نشریه علمی «پدافند الکترونیکی و سایبری»

سال هشتم، شماره ۱، بهار ۱۳۹۹؛ ص ۷۷-۶۷

مدل‌سازی حملات سایبری مبهم مبتنی بر فّن جایگزین حمله

کیانوش شوشیان*[۱]، علی جبار رشیدی[۲]، مهدی دهقانی[۳]

۱- دانشجوی دکتری، دانشگاه امام حسین(ع)، ۲- استادیار، دانشگاه صنعتی مالک اشتر،

۳- استادیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۷/۱۰/۱۰، پذیرش: ۹۸/۱۲/۱۴)

چکیده

با گسترش روزافزون حملات سایبری، ایجاد امنیت برای فضای سایبری نیز حساس‌تر و مهم‌تر شده است. بنابراین رایانه‌ها، شبکه‌های رایانه‌ای و تمام سامانه‌های رایج با قابلیت اتصال به شبکه اینترنت، همواره در معرض خطر حملات سایبری قرار دارند. در این مقاله با ارائه طبقه‌بندی جدیدی در روش‌های مبهم‌سازی، برای مدل‌سازی حملات سایبری مبهم، روشی مبتنی بر فّن جایگزین حمله پیشنهاد شده است. در این روش مهاجم در راهبردهای حمله با جایگزین کردن حملاتی که خصوصیات مشابه دارند، باعث افزایش دسته‌بندی غلط شده و وابستگی میان گام‌های حمله را کاهش می‌دهد؛ بنابراین با افزایش طول دنباله حمله، مدیران امنیت شبکه به‌راحتی نمی‌توانند حملات سایبری را تشخیص دهند. مدل پیشنهادی بر اساس الگوریتم بیزین ارزیابی گردید. نتایج به‌دست‌آمده از تحقیق و اجرای مدل، حاکی از آن است که نرخ دقت درست طبقه‌بندی (برحسب لگاریتم) توسط سامانه‌های تشخیص نفوذ، در بهترین حالت برای حملات پاک در دنباله حمله ۴۰ برابر ۰۲/- و برای حملات مبهم در سطح اقدام برابر ۰/۱۹- است؛ درصورتی‌که در همین دنباله برای حملات مبهم با فن جایگزین حمله به ۳- و برای فن اضافه حمله به ۶/۷۴- تقلیل می‌یابد. در مدل‌پیشنهادی مانند فن مبهم‌ساز افزودن حمله، از روش حمله متناظر استفاده شده است، به علت تفاوت در نوع مدل مبهم‌سازی نتایج مختلفی به‌دست می‌آید و ترکیب این دو فن مبهم‌ساز در حملات سایبری می‌تواند در فریب سامانه‌های تشخیص نفوذ و ایجاد عدم قطعیت در دنباله حملات مشاهده‌شده، نتایج بهتری برای مهاجم به ارمغان آورد.

کلیدواژه‌ها: مدل‌سازی حملات سایبری، مبهم‌سازی حمله، جایگزین حمله، دنباله حمله

۱. مقدمه

ابزار، دانش، تجهیزات و دکترین سایبری دشمنان به صورتی است که تشخیص روش‌ها و فنون حملات مهاجمان بسیار مشکل شده است. برای مقابله و بازدارندگی دشمنان از تهدیدات سایبری باید روش حملات آن‌ها شناسایی شود تا بتوان اقدام مناسب دفاعی را انجام داد. یکی از راه‌کارهای بازدارندگی مهاجمین می‌تواند دفاع پیش‌کنش‌گرانه فعال و هوشمند باشد، لذا باید تحقیقات به‌عمل‌آمده بتواند از شناسایی و تشخیص فن‌های نوظهور در حملات سایبری، پشتیبانی نماید.

لفظ مبهم‌سازی[۱] از مخفی‌کاری، تاریکی و تیرگی است. در حملات سایبری از اصطلاح مبهم‌سازی برای پنهان کردن اطلاعات مهم در حمله صورت گرفته، استفاده می‌شود. مبهم‌سازی، سازوکاری برای پنهان‌سازی هدف یا رفتار اصلی حمله است. به‌عبارت‌دیگر تغییر ظاهر برنامه یا رفتار تاکتیکی حمله بدون تغییر در عملکرد یا هدف غایی آن است، به‌گونه‌ای که شناسایی بدافزار توسط سامانه‌های تشخیص نفوذ در عمل سخت و یا غیرممکن است [۱]. در فنون مبهم‌سازی در سطح حمله، اصولاً خود حمله مبهم می‌شود ولی خصیصه‌ها، رفتار و حتی اثرگذاری حمله روی دارائی‌های قربانی تغییر نمی‌کند. در سامانه‌های تشخیص نفوذ، روش‌های تجزیه‌وتحلیل به دودسته کلی تشخیص سوءاستفاده و تشخیص ناهنجاری و یا ترکیبی از آن‌ها تقسیم می‌شوند [۲]. رویدادهای حمله عموماً از طریق سامانه‌های تشخیص نفوذ در سطح شبکه و یا رخدادهای بازرسی که در سطح میزبان وجود دارند، به شکل مشاهدات دنباله‌ای دیده می‌شوند [۳] مبهم‌سازی، سازوکار حمله به شکستن ماشین تطبیق الگو و یا ایجاد فریب در سامانه تشخیص نفوذ است که منجر به عدم شناسایی و یا سخت‌تر شدن حملات سایبری می‌شود [۴] هدف از مبهم‌سازی در دنباله‌های حمله، تلاش برای مخفی‌کاری و پنهان‌سازی اطلاعات مهم حمله و گمراه‌سازی سامانه‌های همبستگی هشدار به‌منظور عدم‌تشخیص یا تشخیص غلط و نادرست از حمله است [۵].

*رایانامه نویسنده پاسخگو: K.shoushian@chmail.ir

1-Obfuscation

مبهم‌سازی در سه سطح نویز، اقدام[1] و حمله قابل‌اجرا است.

۱-۱. **سطح نویز**، حمله مبهم‌شده‌ای که در آن از دانش مدل مبهم‌سازی برای طبقه‌بندی دنباله‌ها استفاده نشده است. مانند مبهم‌سازی در سطح بسته، سطح کد و یا مبهم‌سازی به‌وسیله رمزنگاری[۶].

- ✓ **سطح بسته**[2] ارسالی بین فرستنده و گیرنده از دانش مدل پروتکل TCP/IP برای اجرای عملکردهای فریب‌کارانه و یا فعالیت‌های زیرکانه و دزدکی سود می‌برد و مهاجم ترافیک مسیر را مبهم می‌نماید. جعل IP منبع، فنی است که به‌طور گسترده به‌منظور پنهان‌سازی هویت واقعی مهاجم استفاده می‌شود. شکل (۱) نمونه‌ای از قوانین اسنورت[3] را بر روی آسیب‌پذیری RPC Sadmind نشان می‌دهد. در این مثال مهاجم می‌تواند از یک ویرایشگر هگز استفاده کند تا یک فایل باینری را که این امضا را شامل می‌شود، بسازد. پس از این‌که اتصال TCP بر روی یک درگاه بازساخته شد، بارگیری پی آیند ساخته‌شده، هشداری را ایجاد خواهد کرد و سبب تزریق یک مشاهده نویزی می‌گردد [۷].

- Rule Header
  - alert tcp $External_NET any -> $Home_Net21
- Rule Options
  - (msg: "ftp Exploit"; flow_to_server, established; content: "|31c031db 41c9b046 cd80 31c031db|"; reference: bugtraq,1387; classtype:attempted-admin; sid 344; rev4;)

شکل (۱): مثالی از قانون Snort RPC Sadmind

- ✓ **مبهم‌سازی کد**[4]، یکی از اولین اهداف مبهم‌سازی کد، مقابله با تحلیل ایستا است. تحلیل ایستا با بررسی و پیمایش خط به خط کد برنامه، سعی در استخراج رفتارهای احتمالی کد دارد. یکی از تلاش‌های معروف جهت مبهم‌سازی کد اجرایی تبدیل یا تغییر کد است. مانند افزودن کدهای مرده، جابجایی دستورالعمل‌های پرش با برخی کدهای خطادار [۸]. این فنون ظاهر برنامه را بدون تغییر در عملکرد آن انجام می‌دهند، به‌گونه‌ای که شناسایی حملات توسط سامانه‌های تشخیص نفوذ در عمل سخت و یا غیرممکن است.

۱-۲. **سطح اقدام**، مبهم‌سازی در سطح اقدام به معنی انجام فنونی در اجرای اقدام و فعالیت‌های مقدماتی[1] حمله است به‌نحوی‌که سامانه‌های تشخیص نفوذ به خاطر افزایش مثبت‌های اشتباه و منفی‌های درست در هشدارها با عدم قطعیت بالایی مواجه می‌شوند لذا مدیران امنیت شبکه فریب‌خورده و حمله واقعی را به‌درستی تشخیص نمی‌دهند. فنون مبهم‌سازی در این سطح شامل تغییر اقدام[5]، افزودن اقدام[6] و حذف اقدام[7] است. با بهره‌گیری از میزبان‌های تسخیرشده (آسیب‌دیده) مهاجم به‌آسانی می‌تواند اقدامات مهم‌تر خود را پنهان کند و یا اقدامات بی‌ربطی را به‌منظور گیج کردن تحلیل‌گران تزریق کند، به‌گونه‌ای که تعداد زیادی از اقدامات از منابع مختلف ناشی می‌شوند. همچنین برای مهاجمان تزریق اقدامات حمله زائد امکان‌پذیر است؛ چراکه امضاهای مخرّب به‌صورت عمومی قابل‌دسترس هستند. مبهم‌سازی در سطح اقدام با سه فن مذکور می‌تواند، علائم بارز نرم‌افزارهای مخرب را پنهان یا تضعیف کند همچنین تحلیل نرم‌افزارهای مخرب را بی‌نتیجه می‌گذارد.

۱-۳. **سطح حمله**، مبهم‌سازی در سطح حمله به معنی انجام فنونی در تغییر حمله است، به‌نحوی‌که سامانه‌های تشخیص نفوذ عملکرد صحیحی دارند و هشدارها را به‌درستی تشخیص می‌دهند، ولی چون نوع حمله مهاجم (با همان اثرگذاری) تغییر کرده است، مدافعین شبکه فریب‌خورده و حمله واقعی را از حمله مبهم‌شده تشخیص نمی‌دهند. مهاجم در این روش ممکن است از چندین اقدام پایه‌ای برای فریب دادن مدیران امنیتی استفاده کند. مهاجم برای مخفی بودن دنباله حملات خود از سه فن مبهم‌ساز بهره می‌برد شامل:

- ✓ **فن افزودن حمله**، یکی از روش‌هایی که تأثیر زیادی در به وجود آوردن عملکرد غلط و گمراه کردن موتورهای تحلیل هشدار وجود دارد، افزودن حمله در دنباله حملات است. افزایش دسته‌بندی غلط در راهبردهای حمله توسط مهاجم باعث جدا شدن وابستگی میان هشدارها و اقدامات حمله می‌شود. با انجام این فن، طول دنباله حمله مبهم بیشتر از طول دنباله حمله پاک می‌شود؛ ولی نوع اثرگذاری دو حمله پاک و مبهم بر روی دارائی‌های قربانی یکسان و برابر است.

$$L(Y1) + L(Y2) \ldots + L(Yn) > L(X1) \quad A(Y) = A(X) \qquad (۱)$$

در رابطه (۱)، X برای حملات پاک، Y برای حملات مبهم، A به معنی حمله و L برای طول دنباله حمله به‌کار رفته است.

- ✓ **فن حذف حمله**، در فن حذف حمله، طول دنباله حمله مبهم، کمتر از طول دنباله پاک می‌گردد. تحلیل‌گران

1- Action-level
2- Packet-level
3- Snort
4- Code-level
5- Action alternation
6- Action insertion
7- Action removal

امنیتی می‌توانند از طریق اضافه و کم کردن پیوندها ساختار مدل را تغییر داده و سناریوهای متنوّع دیگری را برای مدل مبهم با فن حذف حمله منعکس کنند. در این فن طول دنباله حمله مبهم Y از طول دنباله حمله پاک X کوچک‌تر خواهد شد؛ ولی نوع اثرگذاری دو حمله پاک و مبهم یکسان و برابر است.

$$L(Y) < L(X) \quad (۲)$$
$$A(Y) = A(X)$$

در این روش، مهاجم سعی دارد هشداری که نشان‌دهنده حالت نفوذ اصلی است را با حذف برخی از حملات که امکان حذف وجود دارد، مخفی کند.

- ✓ **فن جایگزین حمله،** تغییر یا جایگزینی حمله می‌تواند دنباله‌ی مشابهی از حملات واقعی ایجاد نماید، این دنباله‌ی مشابه می‌تواند تمام دنباله‌های پرکاربردتر را به‌وجود آورد. هم‌چنین می‌تواند از شناسایی شدن توسط تطبیق با الگوی دنباله متداول نفوذی جلوگیری به‌عمل آورد. در مبهم‌سازی با فن جایگزین حمله طول دنباله حمله مبهم برابر طول دنباله حمله پاک است؛ ولی نوع اثرگذاری دو حمله پاک و مبهم مانند دو فن دیگر مبهم‌سازی در این سطح یکسان و برابر است.

$$L(Y) = L(X) \quad (۳)$$
$$A(Y) = A(X)$$

این مقاله در نظر دارد مفهوم مبهم‌سازی در سطح حمله را برای اولین بار تبیین نماید؛ همچنین این‌که تمرکز این پژوهش فقط بر فن جایگزینی حمله استوار است.

بخش‌های بعدی این مقاله به‌صورت زیر خواهند بود. در بخش دوم کارهای مرتبط بیان می‌شود. بخش سوم به بیان مدل پیشنهادی، روش اجرا و نتایج حاصل از مدل اختصاص داده‌شده و سپس در ادامه همین بخش مدل پیشنهادی مورد ارزیابی قرار می‌گیرد و در بخش چهارم و نهایی نتایج به‌دست‌آمده از مبهم‌سازی مورد تحلیل قرار می‌گیرد.

۲. کارهای مرتبط

نجاری [۹] مبهم‌سازی حملات را برای فن حذف اقدام تحلیل کرده است و ضمن تشکیل پایگاه داده‌های هم‌گروه، الگوریتمی برای تولید دنباله‌های حملات مبهم ارائه کرد و سپس روش خود را از منظر میزان نویز تزریقی و طول دنباله حمله مورد ارزیابی قرار داد.

غفوری [۱۰] با توجه به داده‌های ماتریس OPPM[1] پیشنهادی، توانست الگوریتم مبهم‌ساز حمله مبتنی بر جایگزینی اقدام را طراحی کند و به تولید دنباله حمله دست یابد. سپس رفتار دنباله‌های حملات مختلف که از خود طول دنباله حمله تولید می‌شوند، را تحلیل کرد و توانست مقدار پارامتر مؤثر سطح مبهم‌سازی برای تولید یک دنباله حمله مبهم را به‌گونه‌ای تعریف کند که مبهم‌سازی از کارآمدی بیشتری برخوردار شود و در ادامه تحقیق خود، دنباله‌های مختلف به‌دست‌آمده از الگوریتم مبهم‌سازی خود را طبقه‌بندی کرده و چالش‌های مربوط به‌دقت طبقه‌بندی مورد انتظار تحلیل‌گر را برطرف نمود. در آخر با استفاده از حل این چالش‌ها دقت طبقه‌بندی مورد انتظار را در مقایسه با تحقیقات قبلی، بهبود بخشید.

علی‌آبادی [۱۱] از فن حذف اقدام برای تولید دنباله حملات مبهم استفاده کرده و برای تحلیل و ارزیابی تأثیر مبهم‌سازی در حملات از الگوریتم بیز بهره برده است او با بررسی حدود ۱۰۰ نمونه از دنباله حملات پاک و مبهم‌سازی آن‌ها نتیجه گرفت که با افزایش طول دنباله حملات چندگامی، میزان احتمال ابهام‌زدایی حملات بیشتر و میزان مبهم‌سازی آن کاهش می‌یابد.

دو [۱۲] در رساله دکترای خود به مدل‌سازی احتمالی و استنباطی برای دنباله حملات مبهم سایبری پرداخت. در این رساله ابتدا مطالعه‌ای در مورد این نوع از حملات و نحوه مدل‌سازی روش‌های مبهم و طبقه‌بندی کردن دنباله‌ها و همچنین فرموله‌سازی آن‌ها پرداخته و سپس حملات مختلف امکان‌پذیر و روابط اتفاقی ناشی از حملات را به‌دست آورد. این محقق یک دنباله حمله صوری[2] را به‌عنوان بردار متغیرهای تصادفی توصیف‌شده در نظر گرفت و هر مشاهده را یک نمونه از مدل‌های حمله به‌شمار آورد. درنهایت به‌منظور نمایش میزان تأثیر دنباله حمله‌های مبهم و پاک، یک شبیه‌سازی ارائه کرد.

وانگ و همکارانش [۱۳] بحث استفاده از گراف حمله را جهت همبسته‌سازی، فرضیه‌سازی و پیش‌بینی هشدارهای نفوذ مدل‌سازی کردند. ایده اصلی در گراف حمله ارائه یک نمایش کارا و ابزارهای الگوریتمی جهت شناسایی آسیب‌پذیری‌های سامانه‌ای است؛ که احتمال دارد مورد بهره‌برداری مهاجم قرار گیرد. این رویکرد به‌شدت به دانش صحیح و کافی از آسیب‌پذیری‌های سامانه و قواعد دیوار آتش در شبکه وابسته است. باوجودی که هکرها ابزارهای زیادی جهت اسکن کردن شبکه را به‌منظور دریافت اطلاعات در اختیار دارند، ولی در شبکه‌های تجاری بزرگ با چندین سامانه مدیریتی که هر سامانه بخش‌های مختلفی از

1- Obuscation Possible Probability Matrix
2- Formal

شبکه را مدیریت می‌کند، ناکارآمد است. باید توجه داشت که نمایش آسیب‌پذیری‌ها در شبکه توسط محققان دیگر در اواخر دهه‌ی ۹۰ و اوایل ۲۰۰۰ برای مثال فیلیپس و اسویلر [۱۴]، تیدول و همکارانش [۱۵]، دالی و همکارانش [۱۶] انجام شده است. بیش‌تر این کارها مشکل مقیاس‌پذیری را هنگام مدل‌سازی همه مسیرهای آسیب‌پذیر محتمل در شبکه از خود نشان داده‌اند. رویکرد گراف حمله‌ای که به‌وسیله وانگ و همکاران در [۱۳] و نوئل و جاجودیا در [۱۷] ارائه شده است، روش‌هایی را برای کم کردن مشکل مقیاس‌پذیری نشان داده است. از نواقص تحقیقات به‌عمل‌آمده می‌توان به عدم پرداختن به موضوع مبهم‌سازی در سطح حمله اشاره کرد. در این تحقیق با مقایسه اختلاف مبهم‌سازی در سطح اقدام و حمله، اثرگذاری و کارایی بهتر روش پیشنهادی نشان داده خواهد شد. همچنین در تحقیقات مورد اشاره با افزایش طول دنباله حمله، نرخ طبقه‌بندی درست در دنباله حملات برای سامانه‌های تشخیص نفوذ آسان شده و حملات قابل تشخیص می‌گردند.

۳. فضای اقدامات حملات سایبری

اقدامات حملات سایبری را می‌توان با توجه به ویژگی‌های گزارش‌شده و الگوهای حمله آن‌ها مدل کرد که این امر سبب طبقه‌بندی اقدامات حمله در گروه‌های مختلف شده است. پروژه‌های بسیاری روی طبقه‌بندی انواع آسیب‌پذیری‌ها و حملات در سطح وب انجام‌شده است. در این راستا فهرست‌های متعددی نیز تهیه‌شده‌اند که در برخی از آن‌ها اجماع عمومی در مورد شناسایی و نام‌گذاری انواع آسیب‌پذیری‌ها و حملات وجود دارد. چهار مورد از مهم‌ترین این طبقه‌بندی‌ها عبارت‌اند از: برنامه وب و کنسرسیوم امنیتی[1] پروژه امنیت برنامه‌های وب باز[2]، شمارش و طبقه‌بندی الگوهای حمله رایج (کیپک)[3] و شمارش ضعف‌های رایج[4]. در این تحقیق، مبهم‌سازی حملات سایبری بر اساس دسته‌بندی‌های مربوط به شرکت میتره[5] به نام کیپک شکل‌گرفته است. آن‌ها به هر حمله یک شناسه مشخص اختصاص داده‌اند که به دلیل سهولت در مراجعه به لیست فوق سعی شده است شناسه‌های مشخص‌شده مورد استفاده قرار گیرد. براساس این استاندارد الگوی حملات سایبری را می‌توان بر دو محور مکانیسم و دامنه طبقه‌بندی کرد. برای محور مکانیسم داریم:

$$Mechanisms = \{ Category\ 1, \dots, Category\ 9 \} \quad (۴)$$

$$C = \{ Meta\ 1, Meta\ 2 \dots Meta\ n \} \quad (۵)$$

روابط (۴) و (۵) بیان می‌دارد، مکانیسم حملات سایبری به ۹ گروه با ویژگی‌ها و اهداف مختلف مطابق جدول (۱) دسته‌بندی[6] شده‌اند و هر دسته‌بندیC شامل تعدادی حمله سطح بالای متا است [۱۸].

جدول (۱): دسته‌بندی حملات سایبری [۱۸]

ردیف	دسته‌بندی حمله	شناسه
۱	مشارکت در تعاملات فریبنده	۱۵۶
۲	سوءاستفاده از عملکرد موجود	210
۳	دست‌کاری ساختار داده‌ها	255
۴	دست‌کاری منابع سامانه	262
۵	تزریق فایل‌های ناخواسته	152
۶	استفاده از روش‌های احتمالی	223
۷	دست‌کاری زمان‌بندی و وضعیت	172
۸	جمع‌آوری و تحلیل اطلاعات	118
۹	ازبین بردن کنترل دسترسی	225

۴. مدل پیشنهادی

مدل پیشنهادی به‌کار رفته شده در این تحقیق برای مدل‌سازی حملات سایبری مبهم مطابق شکل (۲) است.

شکل (۲): مدل پیشنهادی حمله متناظر با فن جایگزین اقدام.

ارائه مدل احتمالاتی مبهم حمله متناظر با فّن جایگزین حمله مبتنی‌بر تأثیر روی دارائی‌ها و سرمایه‌های قربانی خواهد بود. این مدل، با استفاده از مفاهیم شبکه بیزی که از اقدامات حملات پاک متناظرشان پیروی می‌کنند و هم‌گروه هستند، ارائه می‌شود. بر اساس مدل پیشنهادی تحقیق، مبهم‌سازی حملات بر اساس خوشه‌بندی تشابه و عدم تشابه اثرگذاری حمله و اهداف مهاجم شکل می‌گیرد. به‌عبارت‌دیگر نمونه‌های مشابه با یکدیگر در یک خوشه و نمونه‌های غیرمشابه در خوشه‌های متفاوتی گروه‌بندی می‌شوند، بنابراین به‌منظور تشابه‌سنجی، نیاز به مقیاس یا معیار ضروری است. ازآنجاکه هر نمونه می‌تواند صفات خاصه متعددی داشته باشد و هر یک از این صفات خاصه یک نوع داده تلقی می‌شود، لذا در محاسبه یا تحلیل تشابه دو نمونه باید معیار تشابه برای انواع داده تعریف شود و سپس این داده‌ها تبدیل به اطلاعات می‌شود و به‌عنوان پایگاه داده برای شبیه‌سازی و ارزیابی استفاده خواهد شد. برای مبهم‌سازی حملات به

1 Web Application Security Consortium (WASC)
2 OWASP
3 Common Attack Pattern Enumeration and Classification(CAPEC)
4 CWE
5 MITRE
6 Category

گروه‌بندی کردن فضای اقدامات حمله مطابق جدول (۲) نیاز داریم لذا با استفاده از اطلاعات سایت امنیتی کیپک و به‌صورت دستی این کار انجام می‌گردد.

جدول (۲): خوشه‌بندی حملات سایبری مبتنی بر تأثیرات حمله.

اثرگذاری	شناسه دسته	دسته	شناسه حمله
CIA	۱	۱۵۶	۱۳
CIA,AC,AU	۴	۲۶۲	۲۲
CIA,AC,AU	۹	۲۲۵	۱۶۹
C1A	۴	۲۶۲	۷۹

همچنین مطابق جدول (۳) معیار تشابه برای خوشه‌بندی حملات سایبری، اثرگذاری حمله بر روی سرمایه‌ها و دارایی‌های سایبری قربانی است. تکراری بودن شناسه‌ها به این خاطر است که، یک شناسه حمله احتمال دارد چند اثرگذاری مختلف بر روی دارائی‌های قربانی ایجاد کند.

جدول (۳): گروه‌بندی فضای برخی از اقدامات حمله (یافته‌های تحقیق).

گروه اول			گروه دوم			گروه سوم			گروه چهارم			گروه ۵		
محرمانگی			کنترل دسترسی			قابلیت دسترسی			احراز هویت			یکپارچگی		
۱۷	۱۹	۲۱	۱	۳	۴	۲	۵	۱۴	۱	۳	۴	۳	۶	۸
۲۲	۱۵۱	۱۷۳	۵	۶	۹	۱۷۳	۴۱۶	۷	۵	۹	۱۰	۹	۱۰	۱۴
۴۱۶	۹۸	۸۹	۱۰	۱۱	۱۲	۸	۹	۱۰	۱۱	۱۲	۱۶	۱۷	۱۹	۱۹۴
۶	۱۳	۸	۱۳	۱۴	۱۷	۱۳	۱۴	۱۷	۱۷	۱۹	۲۱	۶۳۳	۴۱۶	۱۵۱
۱۳	۱۷۳	۱	۱۸	۱۹	۲۰	۱۹		۲۱	۲۲	۱۵۱	۹۸	۱۴۸	۲۱	
۵۸۷	۲۲	۲۰	۲۱	۲۲	۱۵۱				۱۳	۱۵۴	۱۵۹			

شرط جایگزینی دو حمله، اثرگذاری یک حمله بر قربانی است. که این اثرگذاری در هر سطحی از حمله میسر است. به‌طور مثال اگر بخواهیم چهار حمله ۱۶۹،۱۳،۲۲،۷۹ را طبق جدول (۴) با همدیگر مقایسه کنیم می‌توان نتیجه گرفت:

اگر هدف مهاجم تزریق یا دست‌کاری منابع باشد حمله ۱۳ با حمله ۷۹ قابل جایگزین است و انجام سایر اقدامات مانند دست‌کاری پروتکل و یا تجزیه برای مهاجم می‌تواند به‌عنوان فریب قرار گیرد و به‌عنوان حذف حمله و یا اضافه حمله به‌کار رود. درصورتی‌که مهاجم بخواهد حمله ۱۳ را با حمله ۱۶۹ جابجا کند شرایط فرق می‌کند به‌این‌صورت که فقط زمانی می‌تواند این جایگزینی حمله را انجام دهد که هدف مهاجم تزریق، دست‌کاری پروتکل و یا تجزیه حمله باشد و اجرای دو پارامتر دیگر یعنی دست‌کاری منابع و مهندسی اجتماعی می‌تواند باعث فریب مدافع شبکه قرار گیرد و این اختلاف در اجرای حملات در دو حمله به‌صورت دو فّن تزریق حمله و یا حذف حمله است که با این شرایط مدافع نمی‌تواند تشخیص دهد که مهاجم می‌خواهد حمله ۱۳ را انجام دهد.

جدول(۴): مقایسه پنج حمله ازلحاظ عملکردی.

تاثیرحمله ۱۶۹	تاثیرحمله ۷۹	تاثیرحمله۲۲	تاثیرحمله۱۳
Read Data(RD)	Execute Unauthorized Commands(EUC)	Execute Unauthorized Commands(EUC)	Execute Unauthorized Commands (EUC)
	Bypass Protection Mechanism(BUC)	Gain Privileges(GP)	Bypass Protection Mechanism (BUC)
	Read Data(RD)	Read Data(RD)	Unreliable Execution (UE)
			Read Data(RD)

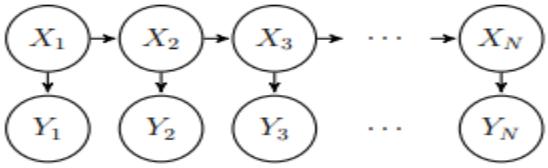
باید توجه داشت حملات ۱۳ و ۲۲ و ۷۹ به‌جز خواندن داده‌های هدف، سودهای دیگری به مهاجم می‌رسانند. لذا با انجام جایگزینی حمله عملاً فّن اضافه حمله نیز صورت گرفته است؛ یعنی اگر فرض شود، حمله ۷۹ جایگزین حمله ۱۶۹ شده است، اثرگذاری‌های EUC و BUC بر روی قربانی نیز انجام‌گرفته است و سامانه‌های تشخیص نفوذ هشدارهای مربوط به حمله ۷۹ را اعلان می‌کنند درصورتی‌که هدف مهاجم فقط عملیات RD بوده است و از آنجائی که این دو حمله مقدمات حملات سطح بالاتری را فراهم می‌کنند، وقتی مهاجم حملات خود را به ریشه حمله اصلی به‌صورت درخت‌واره گسترش دهد، مبهم‌سازی اثرات خود را بیشتر و بیشتر نشان می‌دهد به‌نحوی‌که تشخیص سناریوی نهایی مهاجم شاید اصلاً قابل تشخیص نباشد. حال اگر در نظر گرفته شود، هدف مهاجم عملیات EUC و BUC و RD باشد، برحسب قاعده باید حمله ۷۹ را انجام دهد ولی مهاجم می‌خواهد سامانه‌های تشخیص نفوذ را فریب دهد لذا مهاجم عملیات ۱۳ را انجام می‌دهد، لذا اقدامات مربوط به UE را حذف می‌کند. در اینجا علاوه بر فّن مبهم‌سازی جایگزینی حمله، فّن حذف حمله نیز صورت گرفته است.

۴-۱. روش اجرا

در روش‌های مبهم‌سازی از نوع تغییر یا جایگزینی حمله، مهاجم می‌تواند دنباله حملات مشابهی را ایجاد نماید که این دنباله مشابه می‌تواند تمام دنباله‌های پرکاربردتر را به‌وجود آورد. لذا بهره‌گیری از این فن باعث عدم شناسایی شدن حمله اصلی توسط تطبیق با الگوی دنباله حملات متداول نفوذی می‌شود.

این مدل جایگزینی حمله دنباله حمله پاک و دنباله حمله مبهم با طول یکسان، همان مدل مخفی مارکوف[1] است. HMM مدلی است که به‌طور گسترده‌ای برای توصیف مشاهدات دنباله‌های نویزی درجایی که متغیرهای تصادفی دنباله پاک پنهان شده‌اند و آنچه مشاهده می‌شود، دنباله مبهم است، استفاده می‌شود. شکل (۳) از نمادهای گرافیکی HMM برای نشان دادن دنباله با طول N طبق رابطه (۶) استفاده می‌کند.

$$P(Y|X) = \prod_{k=1}^{N} P(Yk|Xk) \qquad (۶)$$



شکل (۳): مدل گرافیکی برای مدل مخفی مارکوف

در HMM مشاهده می‌شود که رخداد i تنها به‌طور مستقیم به وابستگی حالت پنهان i بستگی دارد، P(Y|X) برای HMM می‌تواند به‌صورت رابطه (۷) نوشته شود.

$$P(Y|X) = \frac{n(Yi \cap (Yi \cup Xi) n(r)}{n(Yi \cup Xi) n(s)} \qquad (۷)$$

اصطلاح P(Y|X) احتمال انتشار نامیده می‌شود که می‌تواند در قالب تابع مبهم g(x,y) تعریف شود. مدل مبهم HMM عملکرد مهاجمان را به‌صورت جداگانه در تمام طول حملات در نظر می‌گیرد و $P(Y_k)$ به‌طور مستقیم وابسته به $P(X_k)$ است. در یک حمله واقعی این حالت هرگز اتفاق نمی‌افتد و رابطه‌های قوی‌تری بین بخش‌های مبهم وجود دارد.

۴-۲. مبهم‌سازی با درصد دلخواه

این طراح حمله سایبری است که تصمیم می‌گیرد چند درصد مبهم‌سازی در دنباله حملات خود صورت دهد. اگر فرض کنیم طراح هیچ‌گونه مبهم‌سازی را در حمله خود انجام ندهد، طبق رابطه (۸) داریم:

$$P(Ai \mid Aj) = \begin{cases} 1 & i=j \\ 0,0 & .w \end{cases} \qquad (۸)$$

درصورتی‌که مهاجم بخواهد α٪ مبهم‌سازی انجام ندهد، $0 \le \alpha/100 \le 1$ است. آنگاه طبق رابطه (۹) داریم:

$$P(Ai \mid Aj) = \begin{cases} \alpha/100 & i=j \\ 1-\frac{\alpha}{100} & i \neq j \end{cases} \qquad (۹)$$

بنابراین، به‌عنوان‌مثال برای فضای اقدامات حمله

$\Omega=\{ A_1 , A_2 , A_3 , A_4 \}$ ماتریس اولیه به‌صورت زیر است:

$$OPPM = \begin{bmatrix} P(A1|A1) & \cdots & P(A4|A1) \\ \vdots & \ddots & \vdots \\ P(A1|A4) & \cdots & P(A4|A4) \end{bmatrix} \qquad (۱۰)$$

حال ماتریس امکان مبهم‌سازی را مطابق روش زیر تعریف می‌کنیم، فرض می‌کنیم A_1 دارای n گام و حمله A_2 دارای n_2 گام شبیه به گام‌های A_1 باشد. آنگاه سطر متناظر با A_1 ماتریس احتمال امکان مبهم‌سازی مانند جدول (۵) خواهد بود.

جدول (۵): سطر متناظر با A_1 ماتریس OPPM.

A_i / P(Ai | Aj)	A_1	A_2	A_3	A_4
P(Ai | A1)	α n/n	α n_2/n	α n_3/n	α n_4/n
...	....	....	....	....
...	....	....	....	....
...	....	....	....	....

از آنجایی‌که مجموع احتمالات باید برابر یک شود برای سطر اول داریم:

$$\sum_{i=1}^{4} P(Ai \mid A1) = 1 \qquad (۱۱)$$

$$\alpha = \left(\frac{n}{n} + \frac{n2}{n} + \frac{n3}{n} + \frac{n4}{n}\right) = 1$$

$$\alpha = \frac{n}{n + n2 + n3 + n4} \qquad (۱۲)$$

به همین ترتیب ماتریس امکان سازی برای سایر حملات به‌صورت رابطه (۱۱) ساخته می‌شود، بنابراین، طراح حمله می‌تواند با توجه به این ماتریس و این‌که مبهم‌سازی با چه درصدی انجام شود نسبت به مبهم‌سازی حملات از طریق جایگزینی دنباله حملات باهم اقدام کند، که در این صورت با تعیین درصد مبهم‌سازی و با توجه به رابطه (۱۲) می‌توان ماتریس احتمالات امکان مبهم‌سازی را به دست آورد.

به‌عنوان‌مثال فرض کنید که طراح قصد دارد ۸۰٪ مبهم‌سازی را انجام دهد، بنابراین، α=۲۰ است. لذا $P(Ai \mid A1) = ۰/۲$ است. که $1 - \frac{\alpha}{۱۰۰} = ۰/۸$ مقدار احتمالی است که A_2 تا A_4 می‌تواند جایگزین A_1 شوند و مبهم‌سازی صورت گیرد.

در اینجا نیز بایستی مجموع احتمالات P (Ai | A1) ، ۲,۳,۴ =i برابر ۰/۸ شود. لذا یک ضریب β تعریف می‌کنیم و برای این مثال سطر اول ماتریس امکان مبهم‌سازی را به‌صورت جدول (۶) تشکیل می‌دهیم.

1- Hidden Markov Model(HMM)

جدول(۶): سطر متناظر با A_1 ماتریس OPPM با تأثیر β.

A_i / P(Ai| Aj)	A_1	A_2	A_3	A_4
P(Ai | A1)	0.2	$n_2/n\beta$	$n_3/n\beta$	$n_4/n\beta$
...	....	.....	....	....
...	.....	.....	.....	.....
...	....	....	.....	.....

به‌این‌ترتیب مقدار β به‌صورت رابطه (۱۳) به‌دست می‌آید:

$$\beta\, n_2/n \;+ \beta\, n_3/n + \beta\, n_4/n = ۰/۸ \quad (۱۳)$$

$$\beta = 0.8\, n\, (n_2 + n_3 + n_4)$$

جدول (۷) تأثیر ضریب β را برای چهار حمله ۱۳ و۲۲ ۷۹ و ۱۶۹را با فضای اقدامات حمله $\Omega_۱=\{ A_1^2, A_2^2, A_5^2, A_6^2 \}$ نشان می‌دهد.

جدول (۷): ماتریس OPPM با تأثیر β برای $\Omega_۱$.

A_i / P(Ai | Aj)	A_1	A_2	A_3	A_4
P(Ai | A1)	0.2	2/4β	2/4β	¾β
...	...	...	...	...
...	...	...	...	...

۴-۳. شاخص‌های ارزیابی مدل پیشنهادی

مدیران امنیت شبکه و مهاجمین، با به‌دست آوردن نرخ طبقه‌بندی درست دنباله حملات می‌توانند کارایی مدل حمله را به دست آورند. مهاجم باید بتواند تناسب افزایش عملکرد طبقه‌بندی بهینه را از افزایش طول دنباله مشاهده‌شده از بین ببرد، چراکه بهبود عملکرد حمله در هنگامی‌که طول دنباله کوچک است و سطح ابهام بالاست، بسیار اهمیت دارد. مدافع نیز باید بتواند پس از دریافت هشدارهای نفوذ و کاهش مثبت‌های اشتباه با همبسته‌سازی حملات، سناریوهای حمله مهاجم را به‌هم ربط دهد تا هدف نهایی مهاجم را تشخیص دهد. برای ارزیابی عملکرد مدل پیشنهادی شاخصه‌ای برای محاسبه نرخ تشخیص حملات سایبری مبهم تعریف نموده‌ایم:

تعریف ۱: مجموع دنباله‌های مشاهده‌شده از حملات مختلف را تحت عنوان «طول دنباله حمله» تعریف کرده‌ایم. طول دنباله حملات به دو صورت حمله پاک X طبق رابطه (۱۴) و حمله مبهم Y طبق رابطه (۱۵) تعریف می‌شوند.

$$X=\sum_{i=1}^{n} X1, X2, \ldots . Xn \quad (۱۴)$$

$$Y=\sum_{i=1}^{n} Y1, Y2, \ldots . Yn \quad (۱۵)$$

بدیهی است ارتباط زیادی بین طول دنباله حمله مبهم و دنباله حمله پاک وجود دارد. این روابط بر اساس فن‌های مختلف مبهم‌سازی متفاوت است.

تعریف ۲: نسبت تعداد اثرگذاری‌های حملات متناظر (m) بر طول دنباله کل حملات(n) در یک بازه زمانی مشخص انجام می‌شود. یعنی نسبت تعداد عملیات جایگزینی حمله بر روی یک حمله که مهاجم برای به نتیجه رسیدن حمله‌اش انجام داده به تعداد کل دنباله حملات. این نسبت را تحت عنوان «درصد مبهم‌سازی (OP)» تعریف نموده‌ایم و به‌صورت عبارت (۱۶) محاسبه می‌شود.

$$OP = m/n \quad (۱۶)$$

بدیهی است هر چه OP افزایش یابد، احتمال شناسایی حمله مبهم Y از روی حمله پاک X کاهش پیدا خواهد کرد. هم‌چنین این دو شاخص معرفی‌شده در تعاریف ۱و۲، پارامترهایی هستند که وجود ترکیبی آن‌ها، نشان‌دهنده نرخ مخفی‌سازی حمله را مشخص می‌کند.

۴-۴. ارزیابی مدل پیشنهادی

در این زیر بخش، برای تحلیل ارزیابی مدل پیشنهادی، پنج نمونه دنباله‌ی حملات مبهم را برای طول‌های مختلف مثال زده خواهد شد و براساس روابط زیر بخش قبل نتیجه خواهیم گرفت، در یک طول دنباله مشخص، آن دنباله با چه مقدار احتمالی مبهم شده است. برای این منظور، محاسبات لازم را بر اساس الگوریتم بیزین برای این پنج دنباله انجام می‌شود و نمودار احتمالات را برای دنباله‌های مبهم به دست می‌آوریم. در مثال ذکرشده برای پنج نمونه دنباله حمله پاک D`,E`,A`,B`, C` با حداکثر طول ۸، پنج دنباله مبهم شده A,B,C,D,E با حداکثر طول دنباله حمله برابر ذکر شده است، سپس احتمالات مبهم‌سازی این دنباله‌های حملات مبهم برحسب لگاریتم در طول‌های از ۱ تا ۸ (بر اساس طول‌های دنباله‌های پاک متناظرشان) محاسبه می‌گردد.

A`= {۱۷,۱۹,۲۱,۲۲,۱۵۱,۶,۱۳,۶۸}

A ={ ۱,۲۰,۱۷۳,۴۱۶,۴,۹۰,۱۸,۹۸}

B`={۱۵۹ ,۴۱۶,۵,۲۲,۱۵۱,۲۱,۹۸,۱}

B = {۹,۱۳,۶,۱۱,۱۲,۱۵۹,۱۷,۱۸}

C`={۱۷,۸,۱۷۳,۴۱۶,۱۸,۶,۱۹,۱۱}

C = {۵,۱۴,۱۳,۲۲,۷,۹,۱۰,۲۱}

D ={۳,۴,۱,۵,۹,۱۰,۱۱,۱۲}

D`= {۱,۱۹,۲۱,۲۲,۹۸,۱۵۱,۱۳,۱۴}

E`={ ۳,۶, ۸, ۱۴,۹,۱۹,۱۰,۱۷}

E = {۲۱,۱۴۸,۹۸,۴۱۶,۲۲,۱۷۳,۷,۱۸}

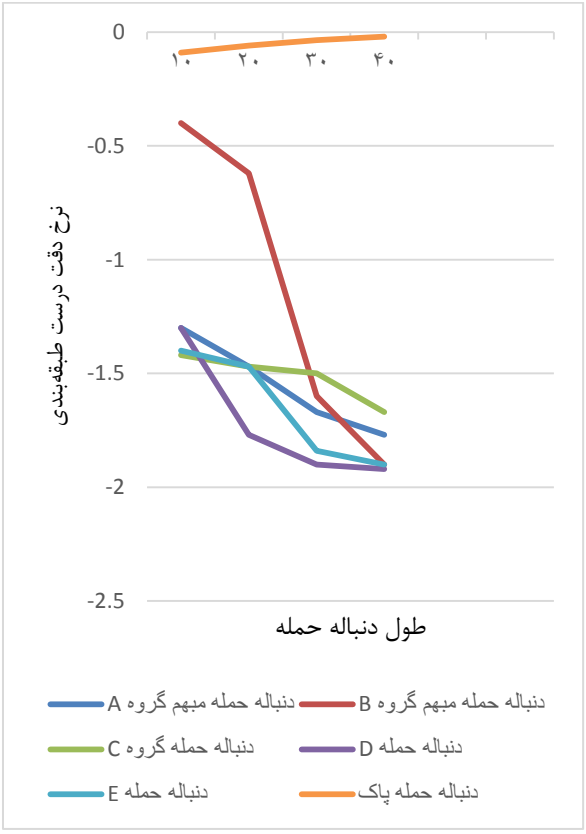
جدول (۸)، مثالی از دنباله حمله پاک و دنباله حمله مبهم را نشان می‌دهد. در این مثال طول دنباله حملات n=۲۰ است و در این مسئله بیشترین وزن احتمالاتی در ماتریس OPPM ملاک انتخاب حمله جایگزین قرار داده شده است.

جدول (۸): دنباله حمله پاک و دنباله حمله مبهم.

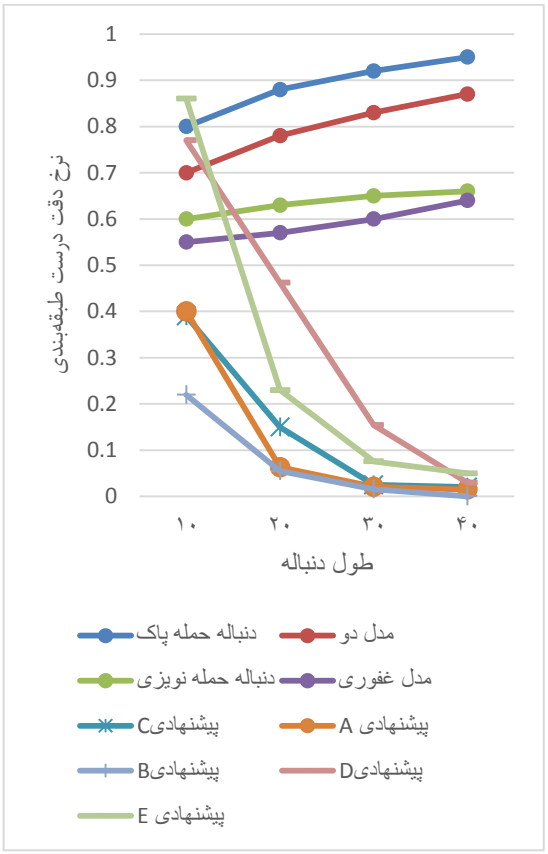
شماره	دنباله پاک	شناسه دنباله پاک	دنباله مبهم	شناسه دنباله مبهم	تعداد اثرگذاری	سطح مبهم‌سازی	لگاریتم سطح مبهم‌سازی
۱	A_2^1	۱۹	A_8^1	۲۰	۱/۱	۱/۲۰	-۱/۳
۲	A_4^1	۲۲	$A`_4^1$	۴۱۶	۳/۷	۳/۱۴۰	-۱/۶۷
۳	A_6^1	۶	$A`_6^1$	۹۰	۲/۳	۲/۶۰	-۱/۴۷
۴	A_8^1	۶۸	$A`_8^1$	۹۸	۱/۳	۱/۶۰	-۱/۷۷
۵	B_2^2	۱۳	$B`_2^2$	۴۱۶	۲/۷	۲/۱۴۰	-۱/۸۴
۶	B_4^2	۱۱	$B`_4^2$	۲۲	۲/۳	۲/۶۰	-۱/۴۷
۷	B_6^2	۱۵۹	$B`_6^2$	۲۱	۱/۱	۱/۲۰	-۱/۳
۸	B_8^2	۱۸	$B`_8^2$	۱	۱/۱	۱/۲۰	-۱/۳
۹	C_2^3	۱۴	$C`_2^3$	۸	۳/۴	۳/۸۰	-۱/۴۲
۱۰	C_4^3	۴۱۶	$C`_4^3$	۲۲	۲/۳	۲/۶۰	-۱/۴۷
۱۱	C_6^3	۹	$C`_6^3$	۶	۳/۳	۳/۶۰	-۱/۳
۱۲	C_8^3	۱۰	$C`_8^3$	۲۱	۲/۳	۲/۶۰	-۱/۴۷
۱۳	D_2^4	۴	$D`_2^4$	۱۹	۱/۴	۱/۸۰	-۱/۹
۱۴	D_4^4	۵	$D`_4^4$	۲۲	۱/۳	۱/۶۰	-۱/۷۷
۱۵	D_6^4	۱۰	$D`_6^4$	۱۵۱	۱/۱	۱/۲۰	-۱/۳
۱۶	D_8^4	۱۰	$D`_8^4$	۱۴	۱/۴	۱/۸۰	-۱/۹
۱۷	E_2^5	۶	$E`_2^5$	۱۴۸	۱/۱	۱/۲۰	-۱/۳
۱۸	E_4^5	۱۴	$E`_4^5$	۴۱۶	۴/۶	۴/۱۲۰	-۱/۴۷
۱۹	E_6^5	۱۹	$E`_6^5$	۱۷۳	۲/۷	۲/۱۴۰	-۱/۸۴
۲۰	E_8^5	۱۷	$E`_8^5$	۱۸	۲/۲	۲/۴۰	-۱/۳

نمودار شکل (۴) شش مدل مختلف از طبقه‌بندی تشخیص حملات را با همدیگر مقایسه کرده است. در یک طبقه مبهم‌سازی صورت نگرفته (حمله پاک) و در شکل (۵) مدل دیگر مبهم‌سازی جایگزین حمله انجام شده است. طبق مدل پیشنهادی بدون هیچ پیش فرضی روی درصد مبهم‌سازی ماتریس OPPM و تنها با استفاده از اشتراک رفتاری در تأثیرات گذاشته شده روی هدف، انجام شده را نشان می‌دهد، نتایج آن در ادامه بیان گردیده است.

در دنباله حمله پاک، طبقه‌بندی حملات سایبری به‌خوبی انجام شده است. در تمام شناسه‌های حملات مبهم‌سازی با وجود اختلاف زیاد با غیرمبهم‌سازی، تفاوتی بین گروه‌ها وجود ندارد و این تعداد اقدام اثرگذار حمله است که در وزن احتمالاتی در ماتریس OPPM مؤثر است و به عبارتی سطح مبهم‌سازی را تعیین می‌کند. بنابراین، در هر مرحله از مبهم‌سازی حمله هرچه اثرپذیری به عدد یک نزدیک‌تر باشد مهاجم موفق‌تر عمل کرده است و هرچه اثرپذیری به عدد صفر نزدیک‌تر باشد مدافع بهتر عمل کرده است و به‌عبارت‌دیگر، با افزایش سطح مبهم‌سازی احتمال شناسایی حمله مبهم Y از روی X کاهش پیدا خواهد کرد. در نمودار شکل (۶) حملات $[E_2^5, D_6^4, C_6^3, B_8^2, B_6^2, A_2^1]$ بیشترین احتمال مبهم‌سازی یعنی ۱۰۰ درصد انجام شده است و حملات $[D_4^4, A_8^1]$ کمترین وزن احتمالاتی (۳۳٪) در ماتریس OPPM است، در نتیجه تشخیص دنباله حمله اصلی از دنباله حمله مبهم برای تحلیل‌گر شبکه آسان‌تر می‌شود.



شکل (۴): مقایسه سطح مبهم‌سازی روی حملات مختلف.



شکل (۶): مقایسه دقت طبقه‌بندی مدل پیشنهادی برای طول‌های مختلف.

۴-۵- تحلیل نتایج ارزیابی

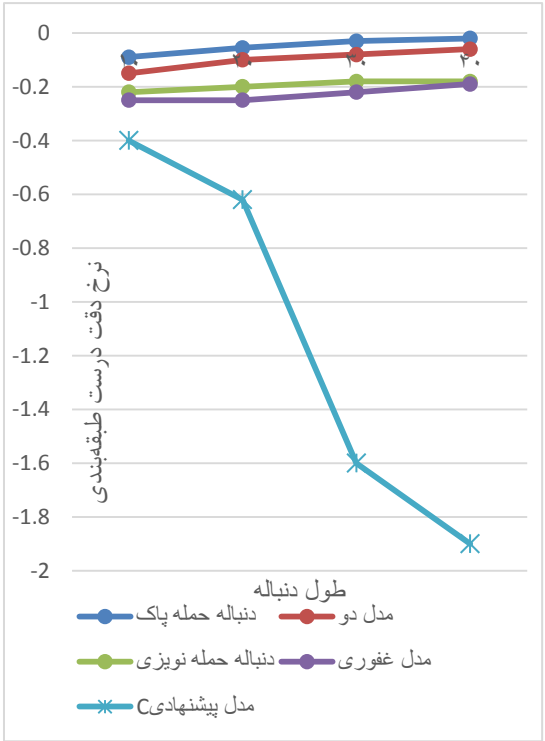
مدل ارائه‌شده، از روش مدل‌سازی احتمالاتی مورد ارزیابی و بررسی قرار گرفت و نتایج در ادامه بیان می‌گردد.

مبهم‌سازی حمله مدل پیشنهادی برای ۵ گروه با سایر مدل‌ها طبق رابطه (۱۷) نشان داده شده است:

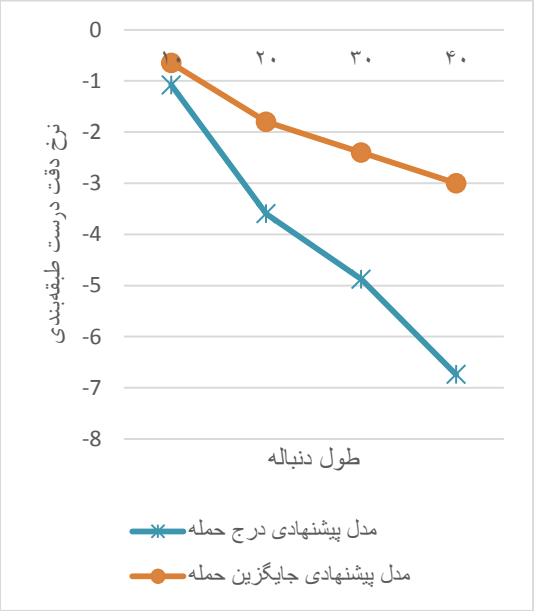
$$\left\{ A> \ E >B >D> C \ > \right\} \text{ پاک} > \text{ دو} > \text{ نویزی} > \text{ غفوری} \quad (۱۷)$$

همان‌طور که در شکل‌های (۵) و (۶) ملاحظه می‌شود مدل پیشنهادی حمله متناظر کارایی بسیار بهتری نسبت به مدل دو [۱۲] و مدل غفوری [۱۰] دارد اگرچه در طول‌های ۱۰ تا ۲۰ بین ۵ گروه مدل پیشنهادی تفاوت‌هایی وجود دارد، ولی در طول دنباله ۳۰ تا ۴۰ این اختلاف کمتر شده و از ۴۰ به بعد تمامی گروه‌ها به صفر نزدیک می‌شوند و افزایش طول دنباله حمله نه‌تنها باعث افزایش تشخیص دقت طبقه‌بندی نمی‌شود بلکه باعث کاهش تشخیص دقت طبقه‌بندی نیز می‌گردد.

در ادامه فن جایگزین حمله را با فن افزودن حمله بیان شده در مرجع [۱۹] مقایسه شده و نمودار شکل (۷) به‌دست می‌آید.



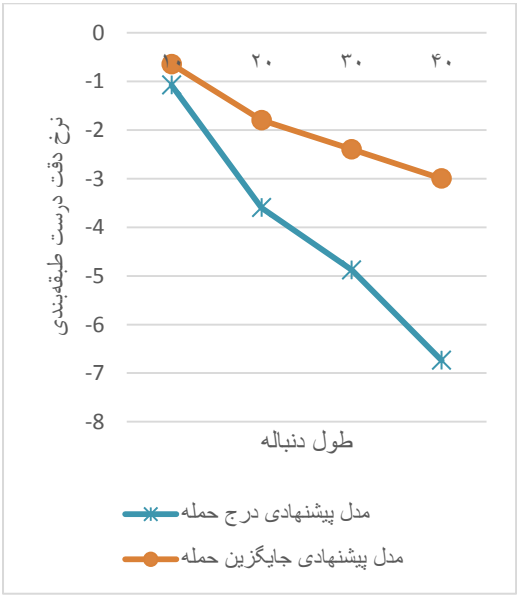
شکل (۵): مقایسه دقت طبقه‌بندی مدل حمله پیشنهادی.



شکل (۷): مقایسه دقت طبقه‌بندی در دو مدل حمله.

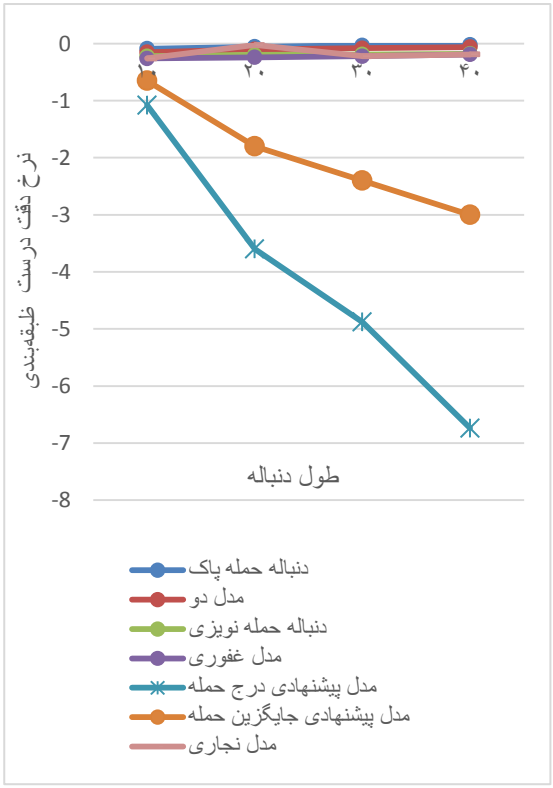
ملاحظه می‌شود که نرخ دقت درست طبقه‌بندی با طول دنباله حمله ۴۰ برای مبهم‌سازی با فن افزودن حمله ۶/۷۴-(برحسب لگاریتم) است و با فن جایگزین حمله با همین طول حمله برابر ۳- است. بنابراین، فن افزودن حمله توانمندی بیشتری در ایجاد عدم قطعیت در تشخیص حملات و کاهش نرخ طبقه‌بندی درست دارد. مبهم‌سازی حمله برای دو فن مذکور طبق رابطه (۱۸) نشان داده‌شده است:

فن جایگزین حمله < فن اضافه حمله (۱۸)



شکل (۷): مقایسه دقت طبقه‌بندی در دو مدل حمله.

جهت ارزیابی مدل پیشنهادی، طبق نمودار شکل (۸) ملاحظه می‌گردد، مدل دو [۱۲]، مدل‌های ارائه‌شده توسط نجاری [۹] و غفوری [۱۰] خیلی شبیه هم هستند و نرخ دقت درست طبقه‌بندی دنباله حمله برای مدافعین شبکه تقریباً به یک اندازه است ولی اگر مهاجم از مدل حمله متناظر پیشنهادی استفاده کند، کار برای سامانه‌های تشخیص نفوذ بسیار سخت خواهد شد و دقت درست طبقه‌بندی دنباله حملات برای تحلیل‌گر شبکه کاهش می‌یابد.



شکل (۸): مقایسه دقت طبقه‌بندی حمله متناظر پیشنهادی.

۵. نتیجه‌گیری

فّن جایگزین حمله با کاهش نرخ طبقه بندی درست در دنباله حملات می‌تواند مدافعین امنیت شبکه را فریب دهد و به‌خاطر وسعت و دامنه اجرا، مبهم‌سازی را برای مهاجم ساده و تشخیص حملات را برای مدافعین بسیار سخت خواهد کرد. درصورت به‌کارگیری ترکیبی این فن با سایر فنون مبهم‌سازی (اضافه حمله و حذف حمله) در دنباله حملات، تشخیص حملات سایبری سخت‌تر خواهد شد. با بررسی مدل طبقه‌بندی اقدامات حمله این نتیجه حاصل می‌شود که الگوهای مختلف اقدامات حمله درعین‌حال که هشدارهای مختلفی در IDS تولید می‌کنند، می‌توانند آسیب‌پذیری‌های یکسانی داشته باشند،

همچنین الگوهایی که از آسیب‌پذیری‌های مشابهی تبعیت می‌کنند نیز دارای گام‌هایی از حمله هستند که در بین روش‌های به‌کار رفته در آن‌ها اشتراک وجود دارد.

۶. منابع

[1] A.Kott, C.Wang, and R.F.Erbacher,"Cyber defense and situational awareness", vol.62.Springer,2015.

[2] Veeraswamy, A., S. Appavu, and E. Kannan, "An Implementation of Efficient Datamining Classification Algorithm using Nbtree", International Journal of Computer Applications, 2013.

[3] F.Valeur, et al., "Comprehensive approach to intrusion detection alert correlation", IEEE Transactions on dependable and secure computing, 2004. p. 146-169.

[4] S. Ruggieri, "Efficient C4. 5 [classification algorithm]. transactions on knowledge and data engineering", IEEE 2002. 14(2): p. 438-444.

[5] A.Kott, C. Wang, and R.F. Erbacher, "Cyber defense and situational awareness". Vol. 62. 2015: Springer.

[6] H.Du, and S.J. Yang. "Probabilistic inference for obfuscated network attack sequences", Annual IEEE/IFIP International Conference on Dependable Systems and Networks. 2014.

[7] H. Debar and M. Dacier, "Towards a taxonomy of intrusion-detection systems," Computer Networks, vol. 31, no. 8, pp. 805 – 822, 1999.

[8] S.Parsa,H.salehi,M.H.Alaeiyan,"Code Obfuscation to Prevent Symbolic Execution", Journal of Electoronic & Cyber defence, Imam Hossein Comprhensive Univercity, Vol. 6,No. 1, 2018 (in persian).

[9] M.H.Najari," The design and simulation of an efficient algorithm for modeling the obfuscation of cyber attacks based on action insertion", M.Sc, Malek-e-Ashtar University, 2017 (in persian).

[10] N.Ghafori," The design and simulation of an efficient algorithm for modeling the obfuscation of cyber attacks based on action alteration", M.Sc, Malek-e-Ashtar University, 2017 (in persian).

[11] R. Aliabadi," The design and simulation of an efficient algorithm for modeling the obfuscation of cyber attacks based on action removal", M.Sc, Malek-e-Ashtar University, 2017 (in persian).

[12] H.Du, "Probabilistic Modeling and Inference for Obfuscated Network Attack Sequences", PhD diss, Rochester, New York, 8-2014.

[13] L.Wang, A. Liu, and S. Jajodia, "Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts," Comput. Commun, vol. 29, no. 15, pp. 2917–2933, 2006.

[14] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," presented at the Proceedings of the 1998 workshop on new security paradigms, pp. 71–79,1998.

[15] T. Tidwell, R. Larson, K. Fitch, and J. Hale, "Modeling internet attacks," presented at the Proceedings of the IEEE Workshop on Information Assurance and security, vol. 59, 2001.

[16] K. Daley, R. Larson, and J. Dawkins, "A structural framework for modeling multi-stage network attacks," presented at the Parallel Processing Workshops, Proceedings. International Conference on, pp. 5–10, 2002.

[17] S. Noel and S. Jajodia, "Advanced vulnerability analysis and intrusion detection through predictive attack graphs," Crit. Issues C4I Armed Forces Commun. Electron. Assoc. AFCEA Solut. Ser. Int. J. Command Control, 2009.

[18] Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description, 2019.

[19] K.Shoushian,A.J.Rashidi,M.Dehghani," Modeling of cyber attacks obfuscation based insertion technique of attack", Journal of Electoronic & Cyber defence, Imam Hossein Comprhensive Univercity(printing) (in persian).

Journal of Electronical & Cyber Defence
Vol. 8, No. 1, 2020, Serial No. 29

Modeling of Cyber-Attacks Obfuscation, Based on Alteration Technique of Attack

K. Shoushian, A. J. Rashidi, M. Dehghani

*Imam Hossein Comprehensive University

(Received: 02/05/2018, Accepted: 05/03/2019)

ABSTRACT

With the increasing rate of cyber-attacks, creating security for cyberspace has become more important and crucial. Therefore computers, computer networks and all current systems connected to the Internet are always at risk of cyber-attacks. In this paper, a novel technique based on alteration technique of attack is proposed by providing a new classification in the methods of obfuscation. In this method, by replacing the attacks that have similar characteristics in the attack strategies the attacker causes an increase in wrong classification and thus reduces the dependence between attack steps. Therefore, by increasing the length of the attack, network security managers cannot easily distinguish cyber-attacks. The proposed model was assessed based on the Bayesian algorithm. The results of the research and implementation of the model indicate that the accuracy of classification (in terms of log) by intrusion detection systems for the best case of clean attacks in the sequel of attack, is -0.02 and for obfuscation attacks at the action level is -0.19. For obfuscate attacks with the alternative technique it becomes -3 and for the insertion technique it decreases to -6.74. In the proposed model, as in the obfuscation-based insertion technique, the corresponding attack method has been used. Due to the difference in the type of ambiguity model, different results are obtained, and the combination of these two obfuscating techniques in cyber-attacks can bring better results to the attacker in deceiving the intrusion detection systems and creating uncertainties in the sequence of observed attacks.

Keywords: Modeling of cyber-attacks, attacks obfuscation, alteration attack, sequel attack

* Corresponding Author Email: K.shoushian@chmail.ir