حملات انکار سرویس (DoS) و حملات توزیع شده انکار سرویس (DDoS) تلاش‌های مخربی هستند که با فراگیر کردن یک سیل ترافیک، قابلیت دسترسی به یک سرویس یا سیستم را مختل می‌کنند. تشخیص و کاهش این حملات برای حفظ عملکرد طبیعی شبکه‌ها و جلوگیری از اختلال در سرویس‌ها بسیار حیاتی است. روش‌های یادگیری ماشین می‌توانند برای تشخیص و کاهش حملات DoS و DDoS با تحلیل الگوهای ترافیک شبکه و شناسایی ناهنجاری‌ها که نشاندهنده این حملات هستند، استفاده شوند.

چندین روش بر پایه یادگیری ماشین برای تشخیص حملات DoS و DDoS وجود دارد. در ادامه نمونه‌هایی از روش‌های تشخیص حملات DoS و DDoS مبتنی بر یادگیری ماشین را می‌توانید مشاهده کنید:

1. ماشین بردار پشتیبان (SVM): SVM یک الگوریتم یادگیری نظارت شده محبوب برای وظایف طبقه‌بندی است، از جمله تشخیص حملات DoS و DDoS. آن یک هایپرپلین ایجاد می‌کند که ترافیک طبیعی و حمله را در یک فضای ویژگی با بعد بالا از یکدیگر جدا می‌کند. SVM قادر است با مسائل طبقه‌بندی خطی و غیرخطی برخورد کند و از این روی می‌تواند الگوهای پیچیده حملات را تشخیص دهد.

2. جنگل تصادفی: جنگل تصادفی یک تکنیک یادگیری ترکیبی است که تعدادی از درختان تصمیم را برای پیش‌بینی‌ها به کار می‌گیرد. هر درخت تصمیم بر روی یک زیرمجموعه تصادفی از ویژگی‌ها از مجموعه داده آموزش آموزش دیده می‌شود. جنگل تصادفی قادر است به خوبی با داده‌های با بعد بالا برخورد کند و روابط پیچیده بین ویژگی‌ها را درک کند که آن را برای تشخیص حملات DoS و DDoS مناسب می‌سازد.

3. k-نزدیک‌ترین همسایه (k-NN): k-NN یک الگوریتم ساده و قابل فهم است که نمونه‌های جدید را بر اساس آرا‌ی اکثریت همسایگان نزدیکشان در مجموعه داده آموزش، دسته‌بندی می‌کند. این الگوریتم از طریق معیارهای فاصله، شباهت بین نمونه‌ها را اندازه‌گ

یری می‌کند. k-NN می‌تواند با در نظر گرفتن شباهت الگوهای ترافیک شبکه و برچسب‌گذاری نمونه‌ها، در تشخیص حملات DoS و DDoS مورد استفاده قرار گیرد.

4. شبکه‌های عصبی: شبکه‌های عصبی، به خصوص ساختارهای یادگیری عمیق مانند شبکه‌های عصبی پیچشی (CNN) و شبکه‌های عصبی بازگشتی (RNN)، در حوزه‌های مختلف موفق بوده‌اند، از جمله امنیت سایبری. این مدل‌ها می‌توانند الگوها و روابط پیچیده در داده‌های ترافیک شبکه را یاد بگیرند و از این روی حملات پیچیده DoS و DDoS را تشخیص دهند. CNN برای تحلیل ویژگی‌های سطح بسته مناسب است، در حالی که RNN می‌تواند وابستگی‌های زمانی در توالی‌های ترافیک را ضبط کند.

5. بیز ناخوشه‌ای: بیز ناخوشه‌ای یک طبقه‌بند احتمالی است که احتمال نمونه‌ای را که بر اساس ویژگی‌های مشاهده‌شده، در یک کلاس خاص قرار دارد، محاسبه می‌کند. با وجود فرضیات ساده خود، بیز ناخوشه‌ای در موارد خاصی نظیر تشخیص حملات DoS و DDoS موثر بوده است. این الگوریتم با داده‌های با بعد بالا به خوبی کار می‌کند و به دلیل سادگی و کارایی خود قادر است به طور زمان واقعی تشخیص را انجام دهد.

6. روش‌های مبتنی بر خوشه‌بندی: الگوریتم‌های خوشه‌بندی مانند k-means یا DBSCAN می‌توانند برای گروه‌بندی نمونه‌های مشابه بر اساس ویژگی‌هایشان استفاده شوند. با تجزیه و تحلیل ویژگی‌های هر خوشه، ناهنجاری‌ها به عنوان حملات محتمل شناسایی می‌شوند. این روش بدون نیاز به داده‌های آموزش برچسب‌گذاری شده است و برای تشخیص حملات ناشناخته یا حملاتی با تاریخچه معلوم نیز مناسب است.

این فقط چند نمونه از روش‌های یادگیری ماشینی است که برای تشخیص حملات DoS و DDoS استفاده می‌شود. هر روش دارای نقاط قوت و محدودیت‌های خود است و انتخاب روش به عواملی مانند مجموعه داده موجود، منابع محاسباتی و ویژگی‌های خاص حملاتی که قصد تشخیص آن‌ها را دارید، وابسته است. در انتخاب یک روش برای استقرار، مهم است که برداشت‌ها و تضادهای بین دقت تشخیص، پیچیدگی محاسباتی و عملکرد به طور زمان واقعی را در نظر بگیرید.

در ادامه مثالی از یک پیاده‌سازی که یادگیری ماشین را با تحلیل ترافیک شبکه برای تشخیص حملات DDoS ترکیب می‌کند، آورده شده است:

۱. جمع‌آوری مجموعه داده: یک مجموعه داده از ترافیک شبکه جمع‌آوری می‌شود که شامل هر دو ترافیک طبیعی و نمونه‌هایی از حملات DDoS است. این مجموعه داده باید برچسب‌گذاری شده باشد تا بتوان بین ترافیک طبیعی و حمله تمایز قائل شد.

۲. استخراج ویژگی: ویژگی‌های مرتبط از داده‌های ترافیک شبکه استخراج می‌شود. این ویژگی‌ها می‌توانند شامل اندازه بسته، نرخ بسته، نوع پروتکل، آدرس IP مبدأ/مقصد، شماره پورت و سایر ویژگی‌های سطح شبکه باشند.

۳. پیش‌پردازش داده: مجموعه داده پیش‌پردازش می‌شود تا کیفیت آن تأمین شده و برای الگوریتم‌های یادگیری ماشین آماده شود. این مرحله شامل پاک‌سازی داده، نرمال‌سازی و مقیاس‌بندی، و همچنین رفع مقادیر گم‌شده یا ناهنجاری‌ها در صورت لزوم است.

۴. مرحله آموزش: مجموعه داده پیش‌پردازش شده به دو قسمت تقسیم می‌شود: مجموعه آموزش و مجموعه آزمایش. مجموعه آموزش برای آموزش مدل یادگیری ماشین استفاده می‌شود. می‌توان از انواع الگوریتم‌های یادگیری نظارت‌شده مانند درخت تصمیم، جنگل تصادفی، ماشین‌های بردار پشتیبان (SVM) یا شبکه‌های عصبی استفاده کرد. با استفاده از نمونه‌های برچسب‌گذاری شده از ترافیک طبیعی و حمله، مدل به یاد می‌گیرد الگوها و ویژگی‌های هر کلاس را شناسایی کند.

۵. ارزیابی مدل: مدل آموزش دیده با استفاده از مجموعه آزمایش، در تمایز بین ترافیک طبیعی و حمله، عملکرد خود را ارزیابی می‌کند. معیارهای معمول ارزیابی شامل دقت، صحت، بازیابی و امتیاز F1 است.

۶. راه‌اندازی و نظارت به صورت زمان واقعی: هنگامی که مدل عملکرد قابل قبولی را نشان می‌دهد، می‌توان آن را در یک محیط شبکه به صورت زمان واقعی راه‌اندازی کرد تا ترافیک ورودی را به طور مداوم نظارت کند. سپس نمونه‌های ترافیک جدید به مدل داده می‌شوند و بر اساس الگوهای یادگرفته‌شده پیش‌بینی می‌شوند. اگر الگوی ترافیک ورودی به عنوان یک حمله DDoS پتانسیلی شناسایی شود، اقدامات مناسبی مانند فیلتر کردن ترافیک، محدود کردن نرخ و یا سیاه‌نویسی صورت می‌گیرد.

مهم است به این نکته توجه کنید که کارآمدی تشخیص حملات DDoS بر پایه یادگیری ماشین به کیفیت داده‌های آموزش، انتخاب ویژگی‌های مرتبط و انتخاب مناسب الگوریتم‌های یادگیری ماشین وابسته است. به‌روزرسانی‌های مداوم و آموزش دوباره مدل برای سازگاری با تکنیک‌های حمله در حال تکامل لازم است.

به طور خلاصه، تکنیک‌های یادگیری ماشین با تحلیل الگوهای ترافیک شبکه و شناسایی ناهنجاری‌ها، تشخیص حملات DDoS را تقویت می‌کنند. با آموزش یک مدل بر روی مجموعه داده‌های برچسب‌گذاری شده و راه‌اندازی آن به صورت زمان واقعی، سازمان‌ها می‌توانند توانایی تشخیص و کاهش حملات DDoS را بهبود دهند و قابلیت دسترسی و امنیت سرویس‌های خود را تضمین کنند.