نشریه علمی "پدافند الکترونیکی و سایبری"
سال هفتم، شماره ۴، زمستان ۱۳۹۸، ص ۱۰۳-۹۱

مدل‌سازی حملات سایبری مبهم مبتنی بر حمله متناظر با فن افزودن حمله

کیانوش شوشیان[۱]، علی جبار رشیدی[۲*]، مهدی دهقانی[۳]
۱- دانشجوی دکتری، دانشگاه جامع امام حسین(ع)، ۲- استادیار، دانشگاه صنعتی مالک اشتر، ۳- استادیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۷/۰۹/۱۰، پذیرش: ۹۷/۱۲/۱۴)

چکیده

یکی از تهدیدات مهم سال‌های اخیر در حوزه سامانه‌های رایانه‌ای و فضای سایبر، حملات سایبری مبهم است. مبهم‌سازی در سطح حمله به معنای تغییر حمله، بدون تغییر در رفتار و تغییر در نوع اثرگذاری حمله بر قربانی است. در این مقاله با ارائه طبقه‌بندی جدیدی در روش‌های مبهم‌سازی، برای مدل‌سازی حملات سایبری مبهم، روشی مبتنی بر فن افزودن حمله پیشنهاد شده است. مهاجم در این روش با افزایش دسته‌بندی غلط در راهبردهای حمله، باعث جدا شدن وابستگی میان هشدارها و اقدامات حمله می‌شود؛ بنابراین، با افزایش طول دنباله حمله، مدیران امنیت شبکه به‌راحتی نمی‌توانند حملات سایبری را تشخیص دهند. مدل پیشنهادی بر اساس الگوریتم بیزین ارزیابی شد. جداول و نمودارهای ارزیابی، نشان‌دهنده تدوین مناسب ساز و کار ارائه‌شده برای دنباله حملات مبهم بوده به‌طوری‌که احتمال تشخیص حملات مبهم نسبت به حملات پاک بسیار کم‌تر می‌باشد. با افزایش دنباله حملات دقت طبقه‌بندی درست، به صفر میل می‌کند. روش پیشنهادی برای مبهم‌سازی حملات، به دلیل توانایی در فریب سامانه‌های تشخیص نفوذ و ایجاد عدم قطعیت در دنباله حملات مشاهده‌شده، کارایی بیشتری نسبت به منطق مبهم‌سازی در سطح کد و اقدام دارد.

کلیدواژه‌ها: سامانه‌های تشخیص نفوذ، مبهم‌سازی حمله، افزودن حمله، حمله متناظر

۱. مقدمه

امروزه با توجه به گسترش استفاده از رایانه‌ها و فضای سایبری و به تبع آن افزایش چشم‌گیر خطرات موجود در این فضا، نیاز زیادی به کسب دانش در این محیط‌ها احساس می‌شود. نسل جدید شبکه‌های سایبری به الگوریتم‌ها و روش‌های جدیدی نیاز دارند و باید از مواردی نظیر آگاهی وضعیتی سایبری، ارزیابی اثر مبتنی بر گره و واکنش خودکار و پویا به حملات (مانند پیکربندی مجدد، ترمیم و بازسازی) پشتیبانی نمایند. تمامی موارد ذکرشده، تداوم عملکرد در سیستم‌هایی که مأموریت حیاتی دارند را فراهم می‌کنند. حملات سایبری می‌توانند پیامدهای ناگواری را در شبکه‌های نظامی و همچنین زیرساخت‌های شبکه‌ای ملی ایجاد کنند. همچنین یکی از راه‌کارهای بازدارندگی مهاجمین می‌تواند دفاع پیش‌کنش‌گرانه فعال و هوشمند باشد که باید تحقیقات به‌عمل‌آمده از شناسایی و تشخیص فن‌های نوظهور در حملات سایبری، پشتیبانی نماید.

لفظ مبهم‌سازی[۱] از مخفی‌کاری و تاریکی و تیرگی گرفته شده است. در حملات سایبری از اصطلاح مبهم‌سازی برای پنهان کردن اطلاعات مهم در حمله صورت گرفته، استفاده می‌شود. مبهم‌سازی، ساز و کاری برای پنهان‌سازی الگوریتم اصلی است. به عبارت دیگر تغییر ظاهر برنامه بدون تغییر عملکرد آن است، به‌گونه‌ای که شناسایی حملات توسط سیستم‌های تشخیص نفوذ در عمل سخت و یا غیر ممکن است [۱].

مبهم‌سازی، روشی است که باعث درک سخت‌تری از برنامه یا حمله می‌شود. به عبارت دیگر ساز و کار حمله به شکستن ماشین تطبیق الگو و یا ایجاد فریب در سیستم تشخیص نفوذ است، که منجر به عدم شناسایی و یا سخت‌تر شدن حملات سایبری می‌شود [۲].

مبهم‌سازی در چهار سطح بسته[۲]، کد[۳]، اقدام[۴] و حمله قابل اجرا است. لازم به ذکر است انواع تعاریف مختلف برای مبهم‌سازی وجود دارد که نتایج همه آن‌ها معنی «درک سخت‌تر مسئله برای مدیر امنیت شبکه» است.

- **مبهم‌سازی در سطح بسته**

مبهم‌سازی در سطح بسته ارسالی بین فرستنده و گیرنده از دانش مدل پروتکل TCP/IP برای اجرای عملکردهای فریب‌کارانه و یا

* رایانامه نویسنده مسئول: rashidi@mut.ac.ir

[1] Obfuscation
[2] Packet-level
[3] Code-level
[4] Action-level

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. علاوه بر این میزبان‌های تسخیرشده بیشتر و بیشتری به‌عنوان سنگ پله[1] استفاده می‌شوند تا حملات سطح بالاتری را ایجاد کنند. شکل (۱) نمونه‌ای از قوانین اسنورت[2] را بر روی آسیب‌پذیری RPC Sadmind نشان می‌دهد. جدول (۱) پی‌آیندی[3] است تا بتواند از آسیب‌پذیری موجود سوءاستفاده کند و این‌که کد هگز نشان داده‌شده در شکل (۱) را توصیف می‌کند. 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 پورت باز ساخته شد، بارگیری پی‌آیند ساخته‌شده، هشداری را ایجاد خواهد کرد و سبب تزریق یک مشاهده نویزی می‌گردد [۳].

```
alert tcp $EXTERNAL_NET any -> $HOME_NET
1024:(msg:"RPC sadmind query with root
credentials attempt TCP"; flow:to_server
established; content:"|00 01 87 88|";
depth:4; offset:16; content:"|00 00 00
01 00 00 00 01|"; within:8; distance:4;
byte_jump:4,8,relative,align; content:
"|00 00 00 00|"; within:4; metadata:
policy security-ips drop; classtype:
misc-attack; sid:2255; rev:10;)
```

شکل (۱): مثالی از قانون RPC Sadmind Snort

جدول (۱): پی‌آیند هگز و توضیحی برای RPC Sadmind Snort [۳]

کد هگز	توضیح
00 89 9c e2	the request id, a random uint32
00 00 00 00	rpc type (call = 0, response = 1)
00 00 00 02	rpc version (2)
00 01 87 88	rpc program (0x00018788 = sadmind)
00 00 00 0a	rpc program version (0x0000000A = 10)
00 00 00 01	rpc procedure (0x00000001 = 1)
00 00 00 01	credential flavor (1 = auth unix)

- **مبهم‌سازی در سطح کد**

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. به این کد اجرایی یا باینری، از آن‌جا که تعداد دستورات محدودی دارد و بر روی زبان ماشین مقصد ترجمه می‌شود برای مقاصد تحلیل مناسب و سریع هستند. مبهم‌سازی در این سطح متشکل از تبدیل و دگرگون‌سازی کد است که در عین حفظ شدن ویژگی‌های اصلی با تغییر در ساختار خود، درک برنامه را برای تحلیل‌گر دشوار می‌نماید. در این روش دنباله کد اصلی بدافزار با قطعه داده‌ای، شامل دنباله کدی که فشرده و رمز شده است، جایگزین می‌شود. یک روال بازکننده که دنباله کد اصلی را، در زمان اجرا، از قطعه داده جایگزین شده بازیابی می‌کند، نیز در این بسته قرار دارد. نتیجه حاصل از این روش مبهم‌سازی، برنامه خود تولید است. برنامه خود تولید، برنامه‌ای است که به‌طور خودکار کدی را در حافظه تولید و سپس آن را اجرا می‌کند [۴].

- **مبهم‌سازی در سطح اقدام**

مبهم‌سازی در سطح اقدام به معنی انجام فنونی در اجرای اقدامات و فعالیت‌های مقدماتی حمله است به‌نحوی‌که سیستم‌های تشخیص نفوذ عملکرد صحیحی دارند و هشدارهای مناسب می‌دهند ولی چون اقدامات مهاجم تغییر کرده است، مدیران امنیت شبکه فریب‌خورده و حمله واقعی را تشخیص نمی‌دهند. مهاجم در این روش‌ها از چندین اقدام پایه‌ای استفاده می‌کند تا به فریب دادن مدیران امنیتی دست یابد. فنون مبهم‌سازی در برگیرنده راه‌کارهایی همچون تغییر اقدام، افزودن اقدام و حذف اقدام است [۵].

با بهره‌گیری از میزبان‌های تسخیرشده (آسیب‌دیده) مهاجم به آسانی می‌تواند اقدامات مهم‌تر خود را پنهان کند و یا اقدامات بی ربطی را به‌منظور گیج کردن تحلیل‌گران تزریق کند، به‌گونه‌ای که تعداد زیادی از اقدامات از منابع مختلف ناشی می‌شوند. همچنین برای مهاجمان تزریق اقدامات حمله نویزی امکان‌پذیر است؛ چرا که امضاهای مخرّب به‌صورت عمومی قابل دسترس 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. به عبارت دیگر می‌توان مبهم‌سازی را این‌طور تعریف کرد که: مبهم‌سازی روشی است که باعث درک سخت‌تری از برنامه یا حمله (بسته به کاربرد آن) می‌شود. برای این منظور، یک برنامه یا حمله را به یک نسخه جدید حمله تبدیل می‌کند درحالی‌که آنها را به‌طور عملی با یکدیگر برابر می‌کند.

[1] Stepping Stones
[2] Snort
[3] Payload

✓ **تغییر اقدام**[1]

برای موتور تشخیص مبتنی بر امضاء، تغییر پی‌آیند و ساختن امضایی برای هشدارهای از قبل تعیین‌شده می‌تواند به آسانی صورت گیرد. از این‌رو، مهاجم امکان تغییر در هشدارها را دارد تا مبدأ صحیح حمله یا مشخصه حمله را پنهان سازد. به‌علاوه گاهی اوقات برای رسیدن به همان هدف مورد شناسایی یا مورد نفوذ، بسیاری از اقدامات قابل تعویض می‌باشند. تغییر ترتیب اقدامات حمله می‌تواند دنباله معادل دیگری بسازد که کل دنباله را تطبیق‌پذیرتر کرده و با تطبیق کردن با الگوی دنباله نفوذ کلاسیکی از شناسایی شدن جلوگیری شود [۵].

✓ **افزودن اقدام**[2]

یکی از روش‌هایی که تأثیر زیادی در به‌وجود آوردن عملکرد غلط و گمراه کردن موتورهای تحلیل هشدار وجود دارد، افزودن اقدام است این روش مهاجم با افزایش دسته‌بندی غلط در راهبردهای حمله، باعث جدا شدن وابستگی میان هشدارها می‌شود.

این تأثیرات می‌تواند شامل موارد زیر باشد:

- افزایش میزان دسته‌بندی غلط راهبرد حمله که باعث جدا شدن وابستگی میان هشدارها می‌شود.
- سرازیر شدن تقاضاهای زیاد به موتورهای تحلیل هشدار[3] به این دلیل که ظرفیت تمامی موتورهای تحلیل محدود است [۵].

✓ **حذف اقدام**[4]

در این روش مهاجم سعی دارد هشداری که نشان‌دهنده چگونگی نفوذ است را با حذف کردن برخی از اقدامات غیر ضروری مخفی کند.

- **مبهم‌سازی در سطح حمله**

مبهم‌سازی در سطح حمله به معنی انجام فنونی در اجرای حملات است به نحوی که سیستم‌های تشخیص نفوذ عملکرد صحیحی دارند و هشدارها را به‌درستی تشخیص می‌دهند، ولی چون نوع حمله مهاجم تغییر کرده است، مدیران امنیت شبکه فریب‌خورده و حمله واقعی را تشخیص نمی‌دهند. مهاجم در این روش ممکن است از چندین اقدام پایه‌ای نیز استفاده کند تا به فریب دادن مدیران امنیتی دست یابد. فنون مبهم‌سازی در این روش نیز مانند مبهم‌سازی در سطح اقدام است با این تفاوت که به‌جای مبهم کردن اقدامات و فعالیت‌ها، این حملات هستند که مبهم می‌شوند. این مقاله در نظر دارد مفهوم مبهم‌سازی در سطح حمله را برای اولین بار تبیین نماید.

بخش‌های بعدی این مقاله به‌صورت زیر خواهند بود. در بخش دوم کارهای مرتبط بیان می‌شود. در بخش سوم فضای اقدامات حملات سایبری که سبب طبقه‌بندی اقدامات حمله در گروه‌های مختلف شده است، توضیح داده می‌شود. بخش چهارم به مدل پیشنهادی اختصاص داده شده است. بخش پنجم را به روش اجرا و نتایج حاصل از مدل توضیح داده می‌شود و در نهایت در بخش ششم مدل پیشنهادی مورد ارزیابی قرار می‌گیرد و در بخش هفتم و نهایی نتایج به‌دست‌آمده از مبهم‌سازی مورد تحلیل قرار می‌گیرد.

۲. کارهای مرتبط

نجاری [۶] مبهم‌سازی حملات را برای فن افزودن اقدام تحلیل کرده است و ضمن تشکیل پایگاه داده‌های هم‌گروه، الگوریتمی برای تولید دنباله‌های حملات مبهم ارائه داده است و سپس روش خود را از منظر میزان نویز تزریقی و طول دنباله مورد ارزیابی قرار داد.

غفوری [۷] با توجه به داده‌های ماتریس OPPM[5] پیشنهادی، توانست الگوریتم مبهم‌ساز حمله مبتنی‌بر جایگزینی اقدام را طراحی کند و به تولید دنباله حمله دست یابد. سپس رفتار دنباله‌های حملات مختلف را 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 باشد و در ادامه تحقیق خود، دنباله‌های مختلف به‌دست‌آمده از الگوریتم مبهم‌سازی خود را طبقه‌بندی کرده و چالش‌های مربوط به دقت 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 انجام‌گرفته، بهبود بخشید.

علی آبادی [۸] 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

[1] Action Alternation
[2] Action insertion
[3] Denial of service (DOS)
[4] Action removal
[5] Obuscation Possible Probability Matrix

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.

هایتو دو [۵] 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 به دست آورد. یک دنباله حمله به‌صورت شکل‌گرا[1] را به‌عنوان بردار متغیرهای تصادفی توصیف‌شده در نظر گرفت و هر مشاهده را یک نمونه از مدل‌های حمله به شمار آورد. در نهایت به‌منظور نمایش میزان تأثیر دنباله حمله‌های مبهم و پاک، یک شبیه‌سازی ارائه کرد.

وانگ و همکارانش [۹] بحث استفاده از گراف حمله را جهت همبسته‌سازی، فرضیه‌سازی و پیش‌بینی هشدارهای نفوذ مدل کردند. ایده اصلی در گراف حمله ارائه یک نمایش کارا و ابزارهای الگوریتمی جهت شناسایی آسیب‌پذیری‌های سیستمی است؛ که احتمال دارد مورد بهره‌برداری مهاجم قرار گیرد. این رویکرد به شدت به دانش صحیح و کافی از آسیب‌پذیری‌های سیستم و قواعد دیوار آتش در شبکه وابسته است. با وجودی که هکرها ابزارهای زیادی جهت اسکن کردن شبکه را به‌منظور دریافت اطلاعات در اختیار دارند، ولی در شبکه‌های تجاری بزرگ با چندین سیستم مدیریتی که هر سیستم بخش‌های مختلفی از شبکه را مدیریت می‌کند، ناکارآمد است. باید توجه داشت که نمایش آسیب‌پذیری‌ها در شبکه توسط محققان دیگر در اواخر دهه ۹۰ و اوایل ۲۰۰۰ (بری مثال فیلیپس و اسویلر[2] [۱۰]، تیدول[3] و همکارانش [۱۱]، دالی[4] و همکارانش [۱۲]. 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 [۹] و نوئل و جاجودیا در [۱۳] 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 کارائی بهتر روش پیشنهادی (مبهم‌سازی در سطح حمله) را نشان خواهیم داد. همچنین در تحقیقات مورد اشاره با افزایش طول دنباله حمله، طبقه‌بندی هشدارها برای سیستم‌های تشخیص نفوذ آسان شده و حملات قابل تشخیص هستند. لازم به ذکر است؛ مهاجم هرچه بیشتر بتواند، همبستگی حملات را کاهش دهد، مدیران شبکه کمتر می‌توانند رد حملات را کشف کنند.

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 انجام شده است. در این راستا فهرست‌های متعددی نیز تهیه شده‌اند 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[5] پروژه امنیت برنامه‌های وب باز[6]، شمارش و طبقه‌بندی الگوهای حمله رایج (کیپک)[7] و شمارش ضعف‌های رایج[8]. در این تحقیق، مبهم‌سازی حملات سایبری بر اساس دسته‌بندی‌های مربوط به شرکت میتره[9] به نام کیپک شکل گرفته 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. بر اساس این استاندارد الگوی حملات سایبری را می‌توان بر دو محور مکانیسم و دامنه طبقه‌بندی کرد. در محور مکانیسم داریم:

$$\text{Mechanisms} = < \text{Category 1}, \ldots, \text{Category 9} > \quad (۱)$$

$$C = < \text{Meta 1}, \text{Meta 2} \ldots \text{Meta n} > \quad (۲)$$

روابط (۱ و ۲) بیان می‌دارد، سازوکار حملات سایبری به ۹ گروه با ویژگی‌ها و اهداف مختلف مطابق جدول (۲) دسته‌بندی[10] شده‌اند. و هر دسته‌بندی شامل تعدادی حمله سطح بالای متا[11] می‌باشد [۱۴].

[1] Formal
[2] Phillips & Swiler
[3] Tidwell
[4] Daley

[5] Web Application Security Consortium (WASC)
[6] OWASP
[7] Common Attack Pattern Enumeration and Classification(CAPEC)
[8] CWE
[9] MITRE
[10] Category
[11] حمله سطح متا به حملات جامع سایبری گفته می‌شود که مهاجم از یک روش یا فن خاص استفاده می کند. یک حمله متا معمولا نتیجه‌ای از یک فناوری یا عملکرد خاص به شمار می رود و به منظور بیان مفهوم یک رویکرد سطح بالا طراحی شده است.

جدول (۲): دسته‌بندی حملات سایبری [۱۸]

ردیف	دسته‌بندی حمله	شناسه
۱	مشارکت در تعاملات فریبنده[۱]	۱۵۶
۲	سوء استفاده از عملکرد موجود[۲]	۲۱۰
۳	دست‌کاری ساختار داده‌ها[۳]	۲۵۵
۴	دست‌کاری منابع سیستم[۴]	۲۶۲
۵	تزریق فایل‌های ناخواسته[۵]	۱۵۲
۶	استفاده از روش‌های احتمالی[۶]	۲۲۳
۷	دست‌کاری زمان بندی و وضعیت[۷]	۱۷۲
۸	جمع‌آوری و تحلیل اطلاعات[۸]	۱۱۸
۹	از بین بردن کنترل دسترسی[۹]	۲۲۵

برای طراحی دنباله حملات مبهم، به تولید اطلاعات نیاز است؛ لذا برای درک مسئله به یک دسته از حملات با شناسه ۱۵۶ با هدف مشارکت در تعاملات فریبنده می‌پردازیم.

هدف الگوهای حمله در این دسته‌بندی بر تعاملات مخرب است و تمرکز مهاجم برای فریب قربانی و متقاعد کردن او می‌باشد و تلاش می‌کند که با عوامل دیگری تعامل داشته باشد. مهاجم چنین اقداماتی را براساس سطح اعتماد که بین قربانی و عامل دیگر وجود دارد انجام می‌دهد. این نوع حملات به جعل محتوای و یا هویت، به‌گونه‌ای تکیه دارند که هدف، به اشتباه به مشروعیت محتوی اعتماد پیدا می‌کند. این دسته از حمله به شکل‌های زیادی در فضای سایبری به کار گرفته می‌شود که هر کدام نیاز به برخی از انواع نمایش جعلی اطلاعات و روش‌های متنوع، برای اجرای عملیات دارند. ولی طبق استاندارد مرجع تحقیق، چهار نوع از حمله متا، می‌توانند این حمله را انجام دهد که هر کدام از حملات متا خود شامل حملات دیگر است که در شکل (۲) و روابط (۳-۸) صورت کلی این حمله به همراه جزئیات حملات آورده شده است.

$$A156=A148\,(M)+A151(M)+A154(M)+A173(M)+A416(M) \quad (۳)$$

$$A148\,(M)=A145(D)+A218(D)+A502(S)+A572(D)+A627(S) \quad (۴)$$

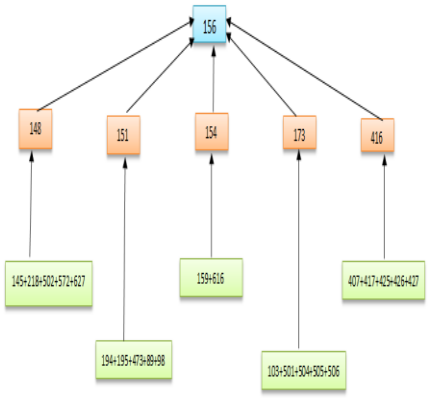
$$A151(M)=A194(S)+A195(S)+A473(S)+A89(S)+A98(S) \quad (۵)$$

$$A154(M)=A159(S)+A616(S) \quad (۶)$$

$$A173(M)=A103(S)+A501(D)+A504(D)+A505(D)+A506(S) \quad (۷)$$

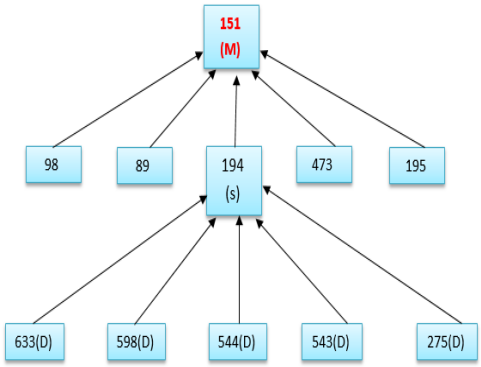
$$A416(M)=A407(S)+A417(S)+A425(S)+A426(S)+A427(S) \quad (۸)$$

[1] Engage in Deceptive Interactions
[2] Abuse Existing Functionality
[3] Manipulate Data Structures
[4] Manipulate System Resources
[5] Inject Unexpected Items
[6] Employ Probabilistic Techniques
[7] Manipulate Timing and State
[8] Collect and Analyze Information
[9] Subvert Access Control



شکل (۲): نمایش مدل حمله مشارکت در تعاملات فریبنده با شناسه حمله ۱۵۶

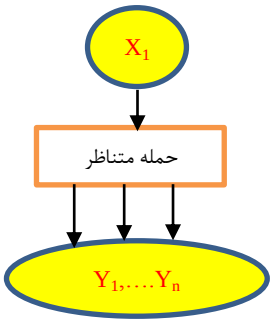
برخی از اهداف مهاجم می‌تواند در سطح پائین باشد مثلاً: سرگرمی، دزدی، انتقام و یا برخی اهداف بدخواهانه دیگر مهاجم می‌تواند در سطوح عملیاتی و راهبردی باشد و اثر این حملات می‌تواند خیلی شدید باشد و می‌تواند اثرات مخربی را بر روی یک سازمان و حتی یک کشور ایجاد کند. برای انجام یک حمله سطح بالای متا، باید تعدادی از حملات سطوح پائین‌تر استاندارد را اجرا کرد و برای اجرای حمله استاندارد باید حملات سطح پائین‌تر و اقدامات پیش‌نیاز را انجام داد. این حملات به‌صورت گراف حمله از پائین به بالا مدل‌سازی می‌شود. انجام حمله متا با شناسه ۱۵۱ مطابق شکل (۳) می‌باشد.



شکل (۳): نمایش حمله متا با شناسه ۱۵۱

۴. مدل پیشنهادی

مدل به‌کار رفته شده در این تحقیق مطابق شکل (۴)، برای مدل‌سازی احتمالاتی حملات سایبری مبهم، ارائه روش مبهم ساز حمله متناظر با فن افزودن حمله مبتنی بر تأثیر حمله خواهد بود. مدل‌های احتمالاتی مبهم، با استفاده از مفاهیم شبکه بیزین که از اقدامات حملات پاک متناظرشان پیروی می‌کنند و هم‌گروه هستند، ارائه می‌شود.



شکل (۴): مدل پیشنهادی

بر اساس مدل پیشنهادی تحقیق، مبهم‌سازی حملات بر اساس خوشه‌بندی تشابه و عدم تشابه اثرگذاری حمله و اهداف مهاجم شکل می‌گیرد. حملات با توجه به تشابه اثرگذاری‌شان بر دارائی‌های قربانی خوشه‌بندی می‌شوند. به عبارت دیگر نمونه‌های مشابه با یکدیگر در یک خوشه و نمونه‌های غیر مشابه در خوشه‌های متفاوتی گروه‌بندی می‌شوند، بنابراین، به‌منظور تشابه‌سنجی، نیاز به مقیاس یا معیار ضروری است. از آنجا که 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. مطابق جدول (۳) معیار تشابه برای داده‌ها، اثرگذاری حمله بر روی سرمایه‌ها و دارایی‌های سایبری هدف مهاجم می‌باشد. علت تکراری بودن شناسه‌ها این است که، یک شناسه حمله ممکن است چند اثرگذاری مختلف بر روی دارائی‌های قربانی ایجاد کند.

جدول (۳): خوشه‌بندی حملات سایبری مبتنی بر تأثیرات حمله (یافته‌های تحقیق)

شناسه حمله	اثرگذاری حمله	مخفف تأثیر حمله	کنترل امنیتی
۱,۳,۴,۵,۹,۱۰,۱۱,۱۲,۹۸,۱۷,۱۹,۲۱,۲۲,۱۵۱,۱۷۳,۴۱۶,۶۸,۷۰,۷۹,...	ارتقاء سطح دسترسی[۲]	GP	محرمانگی[۱]
۶,۷,۸,۹,۱۰,۱۱,۱۲,۱۳,۱۴,۱۷,۱۸,۱۹,۸۹,۱۱۸,۷۹,۱۶۹,۷۹,۲۰,۲۱,...	خواندن داده‌ها[۳]	RD	
۷,۸,۹,۱۰,۱۳,۱۴,۱۷,۱۸,۲۲,۱۷۳,۴۱۶,۷۹,۴۴,...	اجرای فرمان‌های غیر مجاز[۴]	EUC	
۱۳,۱۷۳,۴۱۶,۷۹,۹۶,۱۰۰,۳۲۰,۳۲۵,۳۳۰,۹۰,...	سازوکار دور زدن سامانه‌های حفاظتی[۵]	BPM	
۳۲۵,۳۳۰	مخفی کردن فعالیت‌ها	RC	
۱,۴,۵,۶,۹,۱۰,۱۱,۱۲,۱۶,۱۷,۱۹,۲۱,۲۲,۱۵۱,۴۷۳,۹۸,۷۰,۹۰,...	ارتقاء سطح دسترسی	GP	کنترل دسترسی[۶]
۱۳,۱۵۹,۹۶,۱۰۰,۳۲۰,۳۲۵,۳۳۰,۹۰,...	سازوکار دور زدن سامانه‌های حفاظتی	BPM	
۳۱۲,۳۰۰,۳۲۵,۳۳۰,...	مخفی کردن فعالیت‌ها[۷]	HA	
۲,۵,۱۴,۱۷۳,۴۱۶,...	مصرف منابع[۹]	RC	دسترسی‌پذیری[۸]
۷,۸,۹,۱۰,۱۳,۱۴,۱۷,۱۸,۱۹,۲۲,۱۷۳,۴۱۶,۷۹,۴۴,...	اجرای فرمان‌های غیر مجاز[۱۰]	EUC	
۸,۹,۱۰,۱۳,۱۷۳,۴۱۶,۴۴,...	اجرای دستورات غیر قابل اطمینان[۱۱]	UE	
۱,۳,۴,۵,۹,۱۰,۱۱,۱۲,۱۶,۱۷,۱۹,۲۱,۲۲,۱۵۱,۹۸,۶۸,۷۰,۹۰,...	ارتقاء سطح دسترسی	GP	احراز هویت[۱۲]
۱۳,۹۶,۱۰۰,۳۲۰,۳۲۵,۳۳۰,۹۰,...	سازوکار دور زدن سامانه‌های حفاظتی	BPM	
۱۵۴,۱۵۹,...	اجرای فرمان‌های غیر مجاز	EUC	
۳۱۲,۳۲۵,۳۳۰,...	مخفی کردن فعالیت‌ها	HA	
۳,۶,۸,۹,۱۰,۱۴,۱۷,۱۹,۲۱,۱۴۸,۱۷۳,۴۱۶,۱۴۸,۶۲۷,۹۸,...	دست‌کاری اطلاعات	MD	یکپارچگی[۱۳]
۷,۸,۹,۱۰,۱۳,۱۴,۱۷,۱۸,۲۲,۱۷۳,۴۱۶,۷۹,۴۴,..	اجرای فرمان‌های غیر مجاز	EUC	
۱۵۱,۱۷۳,۴۱۶,۱۹۴,۶۳۳,...	ارتقاء سطح دسترسی	GP	
۱۹۴,۶۳۳,...	تغییر منطق اجرایی	AEL	
۱۹۴,۶۳۳,...	مخفی کردن فعالیت‌ها	HA	

[1] Confidentiality
[2] Gain Privileges
[3] Read Data
[4] Execute Unauthorized Commands
[5] Bypass Protection Mechanism
[6] Access Control
[7] Hide Activities
[8] Availability
[9] Resource Consumption
[10] Unreliable Execution
[11] Unreliable Execution
[12] Authorization
[13] Integrity

برای مبهم‌سازی حملات به گروه‌بندی کردن فضای اقدامات حمله مطابق جدول (۴) نیاز داریم لذا با استفاده از اطلاعات سایت امنیتی کیپک و به‌صورت دستی این کار انجام می‌گردد.

جدول (۴): گروه‌بندی فضای برخی از اقدامات حمله (یافته‌های تحقیق)

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

۵. روش اجرا

یکی از روش‌هایی که تأثیر زیادی در به‌وجود آوردن عملکرد غلط و گمراه کردن موتورهای تحلیل هشدار وجود دارد، افزودن حمله است. افزایش دسته‌بندی غلط در راهبردهای حمله توسط مهاجم باعث جدا شدن وابستگی میان هشدارها و اقدامات حمله می‌شود. برخی از روش‌های انجام فن افزودن حمله به شرح زیر است:

ایجاد نفوذ اضافی در میان حملات (ایجاد اقدام‌های اضافی)، می‌توانند از فعالیت‌های نفوذی مثل دست‌کاری اطلاعات و یا اجرای فرمان‌های غیر مجاز در سیستم هدف (که در حمله صورت می‌گیرند) از شناسایی این حمله محافظت کرد.

- حلقه کنترلی تکرارشونده، که با تکرار رخدادها و گام‌های حمله از قبل اتفاق افتاده، باعث جلوگیری از کشف حالت‌های جدید نفوذ می‌شود.

- جایگزینی با حملاتی که مجموع آن حملات تشکیل‌دهنده حمله مورد نظر مهاجم باشد. یعنی عملاً مهاجم به‌جای یک حمله، دو حمله یا بیشتر انجام می‌دهد.

- افزودن فعالیت‌های پرقدرت و پیچیده می‌توانند اقدامات حمله را برای تأثیرگذاری روی موتور تحلیل هشدار از هم تفکیک کند. برای مثال می‌توان به افزایش دسته‌بندی اشتباه و غلط از راهبرد حمله اشاره کرد. حتی فعالیت‌های پرقدرت می‌توانند باعث انکار خدمات انکار سرویس روی موتور تحلیل شوند، زیرا ظرفیت تمام موتورهای تحلیل هشدار محدود می‌شوند. یک نمونه از نمایش افزودن حمله در جدول (۵) نشان داده شده است. عملکرد مبهم شده با علامت (*) برچسب‌زده شده است.

جدول (۵): نمونه‌ای از سناریوی مبهم‌سازی با فن افزودن حمله

حمله مبهم	حمله مشاهده‌شده	شناسه حمله	حمله اصلی	شناسه حمله
۱*	Subverting Environment Variable Values	۱۳	Subverting Environment Variable Values	۱۳
۲*	Using Slashes in Alternate Encoding	۷۹		
۳	Manipulate Human Behavior	۴۱۶		
۴	Action Spoofing	۱۷۳	Using Slashes in Alternate Encoding	۷۹
۵	Blind SQL Injection	۷		
۶	Redirect Access to Libraries	۱۵۹		

مطابق مدل پیشنهادی شکل (۳) و روابط (۱۲-۹) ملاحظه می‌شود که مبهم‌سازی با فن افزودن حمله طول دنباله حمله مبهم بیشتر از طول دنباله حمله پاک می‌شود.

$$L(Y_1) + L(Y_2), \ldots + L(Y_n) \quad (۹)$$

$$A(Y_1, Y_2 \ldots Y_n) = A(X_1)Y_n) > L(X_1$$

مطابق جدول (۶) برای مبهم‌سازی حمله 79 داریم:

$$X1 = 79 \;\&\; Y1 = 169 \;\&\; Y2 = 7 \;\&\; Y3 = 159$$

$$L(169) + L(7) + L(159) > L(X1) \quad (۱۰)$$

$$A(169, 7, 159) = A(7$$

روش اول، برای مبهم‌سازی حمله 13 :

$$X1 = 13 \ \& \ Y1 = 79 \ \& Y2 = 173 \qquad (۱۱)$$

$$L(79) + L(173) > L(13)$$
$$(79 + 173) = A(79)$$

روش دوم: برای مبهم‌سازی حمله 13 :

$$X_1 = 13 \ \& \ Y_1 = 79 \ \& Y_2 = 416 \qquad (۱۲)$$

$$L(79) + L(416) > L(13)$$
$$A(79 + 416) = A(79)$$

طول دنباله مبهم بیشتر از دنباله حمله پاک باشد. (اگر طول دنباله X=N باشد و m=2 در نظر گرفته شود، طول دنباله حمله مبهم $Y_N=Y_{N/2}$*2=Y خواهد گردید).

برای مدل مذکور احتمال مبهم‌سازی با بهره‌گیری از الگوریتم بیز [۱۴] رابطه (۱۳) به دست می‌آید:

$$P(Y|X) = P(Y1|X1)P(Y2|Y1 \cup X1)\prod_{i=2}^{\frac{N}{2}} P(Y2i-1|Y2i-2 \cup Xi)\, P(Y2i|Y2i-1 \cup Xi) \qquad (۱۳)$$

لازم به ذکر است که برای نمونه مدل، دنباله حمله پاک را با X_i برای $i=\{1,2,3,\dots N/2\}$ و دنباله حمله مبهم را با Y_i برای $i=\{1,2,3,\dots N\}$ نمایش داده شده است.

برای محاسبه فرمول بالا نیاز است که برای یک دنباله حمله پاک $X<x_1,x_2,\dots x_i>$ و حمله مبهم $Y<y_1,y_2,\dots y_i>$ ، مقادیر $P(Y_{2i-1}|Y_{2i-2} \cup X_i)$ و $P(Y_{2i}|Y_{2i-1} \cup X_i)$ محاسبه شوند.

به این منظور جداول مذکور تشکیل خواهد شود و احتمالات داخل جداول بر اساس نظریه احتمالات برای هر یک از y های زوج و فرد به‌صورت زیر محاسبه می‌شود (قابل ذکر است که تعداد فضای نمونه در هر دو رابطه (۱۴) و (۱۵) برای مخرج‌های احتمالات، یکسان و برابر n(s) است).

$$P(Y2i-1|Y2i-2 \cup Xi) = \frac{P(Y2i-1 \cap Y2i-2 \cup Xi)}{P(Y2i-1 \cup Xi)} \qquad (۱۴)$$
$$= \frac{n(Y2i-1 \cap (Y2i-2 \cup Xi))/n(s)}{n(Y2i-2 \cup Xi)/n(s)}$$
$$= \frac{n(Y2i-1 \cap Y2i-2 \cup Xi)}{n(Y2i-2 \cup Xi)}$$

$$P(Y2i|Y2i-1 \cup Xi) = \frac{P(Y2i \cap Y2i-1 \cup Xi)}{P(Y2i-1 \cup Xi)} \qquad (۱۵)$$
$$= \frac{n(Y2i \cap (Y2i-1 \cup Xi))/n(s)}{n(Y2i-1 \cup Xi)/n(s)}$$
$$= \frac{n(Y2i \cap Y2i-1 \cup Xi)}{n(Y2i-1 \cup Xi)}$$

n(s) تعداد کل گام‌های اقدامات دنباله حمله پاک به طول n/2 و دنباله حمله مبهم به طول n در حمله مورد نظر است.

مخرج کسر رابطه $P(Y2i|Y2i-1 \cup Xi)$، به‌صورت تجربی اجتماع تعداد گام‌های اقدامات x_i و y_{2i-1} از یک گروه و صورت کسر، اشتراک تعداد گام‌های y_{2i} با اجتماع تعداد گام‌های x_i و y_{2i-1} است.

به همین ترتیب برای رابطه $P(Y2i-1|Y2i-2 \cup Xi)$ مخرج کسر، اجتماع تعداد گام‌های اقدامات x_i و y_{2i-2} از دو گروه یا یک گروه (x_i از همان گروه اما y_{2i-2} چون اقدام قبلی است بسته به x_{i-1} که از شناسه حمله کدام گروه است، ممکن است از همان گروه یا گروه دیگری باشد) و صورت کسر، اشتراک تعداد گام‌های y_{2i-1} با اجتماع تعداد گام‌های اقدامات x_i و y_{2i-2} است. در ضمن احتمال اقدام حمله مبهم y_1 که اولین اقدام است و فقط با x_i ارتباط دارد، همچنین به علت یکسان نبودن تعداد فضای نمونه در مخرج‌های احتمالات و طول دنباله حمله، از رابطه (۱۶) محاسبه می‌شود:

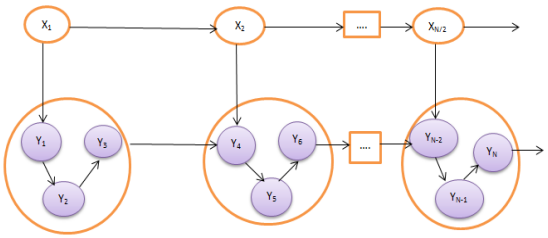
$$P(Y1|X1) = \frac{P(Y1 \cap X1)}{P(X1)} = \frac{n(Y1 \cap X1)/n(s)}{n(X1)/n(r)} = \frac{n(Y1 \cap X1)n(r)}{n(X1)n(s)} \qquad (۱۶)$$

n(r) تعداد کل گام‌های اقدامات دنباله حمله پاک به طول n/2 است.

باید متذکر شد که بر اساس معیار تشابه برای هر اقدام حمله پاک از هر گروه اقدام، n اقدام حمله مبهم از همان گروه جایگزین می‌شود که این دو شناسه حمله مذکور، شامل گام‌های اقدام حمله پاک مربوطه و گام‌های اضافی به‌عنوان نویز در حمله است.

برای مبهم‌سازی با فن افزودن حمله می‌توان از مدل‌های مختلف مانند مدل زنجیره‌ای مارکوف تو در تو استفاده کرد، شمای کلی این مدل در شکل (۶) آورده شده است [۱۶]. همان‌طور که ملاحظه می‌شود، هر حالت از دنباله پاک تبدیل به یک زنجیره مارکوف در دنباله مبهم شده می‌شود. بدین

ترتیب اثبات می‌شود که ساختار مبهم‌سازی دنباله پاک بسیار پیچیده‌تر از مدل ارائه‌شده توسط دو و همکارانش [۵] خواهد گردید که انتظار می‌رود دقت شناسایی سیستم‌های تشخیص نفوذ به مراتب پائین‌تر آید.



شکل (۶): مدل دنباله حملات مبهم با طول سه برابر طول دنباله حملات پاک

احتمال مبهم‌سازی P(Y|X) و توزیع P(Y) برای این مدل به‌صورت روابط (۱۷) و (۱۸) بیان می‌شود:

$$P(Y|X) = \left(\prod_{q=0}^{\frac{N}{3}-1}\left(P(Y3*q+1|Xq) + 1\right)\prod_{j=3*q+2}^{3*q+3} P(Yj|yj - 1)\right) \quad (۱۷)$$

$$P(Y) = \sum_{X} P(X1)\prod_{i=1}^{\frac{N}{3}-1} P(Xi+1|xi)$$

$$P(Y) = P(Y1|X1)P(Y2|Y1)P(Y3|Y2)\prod_{i=1}^{\frac{N}{3}-1} P(Y3i + 1|Xi+1)\,P(Y3i+2|Y3i+1)P|Y3i + 3\,|Y3i+2) \quad (۱۸)$$

۶. ارزیابی مدل پیشنهادی

در این بخش، مدل پیشنهادی حمله متناظر، بر اساس مدل‌سازی احتمالی (الگوریتم بیزین) ارزیابی و نتایج حاصله در بخش بعد مورد تجزیه و تحلیل قرار می‌گیرد. برای ارزیابی مدل حمله متناظر، پنج نمونه دنباله حملات مبهم را با طول‌های مختلف در نظر گرفته‌ایم و در انتهای این بخش نتیجه خواهیم گرفت، در یک طول دنباله حمله مشخص از یک سناریو، آن دنباله با چه مقدار احتمالی، مبهم شده است. برای این منظور، محاسبات لازم را بر اساس الگوریتم بیزین برای این پنج دنباله حمله انجام می‌دهیم و سپس نمودار احتمالات را برای دنباله‌های مبهم رسم می‌کنیم. در تحلیل ذکرشده برای پنج نمونه دنباله پاک `D`,E` A`,B`,C با حداکثر طول ۸، پنج دنباله مبهم-شده A,B,C,D,E با حداکثر طول دو برابر (یعنی ۱۶) در جدول‌های (۱۵-۷) آورده شده است تا احتمالات مبهم‌سازی این دنباله‌های مبهم بر حسب لگاریتم احتمال در طول‌های از ۱ تا ۸ (بر اساس طول‌های دنباله‌های پاک متناظرشان) محاسبه و در جدول (۱۶) آورده شده است.

$X<x_1,x_2,....x_i>$ = طول دنباله حمله پاک

$Y<y_1,y_2,....y_i>$ m=2 طول دنباله حمله مبهم با

A`= < ۱۷,۱۹,۲۱,۲۲,۱۵۱,۱۷۳,۱۶,۹۸>

A= <۱,۹۰,۲۱,۳۰۱,۷۰,۹۰,۹۸,۴۷۳,۴۱۶,۷۹,۱۸,۱۹,۷۹,۱۶۹,۶۲۷,۳۳۰>

جدول (۶): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه A

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}
۱	۹۰	۲۱	۳۰۱	۷۰	۶۸	۹۸	۴۷۳	۴۱۶	۷۹	۱۸	۷۹	۱۶۹	۱۹	۶۲۷	۳۳۰
GP	GP	GP	RD	GP	GP	GP	GP	GP	EUC	EUC	GP	RD	GP	MD	RD
	BPM	RD				RD		RD	RD	RD	RD		EUC		BPM
	RD	MD				MD		EUC	GP		EUC				HA
								BPM							
								RC							
								MD							
								UE							

جدول (۷): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه A`

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
۱۷	۱۹	۲۱	۲۲	۱۵۱	۱۷۳	۱۶	۹۸
GP	GP	GP	GP	GP	GP	GP	GP
RD	EUC	RD	RD		RD		RD
EUC		MD	EUC		EUC		MD
MD					BPM		
					MD		
					RC		
					UE		

جدول (۸): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه B`

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
۳۱۲	۱۳	۱۰۰	۱	۵	۷۰	۲۲	۱۶
RD	UE	GP	GP	GP	GP	GP	RD
HA	RD	UE		RD		RD	
	EUC	EUC				EUC	
	BPM						

B= <۳۱۲,۱۳,۱۰۰,۱,۵,۷۰,۲۲,۱۶>

B = <۳۰۰,۳۲۵,۱۵۹,۹۶,۳۲۰,۹۰,۳,۴,۶,۷,۶۸,۹۸,۱۶,۱۷,۳۰۱,۳۱۲>

جدول (۹): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه B

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}
۳۰۰	۳۲۵	۱۵۹	۹۶	۳۲۰	۹۰	۳	۴	۶	۷	۶۸	۹۸	۱۶	۱۷	۳۰۱	۳۱۲
HA	BPM	BPM	BPM	RD	GP	GP	GP	RD	RD	GP	GP	GP	GP	RD	HA
BPS	HA	EUC	AEL	BPM	BPM	MD		MD	EUC		RD		RD		RD
RD	RD		EUC		RD			EUC			MD		EUC		
EUC			RD										MD		

جدول (۱۰): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه C

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}
۵	۱۴	۴۴	۳۳۰	۱۵۱	۶۳۳	۷۹	۹۰	۳۰۱	۱۶۹	۱۸	۱۷	۵۸۷	۹۵	۱۱	۱۲
GP	RD	EUC	HA	GP	GP	GP	GP	RD	RD	EUC	GP	RD	RD	GP	GP
RC	EUC	UE	RD		HA	RD	BPM			RD	RD			RD	RD
	RC		BPM		AEL	EUC	RD				EUC				
	MD										MD				

جدول (۱۱): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه C`

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
۲	۱۷۳	۴۱۶	۲۲	۷	۸	۹	۱۰
RC	GP	GP	GP	RD	RD	GP	GP
	RD	RD	RD	EUC	EUC	RD	RD
	EUC	EUC	EUC	MD	UE	EUC	EUC
	BPM	BPM			MD	MD	MD
	RC	RC				UE	UE
	MD	MD					

D = <۱۷۳,۴۱۶,۷۰,۹۰,۹۸,۸۹,۱۸,۱۹,۲۱,۲۲,۶۸,۱۵۱,۳۰۱,۳۱۲,۳۲۵,۳۳۰>

D`=<۱, ۳, ۴, ۵, ۹, ۱۰, ۱۱, ۱۲ >

جدول (۱۲): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه D

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}
۱۷۳	۴۱۶	۷۰	۹۰	۹۸	۸۹	۱۸	۱۹	۲۱	۲۲	۶۸	۱۵۱	۳۰۱	۳۱۲	۳۲۵	۳۳۰
GP	GP	GP	GP	GP	RD	EUC	GP	GP	GP	GP	GP	RD	HA	BPM	BPM
RD	RD		BPM	RD		RD	EUC	RD	RD				RD	HA	HA
EUC	EUC		RD	MD				MD	EUC					RD	RD
BPM	BPM														
RC	RC														
MD	MD														
	UE														

جدول (۱۳): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه D`

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
۳	۴	۱	۵	۹	۱۰	۱۱	۱۲
GP	GP	GP	GP	GP	GP	GP	GP
MD			RC	RD	RD	RD	RD
				EUC	EUC		
				MD	MD		
				UE	UE		

جدول (۱۴): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه E`

X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8
۳	۶	۸	۱۴	۹	۱۹	۱۰	۱۷
GP	GP	RD	RD	GP	GP	GP	GP
MD	RD	EUC	EUC	RD	EUC	RD	RD
	MD	UE	RC	EUC		EUC	EUC
		MD	MD	UE		UE	MD
				MD		MD	

E = <۴,۵,۱۸,۷,۷۹,۴۴,۹۸,۶۲۲,۱۴۸,۱۷۳,۱۳,۴۱۶,۲۱,۶۲۷,۷۰,۹۰>

E` =<۳, ۶, ۸, ۹, ۱۰, ۱۴, ۱۷, ۱۹>

جدول (۱۵): تأثیرات گذاشته‌شده بر هدف در اقدامات گروه E

Y_1	Y_2	Y_3	Y_4	Y_5	Y_6	Y_7	Y_8	Y_9	Y_{10}	Y_{11}	Y_{12}	Y_{13}	Y_{14}	Y_{15}	Y_{16}
۴	۵	۱۰۰	۷	۷۹	۴۴	۹۸	۶۲۲	۱۴۸	۱۷۳	۱۳	۴۱۶	۲۱	۶۲۷	۷۰	۹۰
GP	GP	EUC	RD	RD	EUC	GP	RD	MD	GP	RD	GP	GP	MD	GP	GP
	RC	GP	EUC	EUC	UE	RD			RD	EUC	RD	RD			BPM
		UE	MD	GP		MD			BPM	BPM	BPM	MD			RD
									RC	UE	RC				
									EUC		EUC				
											UE				
											MD				

روش محاسبات دنباله A:

$P(Y_1=1|X_1=17) = \frac{P(Y1\cap X1)}{P(X1)} = \frac{n(Y1=1\cap X1=17)n(r)}{n(X1=17)n(s)} = 24/36 * 1/4 = 1/6$

$P(Y_2=9|Y_1=1U\ X_1=17)$

$= \frac{P(Y2\cap(Y1U\ X1)}{P(Y1UX1)} = \frac{n(Y2=9\ \cap(Y1=1U\ X1=17)}{n(X1U\ Y1)} = 1/2$

$P(Y_3|\ (Y_2\ U\ X_2) = 1/3$

بنابراین، احتمال مبهم سازی P(Y|X) برای طول‌های ۱ تا ۱۶ را جهت ۵ گروه A,B,C,D,E محاسبه می‌شود. برای نمونه فقط برای طول‌های ۱ و ۲ از گروه A آورده می‌شود.

L=1:

P (Y| X) = P (Y1 |X1) P (Y2| (Y1UX1)) =24/36*1/4*1/2=0.083

Log (0.083) = -1.08

L=2:

P (Y| X) = P (Y1 |X1) P(Y2|(Y1UX1)) P(Y3|(Y2UX2)) P(Y4|(Y3UX2)) = 24/36*1/4*1/2*1/2*1/4=0.01

Log (0.01) = -2

به همین ترتیب محاسبات برای سایر نمونه حملات انجام‌گرفته و بر حسب لگاریتم احتمال، جدول (۱۶) تشکیل می‌گردد.

جدول (۱۶): احتمالات مبهم سازی برای پنج نمونه حمله مبهم شده

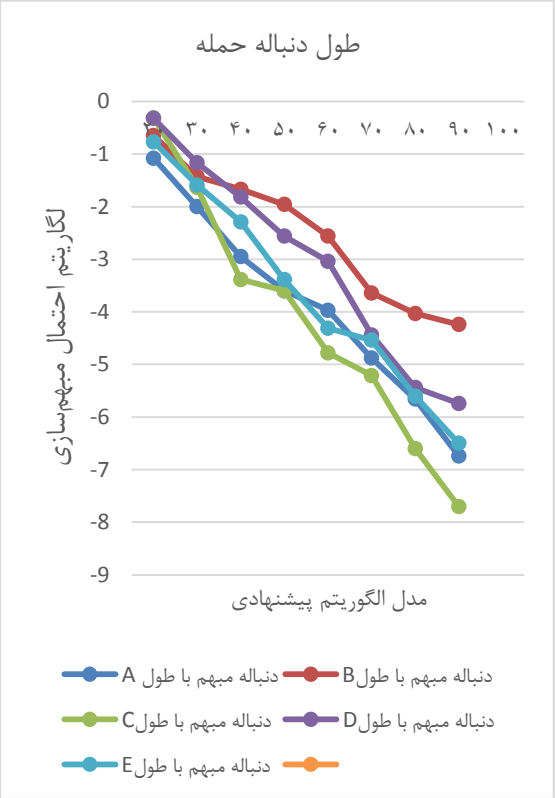
گروه / طول دنباله	A	B	C	D	E
L=۱	-۱/۰۸	-۰/۶۵	-۰/۳۱	-۰/۳۲	-۰/۷۷
L=۲	-۲	-۱/۴۳	-۱/۶۳	-۱/۱۶	-۱/۵۹
L=۳	-۲/۹۵	-۱/۱۷	-۳/۳۸	-۱/۸۲	-۲/۲۹
L=۴	-۳/۶	-۱/۹۶	-۳/۶	-۲/۵۶	-۳/۳۹
L=۵	-۳/۹۷	-۲/۵۶	-۴/۷۸	-۳/۰۴	-۴/۳۱
L=۶	-۴/۸۸	-۳/۰۳	-۵/۲۱	-۴/۴۴	-۴/۵۴
L=۷	-۵/۶۵	-۳/۶۴	-۶/۶	-۵/۴۴	-۵/۶
L=۸	-۶/۷۴	-۴/۲۴	-۷/۴	-۵/۷۴	-۶/۵

۷. تحلیل نتایج ارزیابی

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

در نمودار شکل (۷)، لگاریتم احتمال مبهم‌سازی بر حسب طول دنباله پاک برای پنج نمونه دنباله مبهم A,B,C,D,E نشان داده شده است. همان‌طور که ملاحظه می‌گردد، مبهم‌سازی‌های انجام‌شده توسط محققین قبلی [۵,۶,۷,۸] که

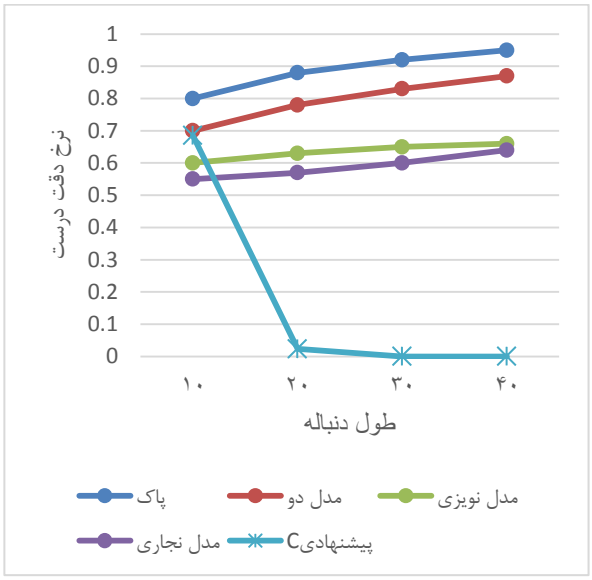
با افزایش طول دنباله، احتمال مبهم‌سازی روند کاهشی را طی می‌کرد؛ زیرا تشخیص دنباله‌های مبهم با افزایش طول دنباله، راحت‌تر می‌شود. ولی در مبهم‌سازی مدل پیشنهادی هر چه طول دنباله حمله بیشتر شود عملیات مبهم‌سازی سخت‌تر می‌شود و دقت طبقه‌بندی حملات توسط سیستم‌های تشخیص نفوذ کاهش می‌یابد.



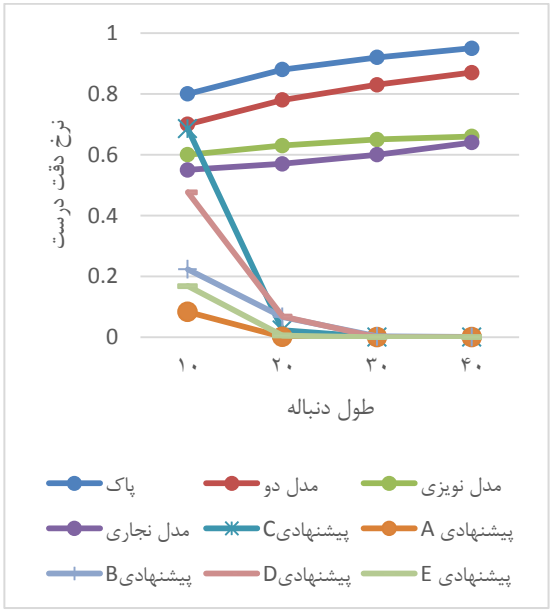
نمودار شکل (۷): نمودار احتمالات دنباله‌های مبهم شده برای طول‌های مختلف (مدل پیشنهادی)

نمودار شکل (۸) دقت طبقه‌بند را برای مدل پیشنهادی در طول‌های ۱۰ تا ۴۰ نمایش داده و مقایسه آن با دقت طبقه‌بند ارائه‌شده توسط دو و همکارانش و نجاری را نشان می‌دهد.

با نگاه به نمودارهای فوق ملاحظه می‌گردد که سیر صعودی در مدل دو و همکارانش برای طول‌های ۱۰ تا ۴۰ سریع است و این نشان از تشخیص راحت‌تر حملات مبهم با افزایش طول حمله دارد اما در مدل نجاری دیده می‌شود که دقت طبقه بند در طول‌های ۱۰ تا ۳۰ تغییر کمتری می‌کند و سیر صعودی نمودار کندتر است و از طول ۳۰ به بعد خطای دقت طبقه‌بند پائین می‌آید و تشخیص حملات مبهم راحت‌تر می‌شود. برای نمونه اگر دقت برای طول ۳۰ در نظر گرفته شود، دقت مدل نجاری در حدود ۵ درصد پائین‌تر از دقت مدل ارائه‌شده توسط دو و همکارانش است و این یعنی خطای طبقه بند در تشخیص حمله مبهم شده، بیشتر می‌شود و کارایی سیستم تشخیص نفوذ برای این مدل مبهم‌سازی کمتر می‌شود. ولی در مدل پیشنهادی همان‌طور که ملاحظه می‌شود اختلاف با سایر مدل‌ها بسیار زیاد است و طول دنباله حمله از ۱۰ تا ۲۰ به شدت پائین آمده و از طول ۲۰ به بعد طبقه‌بندی و تشخیص حمله نزدیک به صفر شده است، این بدان معنی است که مهاجم پیروز شده است و سامانه‌های تشخیص نفوذ خطای کامل انجام داده‌اند. در ادامه نمودار مقایسه‌ای برای ۵ نمونه حمله مبهم شده در شکل (۹) آمده است.



شکل (۸): نمودار مقایسه دقت طبقه‌بندی مدل حمله متناظر (پیشنهادی) m=2 با مدل دو و همکارانش، نجاری و مدل نویزی برای طول‌های مختلف.



شکل (۹): نمودار مقایسه‌ای برای ۵ نمونه حمله مبهم شده

مبهم‌سازی حمله مدل پیشنهادی برای ۵ گروه با سایر مدل‌ها طبق رابطه (۱۹) نشان داده شده است:

$$\begin{bmatrix} \text{پاک} < \text{دو} < \text{نویزی} < \text{نجاری} \\ A > \ E > B > D > C \end{bmatrix} \quad (۱۹)$$

۸. نتیجه‌گیری

مدل پیشنهادی به‌کار رفته شده در این مقاله، برای حملات سایبری، ارائه روش مبهم‌ساز حمله متناظر با فن افزودن حمله، مبتنی‌بر تأثیر حمله می‌باشد. مدل‌های مبهم، با استفاده از مفاهیم شبکه بیزی و زنجیره مارکوف که از اقدامات حمله پاک متناظرشان پیروی می‌کنند و هم‌گروه هستند، ارائه گردید. با بررسی مدل طبقه‌بندی اقدامات حمله به این نتیجه رسیدیم که الگوهای مختلف اقدامات حمله در عین حال که هشدارهای مختلفی در سامانه‌های تشخیص نفوذ تولید می‌کنند، می‌توانند آسیب‌پذیری‌های یکسانی داشته باشند و همین‌طور الگوهایی که از آسیب‌پذیری‌های یکسانی تبعیت می‌کنند نیز دارای گام‌هایی از حمله هستند که در بین روش‌های بکار رفته در آن‌ها اشتراک وجود دارد. به عبارت دیگر اگر حمله‌ای بخواهد رخ دهد، لازم است که اقدام حمله حتماً از آسیب‌پذیری و الگوی یکسان اقدام حمله اصلی پیروی کند. برای مبهم‌سازی این دسته از حملات باید توجه داشت که توانایی‌ها و محدویت‌های مهاجم برای هر کدام از فن‌های مبهم‌سازی متفاوت است. برای فن افزودن حمله، مهاجم هیچ محدودیتی ندارد و به سادگی می‌تواند مدافعین امنیت شبکه را فریب دهد و زمان پاسخ‌گوئی آنها را برای تشخیص راهبردها و سناریوهای مهاجم، به هدر دهد و هزینه‌های گزافی برای مدافعین شبکه ایجاد کند. این فن به خاطر وسعت و دامنه اجرا، مبهم‌سازی را ساده و تشخیص مبهم‌سازی حملات را بسیار سخت می‌کند چرا که مهاجم هر حمله‌ای که کوچک‌ترین شباهت یا وابستگی به حمله مورد نظر و یا حمله‌ای مقدماتی داشته باشد را می‌تواند به سناریوی حمله خود اضافه کند. همچنین با گسترش مبهم‌سازی در حملات و ایجاد یک دنباله حمله مبهم می‌توان با استفاده از فن مبهم‌ساز اضافه حمله، مدیران شبکه را در تشخیص و پیش‌بینی حملات سایبری فریب داد.

۹. مراجع

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

[2] I.You and K.Yim, “Malware Obfuscation techniques: A Brief Survey”, in Beoadband, Wireless Computing, Communication and Applications (BWCCA), International Conference, 2010.

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

[4] 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 (persion)

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

[6] 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 (persion)

[7] 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 (persion)

[8] 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 (persion)

[9] 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.

[10] 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, 1998, pp. 71–79.

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

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

[13] 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

[14] Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description, May2017

[15] Q.Xinzhou, l.Wenke,”Attack plan Recognition and prediction using causal network”, proceedings of the 20th Annual computer security Application conference, 2004.

[16] Grinstead, Charles Miller, and James Laurie Snell, eds. Introduction to probability. American Mathematical Soc, 1997.

Journal of Electronical & Cyber Defence
Vol. 7, No. 4, 2020, Serial No. 28

Modeling of cyber-attacks obfuscation based on the attack analogous to the technique of insertion attacks

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

*Malek Ashtar University of Technology

(Received: 03/12/2018, Accepted: 05/03/2019)

ABSTRACT

One of the most important threats of recent years in computer systems and cyber space is ambiguous cyber-attack.Obfuscation at the level of attack means change of attack, without change in behavior and change in the type of impact of attack on the victim .In this paper, a new classification method has been proposed for modeling cyber attacks, a method based on the technique of insertion attacks. In this method, by increasing the wrong classification in attack strategies, the dependency between the warnings and precautions is separated; so, by increasing the length of the attack, network security managers cannot easily distinguish cyber-attacks. The proposed model is based on Bayesian algorithm .Tables and the assessment figures show the proper formulation of the mechanisms provided for the sequence of attacks so that the detection of obfuscation attacks is far less likely than clean attacks. By increasing the sequence of attacks, the correct classification accuracy tends to zero. The proposed method for obfuscation of the attacks due to the ability to mislead the intrusion detection systems and to create uncertainty in the sequence of the observed attacks, has better performance than the obfuscation logic at both code and action level.

Keywords: Intrusion detection systems, Attacks obfuscation, Insertion attack, Analogous attack

* Corresponding Author Email: rashidi@mut.ac.ir