination with Cross Validation

[4] Gaussian Naı̈ve Bayes

[5] Artificial Immune System for SYN Flood Detection

[6] Dendric Cell Algorithm

بدون پاسخگویی به بسته‌های SYN-ACK دریافت می‌شوند. این رفتار نمونه ای از حملات SYN است و برای شناسایی چنین حملاتی استفاده می‌شود. الگوریتم پیشنهادی در زبان پایتون پیاده سازی شده است.

برون و همکاران در [2] حملات شبکه‌ای را که می‌توان علیه دروازه‌های اینترنت اشیا راه‌اندازی کرد، در مورد تهدیدات امنیت سایبری علیه یک محیط خانه متصل به اینترنت اشیا تحلیل می‌کنند، معیارهای مربوطه را برای شناسایی آن‌ها تعیین می‌کنند و توضیح می‌دهند که چگونه می‌توان آنها را از روی بسته‌ها محاسبه کرد. در یک محیط خانه متصل به اینترنت اشیا، ممکن است ده‌ها یا حتی صدها حسگر با عملکردهای مختلف (به عنوان مثال، اندازه گیری دما، نور، نویز و غیره) علاوه بر محرک‌هایی برای کنترل سیستم‌هایی مانند سیستم گرمایش، تهویه و تهویه مطبوع وجود داشته باشد. هر کدام از این دستگاه‌ها ممکن است از پروتکل‌های مختلف برای اتصال استفاده کنند (وای‌فای، بلوتوث، اترنت، زیگ‌بی[1] و غیره) و اکثر آنها قادر به اتصال مستقیم به اینترنت نیستند. نویسندگان همچنین اصول و طراحی یک رویکرد مبتنی بر یادگیری عمیق را برای تشخیص آنلاین حملات شبکه ارائه می‌دهند. بسته‌های داده مبادله شده با دروازه اینترنت اشیا در تمام رابط‌های شبکه ضبط می‌شوند. سپس این بسته‌ها به منظور استخراج معیارهای مختلف در سطح بسته مورد تجزیه و تحلیل قرار می‌گیرند که از آن‌ها می‌توان حملات شبکه را شناسایی کرد. یک الگوریتم کلاس بندی که قبلاً با ترافیک اینترنت اشیاء «عادی» آموزش داده شده است، این معیارها را به عنوان ورودی می‌گیرد و احتمال اینکه محیط خانه متصل به اینترنت اشیا در حال حاضر مورد حمله قرار گرفته است را پیش‌بینی می‌کند. نتایج اعتبارسنجی تجربی در مورد بسته‌هایی که حملات در آن درج شده‌اند نشان می‌دهد که شبکه عصبی عمیق حملات را به درستی تشخیص می‌دهد، راه حل پیشنهادی قادر است حملات SYN را از تفاوت بین تعداد ارتباطات آغاز شده و ایجاد شده TCP در اسلات‌های زمانی تشخیص دهد.

دایین در [18]، چارچوب SD-IoT را برای تشخیص و کاهش حمله‌ها پیشنهاد کرد که جریان عادی و جریان حمله را با استفاده از مقادیر برداری بسته‌ها مقایسه می‌کند. لبه SW_set پارامترهای شماره نمونه‌ها، طول بردار، فاصله زمانی، بسته در pkin و pkout را در نظر می‌گیرد. برای دستیابی به‌دقت بالا، چند پارامتر بیشتر برای دفاع پیشگیرانه در برابر حملات توزیع‌شده انکار سرویس به طور مؤثرتر موردنیاز است. الگوریتم پیشنهادی از شباهت کسینوس بردارهای نرخ پیام بسته در پورت‌های سوئیچ مرزی SD-IoT برای شناسایی حملات توزیع‌شده انکار سرویس استفاده می‌کند. اما شباهت کسینوس، به‌خصوص در هنگام برخورد با حملات جدید یا پیچیده، ممکن است به‌اندازه کافی قوی نباشد که بتواند الگوهای حمله متنوع را مدیریت کند.

دیر و همکاران [19]، آموزش محلی و تبادل پارامتر(LTPE)[2] را برای تشخیص حمله توزیع شده انکار سرویس پیشنهاد کردند. نویسندگان، حملات سیل UDP، SYN TCP و ICMP با استفاده از مجموعه داده نفوذی NSL-KDD شناسایی می‌شوند. این طرح توابع امنیتی (مانند رمزنگاری) را به گره‌های مه بارگذاری می‌کند و بار محاسباتی و ذخیره‌سازی دستگاه‌های اینترنت اشیا را کاهش می‌دهد. این رویکرد استفاده از منابع را بهینه می‌کند و مقیاس پذیری را افزایش می‌دهد.استفاده از توابع رمزنگاری سبک وزن (به عنوان مثال، رمزنگاری منحنی بیضوی) آن را برای دستگاه‌های اینترنت اشیا تعبیه شده با محدودیت منابع مناسب می‌کند. توزیع ترافیک با جریان عادی و جریان حمله با ۶۷۳۴۳ مجموعه آموزشی و ۹۷۱۱ مجموعه داده تست مقایسه شده است. پارامترهای مثبت کاذب، منفی کادب و دقت الگوریتم LTPE ارزیابی شده است، و به دقت ۹۹.۱۴٪ (دقت)، فراخوانی ۹۹.۱۵٪ برای شبکه اینترنت اشیا کوچک رسیده است. این مقاله از یک الگوریتم رمزنگاری سبک استفاده می‌کند که می‌توان آن را در دسته الگوریتم‌های ابتکاری قرار داد. با این حال، برخی از معایب وجود دارد. تمرکز این طرح بر طراحی سبک وزن ممکن است برخی از ویژگی‌های امنیتی را در مقایسه با روش‌های رمزگذاری قوی تر قربانی کند. ارزیابی اینکه آیا معاوضه بین امنیت و کارایی منابع با موارد استفاده خاص مطابقت دارد یا خیر، ضروری است. پیاده سازی مکانیزم‌های امنیتی توزیع شده در گره‌های مه مستلزم طراحی و هماهنگی دقیق است. اطمینان از سیاست‌های امنیتی و مدیریت کلید می‌تواند چالش برانگیز باشد.

[1] ZigBee

[2] local training and parameter exchange

دانگ و همکاران [20]، یک پارادایم مبتنی بر پروکسی SYN در SDN بنام SSP[1] برای کاهش تهدیدات سیل SYN طراحی کردند. نویسندگان نشان دادند که SSP یک راه حل مبتنی بر شبکه برای محافظت از سرورهای برنامه از نظر کاهش تعداد اتصالات نیمه باز در سرور برنامه و افزایش احتمال ایجاد موفقیت آمیز برای اتصال جریان TCP تحت حمله SYN است. ارزیابی نتایج SSP برروی مجموعه داده CAIDA 2013 نشان می‌دهد که این روش می‌تواند زمان اشغال منبع سوئیچ را تا ۹۴ درصد در مقایسه با راه حل Avant-Guard کاهش دهد. علاوه بر این، SSP نرخ اتصال موفق و میانگین زمان بازیابی اتصال را در مقایسه با راه حل استاندارد Openflow بهبود می‌بخشد.

پاتیل و همکاران [6]، یک سیستم طبقه‌بندی مبتنی بر جریان به نام SSK-DDoS را برای طبقه‌بندی انواع حملات توزیع‌شده انکار سرویس بلادرنگ پیشنهاد کردند. این سیستم برای طبقه بندی شش نوع حمله DDoS-DNS، DDoS-LDAP، DDoS-MSSQL، DDoS-NetBIOS، DDoS-UDP، و DDoS-SYN و ترافیک عادی موجود در مجموعه داده CICDDoS2019 آموزش و آزمایش شد. الگوریتم توسعه یافته ویژگی‌های فرموله شده را با کلاس‌های ارزیابی شده آنها در HDFS ذخیره می‌کند و می‌تواند در طول آموزش مجدد مورد استفاده مجدد قرار گیرد. در نتیجه آزمایش‌ها، نشان داده شد که سیستم تشخیص پیشنهادی، ترافیک شبکه را با نرخ دقت ۸۹.۰۵٪ به هفت کلاس تقسیم می‌کند. این روش از پیچیدگی اجرایی O (NNF/n) برخوردار است.

در[21] ، یک سیستم تشخیص نفوذ برای پیشگیری از هرگونه اختلال در شبکه اینترنت اشیای پرشکی پیشنهاد می‌شود. سیستم تشخیص نفوذ با نظارت بر ترافیک شبکه به عنوان اولین خط دفاعی برای امنیت در نظر گرفته می‌شود. تمامی فعالیت‌های شبکه مورد تجزیه و تحلیل قرار می‌گیرد و هرگونه ترافیک غیرعادی یا فعالیت مخرب توسط سیستم تشخیص نفوذ هشدار داده می‌شود و باید اقدامات لازم انجام شود. هدف اصلی طرح پیشنهادی شناسایی حملات SYN است. در واقع، در این مقاله، یک سیستم تشخیص نفوذ برای شناسایی حمله SYN در شبکه‌های اینترنت اشیا پیشنهاد شده است. برای این منظور، یک الگوریتم جدید برای سیستم تشخیص نفوذ و برای شناسایی فعالیت‌های مخرب در اینترنت اشیای پزشکی پیشنهاد می‌کنند. طرح پیشنهادی برای اطمینان از امنیت داده‌ها و حفظ محرمانه بودن داده‌های جمع آوری شده، تا حد امکان تعداد حملات را به حداقل می‌رساند. به منظور بررسی دوام رویکرد پیشنهادی، نویسندگان به صورت تحلیلی و از طریق شبیه‌سازی عملکرد راه حل پیشنهادی خود را تحت احتمال حملات مختلف ارزیابی می‌کنند. سیستم تشخیص نفوذ پیشنهادی الگوریتمی را برای محاسبه احتمال حمله در هر فاصله زمانی پیاده‌سازی می‌کند. این احتمال با یک مقدار آستانه مقایسه می‌شود و بسته به نتیجه مقایسه، یک آلارم یا سیگنال مناسب مدیریتی ارسال می‌شود. با اینکه رویکرد پیشنهادی شناسایی هدفمند حملات TCP SYN در IoMT را فراهم می‌کند، اما محدودیت‌های آن شامل محدودیت‌های منابع و چالش‌های بالقوه مقیاس‌پذیری است. پیچیدگی اجرایی این الگوریتم O(n) است.

جدول ۱: مقایسه تحقیق‌های انجام شده در رابطه با تشخیص و پیشگیری از حملات SYN

Table 1: Comparison of research conducted on the detection and prevention of SYN attacks

مجموعه‌داده	ابزار ارزیابی	ویژگی	راه‌حل	نوع الگوریتم	راهبرد	سال	منبع
-	پیاده‌سازی در شبکه واقعی	چالش مقیاس‌پذیری و محدودیت منابع	پیاده‌روی تصادفی آستانه با الگوریتم محدودکننده نرخ مبتنی بر اعتبار	ابتکاری	میزبان پایانی	۲۰۱۷	[12]
-	CloudSim	نیازمند نظارت بر درخواست‌ها در هر ماشین مجازی	تشخیص حمله بر اساس قرارداد سطح سرویس	ابتکاری	میزبان پایانی	۲۰۱۸	[7]
-	پیاده‌سازی در شبکه واقعی	افزایش قابل‌توجه مصرف انرژی در ابزار اینترنت اشیا در حمله SYN	شناسایی حمله SYN با نظارت بر بار CPU	ابتکاری	میزبان پایانی	۲۰۱۹	[13]

[1] SDN SYN Proxy

-	پیاده‌سازی در شبکه واقعی	بهبود تشخیص کاهش دقت با افزایش اندازه پنجره	شناسایی حمله با مقادیر آنتروپی	یادگیری ماشین	میزبان پایانی	۲۰۲۰	[14]
CICIDS2017	-	بهبود دقت و کاهش تأخیر	مدل‌های یادگیری ماشین برای طبقه‌بندی ترافیک	یادگیری ماشین	میزبان پایانی	۲۰۲۴	[15]
-	پیاده‌سازی روی کنترل‌کننده‌های floodlightبا Mininet	کاهش مصرف انرژی، کاهش زمان پاسخ، تشخیص حملات	نگاشت آدرس، پروکسی	ابتکاری	میزبان پایانی	۲۰۲۵	[16]
-	-	تشخیص بر اساس نسبت درخواست‌ها و پاسخ‌ها	الگوریتم سلول دندریک	فراابتکاری	مبتنی بر شبکه	۲۰۱۶	[17]
-	پیاده سازی و پایتون	وابستگی به مجموعه آموزشی	رویکرد مبتنی بر یادگیری عمیق را برای تشخیص آنلاین حملات	یادگیری عمیق	مبتنی بر شبکه	۲۰۱۸	[2]
-	پیاده‌سازی با Mininet و پایتون	وابستگی به شباهت کسینوس	شباهت کسینوس بردارهای نرخ پیام	ترکیبی	مبتنی بر شبکه	۲۰۱۸	[18]
-	-	سبک‌وزن بودن نیازمند هماهنگی دقیق	آموزش محلی و تبادل پارامتر	ابتکاری	مبتنی بر شبکه	۲۰۱۸	[19]
CAIDA 2013	BONESI-Wireshark	کاهش زمان اشغال منبع بهبود نرخ اتصال موفق	پارادایم مبتنی بر پروکسی SYN	ابتکاری	مبتنی بر شبکه	۲۰۱۹	[20]
CICDDoS2019	Apache Spark-Apache Kafka-Hadoop	تشخیص شش نوع حمله	سیستم طبقه‌بندی مبتنی بر جریان به نام SSK-DDoS	یادگیری ماشین	مبتنی بر شبکه	۲۰۲۲	[6]
-	Matlab	تضمین امنیت داده‌ها و حفظ محرمانگی داده‌ها	شناسایی هدفمند حملات TCP SYN در IoMT	یادگیری ماشین	مبتنی بر شبکه	۲۰۲۲	[21]
KDD Cup 1999	WEKA 3.8و پایتون	کاهش ویژگی‌ها چالش مقیاس‌پذیری و محدودیت منابع	سیستم تشخیص نفوذ هوشمند را برای شناسایی مؤثر بازتاب و حملات DDoS مبتنی بر بهره‌برداری	یادگیری ماشین	مبتنی بر شبکه	۲۰۲۲	[22]
UNSW-NB15 و NSL-KDD BoT-IoT	ذکر نشده	کاهش وابستگی به داده‌ها مدل منعطف	سیستم تشخیص نفوذ قوی مبتنی بر GAN با استفاده داده‌های مصنوعی	یادگیری عمیق	مبتنی بر شبکه	۲۰۲۴	[23]
KDDCup99	-	کاهش ویژگی‌ها افزایش دقت تشخیص حملات، کاهش نرخ هشدار کاذب	تشخیص حملات در اینترنت اشیا مبتنی بر نرم‌افزار با الگوریتم جایا	فراابتکاری	مبتنی بر شبکه	۲۰۲۵	[24]

کشیرساگر و همکاران [22]، یک رویکرد کاهش ویژگی را برای کاهش هزینه محاسباتی و درعین‌حال شناسایی حملات توزیع‌شده انکار سرویس مبتنی بر بازتاب و بهره‌برداری پیشنهاد کرده‌اند. این روش تکنیک‌های انتخاب ویژگی به‌دست‌آوردن اطلاعات و همبستگی را برای کاهش تعداد ویژگی‌ها ترکیب می‌کند. نویسندگان از مدل طبقه‌بندی‌کننده J48 برای طبقه‌بندی ترافیک

مخرب از ترافیک عادی با استفاده از ترکیب سود اطلاعات و همبستگی استفاده کرده‌اند. آنها رویکرد پیشنهادی را در مجموعه‌داده‌های CICDDoS2019 و KDDCUP1999 تأیید کرده‌اند. رویکرد پیشنهادی به سه مرحله تقسیم می‌شود که عبارت‌اند از: پیش‌پردازش داده، کاهش ویژگی و طبقه‌بندی با استفاده از ابزار WEKA 3.8 آنها از فایل‌های حمله Portmap، SYN، NetBIOS، MSSQL و LDAP از مجموعه‌داده CICDDoS2019 استفاده کرده‌اند. این روش کاهش ۵۶٪ به ۸۲.۹۲٪ در ویژگی‌های اصلی را به دست می‌آورد که از مجموعه ویژگی‌های کامل، بهتر عمل می‌کند. بااین‌حال، محدودیت‌ها شامل عدم رسیدگی صریح به محدودیت‌های منابع و چالش‌های مقیاس‌پذیری را دارد.

رحمان و همکاران [23]، با توجه به اینکه مسئله عدم تعادل داده و هزینه‌های مرتبط با جمع‌آوری داده و اختلال در توانایی مدل‌های یادگیری ماشین را برای یادگیری رفتارهای مخرب، راه حلی بنام SYN-GAN را پیشنهاد کردند. روش آنها پتانسیل استفاده از داده‌های ۱۰۰ درصد مصنوعی تولید شده از طریق شبکه‌های مولد رقابتی (GAN)[1] را برای آموزش مدل‌های یادگیری ماشین در سیستم‌های تشخیص نفوذ شبکه را بررسی می‌کند. GAN یک مدل یادگیری عمیق است. این شبکه‌ها به طور خاص از دو شبکه عصبی تشکیل شده‌اند: یک مولد که نمونه‌های جدید تولید می‌کند و یک تفکیک‌کننده که تلاش می‌کند بین نمونه‌های واقعی و جعلی تمایز قائل شود. GANها به عنوان روشی برای مدلسازی مولد با استفاده از یادگیری عمیق شناخته می‌شوند و معمولاً از شبکه‌های عصبی پیچشی برای بهبود کیفیت تولید داده‌ها استفاده می‌کنند. این الگوریتم‌ها در زمینه‌های مختلفی مانند تولید تصاویر، ویدئوها و حتی موسیقی کاربرد دارند و به دلیل قابلیت‌های خود در یادگیری الگوهای پیچیده، به سرعت در حال پیشرفت هستند. رویکرد پیشنهادی رحمان و همکاران، وابستگی به داده‌های واقعی را به طور قابل توجهی کاهش می‌دهد و راه را برای یک فرآیند ساخت مدل منعطف‌تر و از نظر اخلاقی مناسب‌تر هموار می‌کند. مطالعه به طور موفقیت‌آمیزی داده‌های واقعی تشخیص نفوذ شبکه را تکرار کرده و فرصت‌های جدیدی برای استفاده از داده‌های تولیدی در امنیت سایبری نشان می‌دهد. پیچیدگی اجرایی و زمان اجرای الگوریتم‌ها به‌طور خاص ذکر نشده است. با این حال، معمولاً **GAN** به دلیل نیاز به تعویضات بسیاری و تعادل بین گریدیانتور و ژنراتور، پیچیدگی اجرایی بالایی دارند و ممکن است زمان اجرای آن برابر با چندین دقیقه یا حتی ساعت‌ها باشد، بسته به توانایی محاسباتی و مقدار داده‌های مورد استفاد باشد.

در جدیدترین تحقیقات جاهون و آتولکار [24] ، یک رویکرد کارآمد برای تشخیص حملات در اینترنت اشیا مبتنی بر نرم‌افزار ارائه کردند که از تکنیک انتخاب ویژگی بهینه‌سازی شده با الگوریتم جایا[2] استفاده می‌کند. اجزای اصلی این روش شامل استفاده از الگوریتم فراابتکاری بهینه‌سازی جایا برای انتخاب ویژگی‌های مهم و کاهش ابعاد داده‌ها، به‌کارگیری تکنیک انتخاب ویژگی برای بهبود دقت تشخیص و کاهش پیچیدگی محاسباتی، ترکیب الگوریتم جایا با یک طبقه‌بندی‌کننده ماشین یادگیری برای تشخیص حملات و بهینه‌سازی پارامترهای طبقه‌بندی‌کننده با استفاده از الگوریتم جایا برای بهبود عملکرد کلی سیستم است. این رویکرد باهدف افزایش دقت تشخیص حملات، کاهش نرخ هشدار اشتباه و بهبود کارایی محاسباتی در محیط‌های اینترنت اشیا مبتنی بر نرم‌افزار طراحی شده است.

در جدول ۱، تحقیق‌های اخیر در رابطه با تشخیص و پیشگیری از حملات SYN در حوزه اینترنت اشیا را خلاصه کرده‌ایم.

معمولاً برای ارزیابی نتایج تشخیص نفوذ معیارهای دقت، صحت، امتیاز F1، مورد ارزیابی قرار می‌گیرد. معیار دقت، نسبت موارد نفوذ درست تشخیص‌داده‌شده به کل مواردی که سیستم به‌عنوان نفوذ شناسایی کرده است. این معیار نشان می‌دهد چقدر از هشدارهای سیستم واقعاً نفوذ بوده‌اند. معیار صحت، نسبت موارد نفوذ درست تشخیص‌داده‌شده به کل موارد نفوذ واقعی است. این معیار نشان می‌دهد سیستم چه درصدی از نفوذهای واقعی را شناسایی کرده است. امتیاز F1، میانگین هارمونیک دقت و صحت است که تعادلی بین این دو معیار ایجاد می‌کند. این معیار برای ارزیابی عملکرد کلی سیستم تشخیص نفوذ مفید است، زیرا هم مثبت‌های کاذب (هشدارهای اشتباه) و هم منفی‌های کاذب (نفوذهای تشخیص داده نشده) را در نظر می‌گیرد. جدول ۲ نتایج ارزیابی روشهای مختلفی را که بر اساس این معیارها روش پیشنهادی شان را ارزیابی کردند، نشان می دهد.

[1] Generative Adversarial Networks

[2] Jaya algorithm

جدول ۲: مقایسه معیارها در روش‌های مختلف
Table 2: Comparison of criteria in different methods

منبع	مجموعه‌داده	دقت	صحت	امتیاز F1
[15]	CICIDS2017	۹۹/۸۲	۹۹/۸۰	۹۹/۸۲
[19]	-	۹۱/۱۴	۹۹/۱۵	-
[6]	CICDDoS2019	۸۹/۵۰	۸۹	-
[22]	KDD Cup 1999	۹۹/۸۸	۹۹/۸۸	-
[23]	UNSW-NB15	۹۰	۹۱	۸۹
	NSL-KDD	۸۴	۸۵	۸۴
	BoT-IoT	۱۰۰	۱۰۰	۱۰۰
[24]	KDD Cup 1999	۹۹/۹۷	۹۹/۳۹	-

۳- چالش‌های پیش رو

درحالی‌که سیستم‌های امنیتی مصنوعی در تشخیص حملات SYN امیدوارکننده هستند، اما هنوز چالش‌ها، محدودیت‌ها و ضعف‌هایی وجود دارد که نیازمند توجه بیشتر در تحقیق‌های آینده دارد. درارتباط‌با راهبردهای مبتنی بر میزبان پایانی چالش‌های محدودیت منابع، مقیاس‌پذیری، ناهمگونی، توپولوژی شبکه پویا، حفظ حریم خصوصی، حملات خصمانه و بهره‌وری انرژی مطرح است.

دستگاه‌های اینترنت اشیا معمولاً منابع محاسباتی و ظرفیت ذخیره‌سازی محدودی دارند. باتوجه‌به این محدودیت‌ها، سیستم ممکن است برای پردازش و تجزیه‌وتحلیل کارآمد مقدار زیادی از داده‌های ترافیک شبکه مشکل داشته باشد که منجر به تأخیر یا ناتوانی در برآوردن الزامات بلادرنگ در شناسایی می‌شود.

با افزایش تعداد دستگاه‌های اینترنت اشیا، مقیاس‌پذیری بسیار مهم می‌شود. سیستم‌های تشخیص نفوذ میزبان پایانی باید یک شبکه بزرگ و پویا با الگوهای ترافیکی متفاوت را کنترل کنند و درعین‌حال دقت و مثبت کاذب پایین را حفظ کنند.

محیط‌های اینترنت اشیا از دستگاه‌های متنوع با سیستم‌عامل‌ها، پروتکل‌های ارتباطی و مکانیسم‌های امنیتی متفاوت تشکیل شده است. توسعه سیستم تشخیص نفوذ میزبان نهایی که بتواند با این ناهمگونی سازگار شود، چالش‌برانگیز است.

شبکه‌های اینترنت اشیا به دلیل تحرک دستگاه، اتصال متناوب و تغییرات توپولوژی مکرر بسیار پویا هستند. اطمینان از تشخیص مؤثر در چنین توپولوژی‌های پویا پیچیده است.

ایجاد تعادل بین اثربخشی تشخیص نفوذ با حفظ حریم خصوصی بسیار مهم است. روش‌های میزبان پایانی نیاز به شناسایی حملات بدون به خطر انداختن حریم خصوصی کاربر یا افشای اطلاعات حساس دارند.

مهاجمان می‌توانند به طور خاص دستگاه‌های اینترنت اشیا را هدف قرار دهند و از آسیب‌پذیری‌های آنها سوءاستفاده کنند. سیستم تشخیص نفوذ میزبان نهایی باید در برابر حملات متخاصم و تکنیک‌های فرار مقاوم باشد.

بسیاری از دستگاه‌های اینترنت اشیا با باتری کار می‌کنند. طراحی سیستم‌های تشخیص نفوذ کارآمد که مصرف منابع را به حداقل می‌رساند و درعین‌حال امنیت را حفظ می‌کند یک چالش است.

به طور خلاصه، پرداختن به این چالش‌ها برای توسعه سیستم‌های تشخیص نفوذ قوی و مؤثر برای اینترنت اشیا با استفاده از روش‌های میزبان پایانی ضروری است.

درارتباط‌با طراحی روش‌های تشخیص نفوذ مبتنی بر شبکه نیز چالش‌هایی وجود دارد. تشخیص‌های مثبت و منفی کاذب یکی از چالش‌های مهم در این زمینه است. سیستم‌های امنیتی مصنوعی ممکن است مثبت کاذب (پرچم‌گذاری نادرست ترافیک قانونی به‌عنوان حمله) یا منفی کاذب (ناتوانی در شناسایی حملات واقعی) تولید کنند. اثربخشی سیستم به کیفیت الگوریتم‌های استخراج و طبقه‌بندی ویژگی بستگی دارد. تنظیم سیستم برای به‌حداقل‌رساندن مثبت‌های کاذب می‌تواند منجر به افزایش منفی‌های کاذب شود و بالعکس.

سازگاری و میزان یادگیری در راهبردهای مبتنی بر شبکه باید با تغییر الگوهای حمله سازگار شوند. بااین‌حال، نرخ یادگیری آنها ممکن است همیشه با تکامل سریع تکنیک‌های حمله مطابقت نداشته باشد. اگر داده‌های آموزشی سیستم قدیمی شود، ممکن است انواع حملات جدید را شناسایی نکند.

سربار منابع موضوع مهم دیگری است که نیازمند توجه محققان است. راهبردهای مبتنی بر شبکه به منابع محاسباتی برای نظارت و تجزیه‌وتحلیل ترافیک شبکه نیاز دارد. سربار می‌تواند بر عملکرد سیستم تأثیر بگذارد و این موضوع به‌ویژه در دوره‌های پر ترافیک مهم‌تر می‌شود. ممکن است در شناسایی بلادرنگ، منابع فشرده باشد و بر پاسخگویی کلی شبکه تأثیر بگذارد.

درک محدود از قصد حمله چالش دیگری است. راهبردهای مبتنی بر شبکه روی تشخیص الگو متمرکز است؛ اما درک عمیقی از قصد حمله ندارد. ممکن است بر اساس زمینه، بین ترافیک مخرب و بدخیم تفاوت قائل نشود. مهاجمان پیشرفته می‌توانند با تغییر نامحسوس الگوهای حمله از شناسایی فرار کنند.

مقیاس‌پذیری سیستم‌های مبتنی بر راهبردهای مبتنی بر شبکه یک نگرانی است. با افزایش ترافیک شبکه، حفظ مدل‌های دقیق چالش‌برانگیز می‌شود. استقرار راهبردهای مبتنی بر شبکه در شبکه‌های بزرگ به طراحی و بهینه‌سازی دقیق نیاز دارد.

مدل‌های مبتنی بر شبکه ممکن است برای تعمیم در محیط‌های مختلف شبکه مشکل داشته باشند. آموزش در یک شبکه ممکن است به طور مؤثر به شبکه دیگر منتقل نشود. سفارشی‌سازی و تنظیم دقیق برای عملکرد بهینه در زمینه‌های خاص ضروری است.

به طور خلاصه، درحالی‌که راهبردهای مبتنی بر شبکه می‌تواند تشخیص SYN را افزایش دهد، رسیدگی به این نقاط ضعف برای استقرار عملی بسیار مهم است. محققان به بررسی راه‌هایی برای بهبود سیستم‌های مبتنی بر شبکه و کاهش محدودیت‌های آن‌ها ادامه می‌دهند.

اخیراً راه‌حل‌هایی بر اساس یادگیری عمیق برای تشخیص حملات در اینترنت اشیا پیشنهاد شده‌اند. در این باره نیز محدودیت‌های وجود دارد که نیازمند توجه محققان است. دستگاه‌های اینترنت اشیا اغلب منابع محاسباتی محدودی دارند (حافظه، قدرت پردازش). پیاده‌سازی مدل‌های پیچیده یادگیری عمیق در چنین دستگاه‌هایی به دلیل محدودیت‌های حافظه می‌تواند چالش‌برانگیز باشد. تکنیک‌های یادگیری عمیق معمولاً به فعالیت اینترنتی قابل‌توجهی نیاز دارند که ممکن است برای دستگاه‌های اینترنت اشیا محدود به منابع امکان‌پذیر نباشد.

مدل‌های یادگیری عمیق شدیداً وابسته به مجموعه داده‌ای هستند که با آن آموزش‌دیده‌اند. مجموعه‌داده‌های برچسب‌گذاری شده چندانی که بتواند به طور بلادرنگ حملات امنیتی اینترنت اشیا، را تشخیص دهد، وجود ندارد. بدون داده‌های کافی، آموزش مدل‌های یادگیری عمیق قوی دشوار می‌شود.

۴- جمع‌بندی و نتیجه‌گیری

حمله SYN یکی از انواع حملات توزیع‌شده انکار سرویس به سرورها است که در سال‌های اخیر رواج یافته است. در این نوع حمله، مهاجمان با ارسال بسته‌های SYN به سرور، تلاش می‌کنند تا اتصال‌های نیمه‌باز را ایجاد کنند و منابع سرور را به طور غیرمجاز مشغول کنند. برای مقابله با حمله SYN ، می‌توان از استراتژی‌های مبتنی میزبان پایانی و استراتژی‌های مبتنی بر شبکه استفاده کرد. معمولاً برای این منظور در مقالات مختلف از روش‌های تشخیص و مسدودسازی، محدودیت نرخ درخواست SYN و سیستم‌های تشخیص نفوذ استفاده می‌شود.

به طور خلاصه، حمله SYN باعث اشغال منابع سرور می‌شود و برای مقابله با آن، استفاده از راهکارهای امنیتی و تشخیصی ضروری است. باوجود تحقیق‌های فراوان انجام شده در این زمینه هنوز چالش‌هایی وجود دارد که نیازمند توجه محققان است. از جمله محدودیت منابع، مقیاس‌پذیری، ناهمگونی، توپولوژی شبکه پویا، حفظ حریم خصوصی، حملات خصمانه و بهره‌وری انرژی را می‌توان نام برد.

برای تشخیص حملات در شبکه اینترنت اشیا، سیستم‌های امنیتی مصنوعی ارائه شده‌اند که از راهکارها و الگوریتم‌های مختلفی برای تشخیص حمله یا نفوذ بهره می‌برند. هر یک از روش‌های الگوریتمی دارای ویژگی‌ها و مزایای خاص خود هستند.

الگوریتم‌های یادگیری ماشین به‌ویژه آن‌هایی که از تکنیک‌های خاصی مانند کاهش داده و نمونه‌برداری استفاده می‌کنند، معمولاً برای مجموعه‌داده‌های نامتوازن مناسب‌تر هستند. این تکنیک‌ها می‌توانند به تعادل بین کلاس‌ها کمک کنند و دقت تشخیص را افزایش دهند.

الگوریتم‌های یادگیری عمیق معمولاً نیاز به حجم بالایی از داده دارند، اما برخی از مدل‌های یادگیری ماشین، مانند درخت تصمیم یا ماشین بردار پشتیبان، می‌توانند با داده‌های کمتر نیز عملکرد خوبی داشته باشند. این الگوریتم‌ها می‌توانند از ویژگی‌های موجود به‌خوبی استفاده کنند و نتایج قابل‌قبولی ارائه دهند.

الگوریتم‌های ابتکاری و فراابتکاری معمولاً در کاهش نرخ مثبت کاذب و منفی کاذب مؤثرتر هستند. این روش‌ها با استفاده از جستجوی هوشمند و بهینه‌سازی می‌توانند به تشخیص دقیق‌تر تهدیدات کمک کنند و در نتیجه، نرخ هشدارهای اشتباه را کاهش دهند.

در نهایت، انتخاب بهترین روش بستگی به شرایط خاص محیط، نوع حملات و ویژگی‌های داده‌ها دارد.

برای تحقیق‌های آینده پیشنهاد می‌شود با تمرکز بر چالش‌های ذکر شده، با کمک مدل‌های مبتنی بر هوش مصنوعی، راه‌حل‌های مقیاس‌پذیر و بادقت بالا برای تشخیص حملات ارائه نمود. تا کنون تلاش‌های زیادی برای ارائه مدل‌های هوش مصنوعی برای تشخیص و پیشگیری از حملات انجام شده است؛ اما باتوجه‌به پیشرفت روزافزون انواع حملات و بدافزارها لازم است راه‌حل‌های پیشنهادی نیز به طور بروز رسانی شوند.

- **مجموعه‌داده‌های متوازن:** برای آموزش مدل‌های تشخیص و پیشگیری نیازمند مجموعه‌داده متوازن هستیم. با بررسی تحقیق‌های اخیر، مشاهده شده است که مجموعه‌داده‌های متعادل دارای الگوهای ترافیک اینترنت اشیا محدود است. در نتیجه، تکنیک‌های تشخیص سوگیری را نشان می‌دهند و خطاهای مثبت و منفی کاذب در آنها مشاهده می‌شود. ارائه مجموعه‌داده‌های واقعی اینترنت اشیا قوی‌تر می‌توانند از ترکیب مناسبی از ترافیک خوش‌خیم و ترافیک مخرب ایجاد شوند.
- **یکپارچه‌سازی اطلاعات حمله به طور بلادرنگ:** ادغام بلادرنگ اطلاعات تهدیدها در سیستم‌های تشخیص حمله این امکان را می‌دهد تا از آخرین امضاها و روندهای حمله مطلع بمانید و سیستم بتواند جدیدترین نوع حملات را تشخیص دهد. این رویکرد پویا می‌تواند به شناسایی و کاهش مؤثر تهدیدات نوظهور کمک کند.
- **نیاز به یک مدل هوش مصنوعی خودکار:** ازآنجایی‌که الگوهای حمله توزیع‌شده انکار سرویس مبتنی بر اینترنت اشیا با سرعت زیادی در حال تغییر هستند، نیاز به مدل‌های هوش مصنوعی خودکار وجود دارد که بتوانند به طور خودکار همراه با الگوهای مختلف ترافیکی به‌روزرسانی شوند.

مراجع

[1] Almazrouei, Essa, Shubair, Raed M., Saffre, Fabrice,, "Internet of nanothings: Concepts and applications," arXiv preprint arXiv:1809.08914., 2018.

[2] Brun, O., Yin, Y., Augusto-Gonzalez, J., Ramos, M., & Gelenbe, E. , "Iot attack detection with deep learning. ," In ISCIS Security Workshop., 2018.

[3] Houbakht Attaran, Nahid Kheibari, Davoud Bahrepour, "Toward integrated smart city: A new model for implementation and design challenges," GeoJournal, pp. 511-526, 2022.

[4] Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F., "Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. ," Mobile Networks and Applications, vol. 28, no. 1, pp. 296-312, 2023.

[5] Cil, A.E.; Yildiz, K.; Buldu, A. , "Detection of DDoS attacks with feed forward based deep neural network

model.," Expert Syst. Appl., vol. 169, 2021.

[6] Patil, N.V.; Krishna, C.R.; Kumar, K., " SSK-DDoS: Distributed stream processing framework based classification system for DDoS attacks.," Clust. Comput. , vol. 25, p. 355–1372, 2022.

[7] Oncioiu, R., & Simion, E., " Approach to prevent SYN flood DoS Attacks in Cloud. ," In 2018 International Conference on Communications (COMM). IEEE., pp. 447-452), 2018.

[8] M. Sanlı, "Detection and Mitigation of Denial of Service Attacks in Internet of Things Networks. ," Arabian Journal for Science and Engineering, pp. 1-11, 2024.

[9] A. Spognardi, M.D. Donno, N. Dragoni, A. Giaretta,, " Analysis of DDoS-capable IoT malwares,," in: Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, IEEE, pp. 807-816, 2017.

[10] Bala, B., & Behal, S. , "AI techniques for IoT-based DDoS attack detection: Taxonomies, comprehensive review and research challenges.," Computer science review,, vol. 52, 2024.

[11] Wong, F., & Tan, C. X., "A survey of trends in massive DDoS attacks and cloud-based mitigations.," International Journal of Network Security & Its Applications, vol. 6, no. 3, p. 57, 2014.

[12] Ozcelik, M.; Chalabianloo, N.; Gur, G., " Software-Defined Edge Defense Against IoT-Based DDoS.," In Proceedings of the 2017 IEEE International Conference on Computer and Information Technology (CIT), Helsinki, Finland, p. 308–313., 2017.

[13] Kepçeoğlu, B., Murzaeva, A., & Demirci, S. , " Performing energy consuming attacks on IoT devices.," In 2019 27th Telecommunications Forum (TELFOR) (pp. 1-4). IEEE., 2019.

[14] Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. , "Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach.," Sensors, vol. 20, no. 3, pp. 816-823, 2020.

[15] Kumari, P., & Jain, A. K., "Timely detection of DDoS attacks in IoT with dimensionality reduction. ," Cluster Computing, , pp. 1-19, 2024.

[16] Sinha, M., Bera, P., & Satpathy, M., "SYN-Monitor: An Energy Efficient Defense System against TCP-SYN Flooding Attacks in SDN. ," In Proceedings of the 26th International Conference on Distributed Computing and Networking, 2025.

[17] Ramadhan, G.; Kurniawan, Y.; Kim, C. S., "Design of TCP SYN flood DDoS attack detection using artificial immune systems.," In IEEE 6th International Conference on System Engineering and Technology (ICSET), pp. 72-76, 2016.

[18] L. DaYin, "A DDoS Attack Detection and Mitigation with Software Defined Internet of Things Framework Security and Trusted Computing For Industrial Internet of Things," IEEE, pp. 24694 -24705, 2018.

[19] Diro, A. A., Chilamkurti, N., & Nam, Y. , "Analysis of lightweight encryption scheme for fog-to-things communication.," IEEE Access, vol. 6, pp. 26820-26830, ۲۰۱۸.

[20] Dang, V. T., Huong, T. T., Thanh, N. H., Nam, P. N., Thanh, N. N., & Marshall, A., " Sdn-based syn proxy—a solution to enhance performance of attack mitigation under tcp syn flood. ," The Computer Journal, vol. 62, no. 4, pp. 518-534, 2019.

[21] Berguiga, A., & Harchay, A., "An IoT-Based Intrusion Detection System Approach for TCP SYN Attacks," Computers, Materials & Continua, vol. 71, no. 2, 2022.

[22] Kshirsagar, D., Kumar, S., "A feature reduction based reflected and exploited DDoS attacks detection system.," J. Ambient Intell. Humaniz. Comput. , vol. 13, no. 1, pp. 393-405, 2022.

[23] Rahman, S., Pal, S., Mittal, S., Chawla, T., & Karmakar, C., "SYN-GAN: A robust intrusion detection system using GAN-based synthetic data for IoT security. ," Internet of Things, vol. 26, 2024.

[24] Chauhan, P., & Atulkar, M., " An efficient attack detection approach for software defined Internet of Things using Jaya optimisation based feature selection technique.," International Journal of Communication Networks and Distributed Systems, vol. 31, no. 1, 2025.