نشریه علمی «پدافند الکترونیکی و سایبری»
سال هشتم، شماره ۲، تابستان ۱۳۹۹؛ ص ۷۳- ۶۱

**علمی–پژوهشی**

# مدل‌سازی احتمالاتی حملات سایبری چندمرحله‌ای مبهم

**کیانوش شوشیان[۱]، علی جبار رشیدی[۲*]، عبدالرسول میرقدری[۳]**

۱- دانشجوی دکتری، دانشگاه امام حسین(ع)، ۲- استادیار، دانشگاه مالک اشتر، ۳- دانشیار، دانشگاه جامع امام حسین(ع)

(دریافت: ۹۸/۳/۲۲، پذیرش: ۹۸/۸/۱)

## چکیده

در سال‌های اخیر حملات سایبری چندمرحله‌ای مبهم تهدیدی اساسی در حوزه سامانه‌های رایانه‌ای و فضای سایبر است. حملات سایبری چندمرحله‌ای از دو یا چند حمله تک‌مرحله‌ای، تشکیل شده است. مبهم‌سازی حمله به معنای تغییر حمله، بدون تغییر رفتار و تغییر در نوع اثرگذاری حمله بر قربانی است. پس مسأله اصلی پیچیده و مبهم بودن حمله و دشوار بودن تشخیص و هشداردهی رخداد حملات چند مرحله‌ای مبهم است. در این مقاله حملات سایبری چندمرحله‌ای مبهم مدل‌سازی می‌گردد، با فراگیری و به‌کارگیری این دانش، مدافعین امنیت شبکه می‌توانند علاوه بر تشخیص به‌موقع حملات سایبری با انجام دفاع پیش‌کنش‌گرانه، برای دشمنان بازدارندگی ایجاد کنند. مهاجم با بهره‌گیری از مدل پیشنهادی می‌تواند به‌وسیله مرحله‌ای کردن حمله و مبهم‌سازی حملات در دنباله حملات مشاهده‌شده، طبقه‌بندی غلط ایجاد کرده و باعث کاهش وابستگی میان هشدارها، اقدام، مراحل و راهبردهای حمله شود. بنابراین، با ایجاد این تغییرات در حملات سایبری، مدیران امنیت شبکه فریب خورده و به‌سادگی نمی‌توانند هدف نهایی مهاجم را تشخیص دهند. برای ارزیابی مدل پیشنهادی از الگوریتم بیزین بهره گرفته‌ایم. نتایج به‌دست‌آمده از تحقیق و شبیه‌سازی مدل، حاکی از آن است که در روش پیشنهادی، نرخ دقت درست طبقه‌بندی، در بهترین حالت، برای حملات تک‌مرحله‌ای پاک ۰/۰۴- (برحسب لگاریتم) است؛ درصورتی‌که برای حملات چندمرحله‌ای مبهم نرخ دقت درست طبقه‌بندی به ۳۵- (برحسب لگاریتم) تقلیل می‌یابد. لذا مدل پیشنهادی برای حملات چندمرحله‌ای مبهم به‌دلیل توانایی در فریب سامانه‌های تشخیص نفوذ و ایجاد عدم قطعیت در هشدارهای نفوذ، کارایی بیشتری نسبت به منطق حملات تک‌مرحله‌ای پاک دارد.

**کلمات کلیدی:** مدل‌سازی احتمالاتی، حملات سایبری چندمرحله‌ای، حملات مبهم، دنباله حمله

## ۱- مقدمه[۱]

امروزه با توجه به گسترش استفاده از رایانه‌ها و فضای سایبری و به‌تبع آن افزایش چشم‌گیر خطرات موجود در این فضا، نیاز مبرمی به کسب دانش در این محیط‌ها وجود دارد. 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 سامانه‌هایی که مأموریت حیاتی دارند را فراهم می‌کنند. حملات سایبری می‌توانند پیامدهای ناگواری را در شبکه‌های نظامی و همچنین زیرساخت‌های شبکه‌ای غیرنظامی ایجاد کنند. با مدل‌سازی حملات سایبری، تحلیل‌گران این حوزه با دانستن انواع مختلف حملات و فنون به‌کار رفته به ارزیابی اثرات هرکدام از حملات پرداخته و خود را برای دفاع پیش‌کنش‌گرانه آماده می‌کنند. دفاع پیش‌کنش‌گرانه تحلیل‌گران امنیت شبکه را قادر خواهد ساخت تا با اولویت‌بندی حملات به‌جای صرفاً واکنش‌های منفعلانه، اقدامات کنش‌گرانه‌ای را در قبال اقدام آتی یک حمله سایبری به اجرا درآورند.

فعالیت‌های تحقیقاتی انجام‌شده توسط محققین، در رابطه با پدافند سایبری یعنی تشخیص و پیش‌بینی حملات سایبری در سطح حملات تک‌مرحله‌ای و یا حملات پاک (غیرمبهم) صورت گرفته است. ولی تاکنون تحقیقات خاص و مؤثری در بخش حملات سایبری چندمرحله‌ای مبهم، یا صورت نگرفته و یا اگر انجام‌شده است، نتایج آن منتشر نشده است و این احتمال وجود دارد که به دلیل خاص و راهبردی بودن مسئله، نتایج و گزارش‌های تحقیقات به‌طور شفاف منتشرنشده باشد. لذا تحقیقات و پژوهش‌های موجود نمی‌تواند پاسخگوی این‌گونه از حملات باشد به همین جهت تمرکز اصلی مقاله بر مسئله مدل‌سازی حملات سایبری چندمرحله‌ای مبهم است. در این مقاله طرح جدیدی از مدل‌سازی حملات سایبری چندمرحله‌ای مبهم ارائه شده است که هدف آن پیچیده و سخت‌تر کردن

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

تشخیص حملات برای مدافعین امنیت شبکه است. از شاخصه‌های ارزیابی عملکرد مدل پیشنهادی می‌توان به محاسبه میزان احتمال تشخیص مبهم‌سازی حمله به‌کار رفته در دنباله حملات و نوع حمله اشاره کرد.

این مقاله در نظر دارد روش مبهم‌سازی را برای اولین بار برای حملات چندمرحله‌ای به‌صورت احتمالاتی مدل‌سازی نماید. ساختار مقاله در بخش‌های دیگر به‌صورت زیر خواهند بود. در بخش دوم کارهای مرتبط بیان می‌شود. برخی از تعاریف و مفاهیم اساسی موردنیاز که در متن مقاله از آن استفاده می‌شود را در بخش سوم بیان می‌کنیم. بخش چهارم به تبیین مدل پیشنهادی، تعریف مسئله و مثالی برای حملات سایبری تک‌مرحله‌ای مبهم به همراه نتایج حاصله پرداخته‌ایم و در بخش پنجم برای صحت‌سنجی و اعتبارسنجی مدل پیشنهادی از قضایا و گزاره‌های ریاضی بهره گرفته‌ایم. در بخش نهایی نتایج حاصل از مدل‌سازی حملات چندمرحله‌ای مبهم مورد تحلیل قرار می‌گیرد

## ۲- کارهای مرتبط با حملات چندمرحله‌ای

مرجع [۱] در ارتباط با چیستی حملات چندمرحله‌ای توضیح نمی‌دهد. ولی به پیچیده بودن و اهمیت پرداختن به حملات سایبری چندمرحله‌ای اذعان دارد و بیان می‌کند، سامانه‌های تشخیص نفوذ سنتی برای تشخیص حملات نوین و حملات سایبری چندمرحله‌ای مؤثر نیستند. مرجع [۲] حملات چندمرحله‌ای را دنباله‌ای از وقایع انجام‌شده توسط مهاجم می‌داند. لذا برای شناخت و رویکرد رفتار مهاجم، نیاز است تمام مراحل حمله را در نظر گرفت و حتی اگر تنها یک گام از حمله ازدست‌رفته باشد، تمام رفتارهای مهاجم ناشناخته خواهد ماند. این مقاله با ارائه چارچوبی جهت بهبود میزان تشخیص حملات و کاهش مثبت‌های کاذب با استفاده از همبستگی هشدارها به آشکارسازی و تشخیص حملات چندمرحله‌ای پرداخته است. مرجع [۳] حمله استاکس‌نت را مشهورترین مثال برای حمله‌ی چندمرحله‌ای به زیرساخت‌های تأسیسات هسته‌ای جمهوری اسلامی ایران معرفی می‌کند. دیسو [۴] در رساله دکتری خود در سال ۲۰۱۱ یک معماری جدید برای سامانه‌های تشخیص نفوذ جهت تشخیص حملات چندمرحله‌ای در یک محیط چندهسته‌ای ارائه داده است و با استفاده از درخت حمله به مدل‌سازی حمله چندمرحله‌ای پرداخت. در مرجع [۵] روشی برای درک حملات چندمرحله‌ای از طریق تجسم جریان‌های ناهمگون بر پایه ردگیری حمله توسط حس‌گرهای تشخیص نفوذ، ثبت رخدادها[1] و سایر منابع رخدادی در شبکه‌های رایانه‌ای ارائه شده است. در این تحقیق از تجمیع و همبستگی وقایع بر اساس محتوای معنایی برای ردیابی حمله‌هایی که در زمان بلادرنگ واقع می‌شود، استفاده شده است. هم‌چنین یک چارچوب تلفیقی مبتنی بر استفاده از مدل‌های عمومی حملات چندمرحله‌ای در کنار اطلاعات IP آدرس رخدادهای ناهمگون که بر اساس مراحل حمله همبسته می‌شوند، ارائه شده است. دو [۶] در رساله دکترای خود در سال ۲۰۱۴ 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. یک دنباله حمله به‌صورت فرمال را به‌عنوان بردار متغیرهای تصادفی توصیف‌شده در نظر گرفت و هر مشاهده را یک نمونه از مدل‌های حمله به شمار آورد. دو و یانگ [۷] در سال ۲۰۱۳ مطالعات مقدماتی بر روی مدل‌سازی فن‌های مبهم‌سازی برای دنباله عملکردهای حمله شبکه‌ای انجام دادند. هدف این پژوهش، توسعه و بهبود یک روش تحلیلی کارآمد است که چگونگی تأثیرگذاری نویز عمدی روی مدل‌سازی و طبقه‌بندی دنباله‌های حمله را نشان می‌دهد. گویال و همکارانش [۸] در سال ۲۰۱۲ به انواع روش‌های مبهم‌سازی در بدافزارهای استاکس‌نت[2] و فلیم[3] پرداختند. آن‌ها ویژگی‌های اصلی برای تشخیص بدافزار و ممانعت شامل موارد امنیتی، ایمنی، مخفی‌سازی و پایداری می‌دانند لذا این خصیصه‌ها را موردبررسی قراردادند و ضمن مشخص کردن ویژگی‌های بدافزار استاکس نت، بدافزار فلیم و بدافزار مایدوم[4]، ویژگی‌های ابهام‌سازی این بدافزارها را مورد بررسی قرار دادند. اندرسون و همکارانش در [۹] و باراک و همکارانش در [۱۰] نیز سعی کردند تا روشی برای مقابله با حملات مبهم‌سازی شده ارائه دهند. در این مطالعه، رفتار هر حمله مورد ارزیابی قرار گرفت. به‌عبارت‌دیگر برای هر حمله، نوع، چگونگی و تعداد تماس‌های سیستم‌عامل در حملاتی که دارای کد اجرایی هستند مورد ارزیابی قرار می‌گیرد و از این طریق حملات شناسایی می‌شوند. در این حالت اگر حملاتی هم مبهم‌سازی شده باشند، رفتار آن‌ها همچنان ثابت است و از این طریق قابل‌شناسایی خواهد بود.

فعالیت‌های تحقیقاتی انجام‌شده توسط محققین پیشین، عمدتاً در مورد تشخیص حملات سایبری تک‌مرحله‌ای و یا حملات سایبری چندمرحله‌ای غیرمبهم صورت گرفته است. یکی از چالش‌های مهم در مبهم‌سازی حملات سایبری، افزایش طول

[1] Log

[2] Stuxnet
[3] Flame
[4] Mydoom

دنباله حمله است. مهاجمین برای انجام حملات پیچیده در محیط راهبردی، ناگزیرند از دنباله حملات طولانی استفاده کنند، لذا این افزایش طول حمله باعث می‌شود سامانه‌های تشخیص نفوذ با طبقه‌بندی دقیق حملات، کارائی خود را بهبود داده و حملات سایبری را با احتمال بیش از ۹۰٪ تشخیص دهند [۱۲].

## ۳- مفاهیم اساسی و اصطلاحات

### ۳-۱- طبقه‌بندی دنباله حملات

به معنی یافتن طبقه موضوعی مناسبی است که با کمترین خطا هدف مهاجم از حمله را نشان دهد. مدافع با این کار می‌تواند با مربوط کردن یک حمله به یکی از طبقات از پیش تعریف شده، صورت پذیرد. هدف مدافع از طبقه بندی این است که ابتدا با استفاده از مجموعه ی کوچکی از دنباله حملات یک مدل مناسب بسازد و سپس برمبنای مدل ایجاد شده داده‌هایی(حملات) که در آینده مشاهده می‌شود را به درستی طبقه‌بندی کند

### ۳-۲- حملات تک‌مرحله‌ای[1]

حملات شایعی هستند که در یک مرحله طرح‌ریزی و اجرا می‌شوند و شامل حملات زیر هستند.

### ۳-۳- حمله متا[2]

به حملات جامع سایبری گفته می‌شود که مهاجم از یک روش یا فن پیشرفته استفاده می‌کند. یک حمله متا معمولاً نوعی نتیجه از یک فن‌آوری با عملکردی با تأثیرگذاری بالا به شمار می‌رود و به‌منظور بیان مفهوم یک رویکرد سطح بالا طراحی شده است. حمله متا از گروهی از حملات استاندارد[3] مشابه و حملات جزئی[4] مشابه تشکیل شده است. این حملات برای معماری و طراحی تهدیدات پیشرفته بسیار مفید هستند. این نوع حملات علاوه بر این‌که به‌تنهایی می‌توانند هدف نهایی یک مهاجم باشد، می‌توانند به‌عنوان یک هدف مقدماتی و یا میانی برای اجرای یک حمله راهبردی و بزرگ‌تر نیز عمل کنند [۱۳].

### ۳-۴- حمله استاندارد

این نوع حملات اغلب به‌عنوان بخشی از یک حمله سطح بالاتر، که به‌طور کامل اجرا شده دیده می‌شوند. یک حمله استاندارد به‌منظور ارائه جزئیات کافی برای درک فن خاص و نحوه عملکرد آن برای رسیدن به هدف مشخص اجرا می‌شود. این حمله نوع خاصی از یک حمله جامع متا محسوب می‌شود. حمله استاندارد شامل گروهی از حملات جزئی، حملات چندگامی و حملات تک گامی در سطح استاندارد و جزئی تشکیل‌شده است. هم‌چنین حمله استاندارد می‌تواند یک یا چند حمله استاندارد مشابه دیگر را برای تکمیل اجرای حمله خود فراخوان کرده و از این نوع حملات کمک بگیرد. این نوع حملات علاوه بر این‌که به‌تنهایی می‌تواند هدف نهایی یک مهاجم باشد می‌تواند به‌عنوان یک هدف مقدماتی و یا میانی برای اجرای یک حمله راهبردی و بزرگ‌تر نیز عمل کنند و به عبارتی مقدمه‌ای برای یک حمله متا هستند [۱۳].

### ۳-۵- حمله جزئی

سطح پایینی از حملات بزرگ‌تر (استاندارد و متا) است و پیش‌نیازی برای آن حملات محسوب می‌شود، البته اجرای حملات جزئی به‌تنهایی نیز یک حمله کامل محسوب می‌شود. مهاجم برای انجام حملات جزئی می‌تواند، با استفاده از فنون مخصوص و فن‌آوری خاص قربانی خود را مورد هدف قرار داده و روند کامل یک حمله را اجرا کند. یک حمله جزئی معمولاً با اتصال به حملات استاندارد به اهداف اصلی خود می‌رسند. حمله جزئی شامل حملات چندگامی و حملات تک گامی تشکیل است. این نوع حملات علاوه بر این‌که به‌تنهایی می‌تواند هدف نهایی یک مهاجم باشد می‌تواند به‌عنوان یک هدف مقدماتی و یا میانی برای اجرای یک حمله عملیاتی و بزرگ‌تر نیز عمل کنند و به عبارتی سرپلی برای یک حمله استاندارد هستند [۱۳].

### ۳-۶- حملات چندگامی[5]

حملات سطح پائینی هستند که اغلب توسط افراد با تخصص کم و دانش ضعیف صورت می‌گیرند و هیچ سناریوی حمله‌ای از قبل تعیین‌شده‌ای توسط مهاجم طرح‌ریزی نشده است. درعین‌حال می‌توان گفت: این نوع حملات به‌عنوان یک گام حمله از یک عملیات سطح بالاتر مانند: حملات جزئی، استاندارد و یا متا قرار گیرند و حتی می‌توانند مقدماتی برای حملات چندمرحله‌ای ایجاد کند مانند حملات تغییر کوکی‌های HTTP، حملات دسترسی به کاربر و... [۱۳].

### ۳-۷- حملات تک‌مرحله‌ای

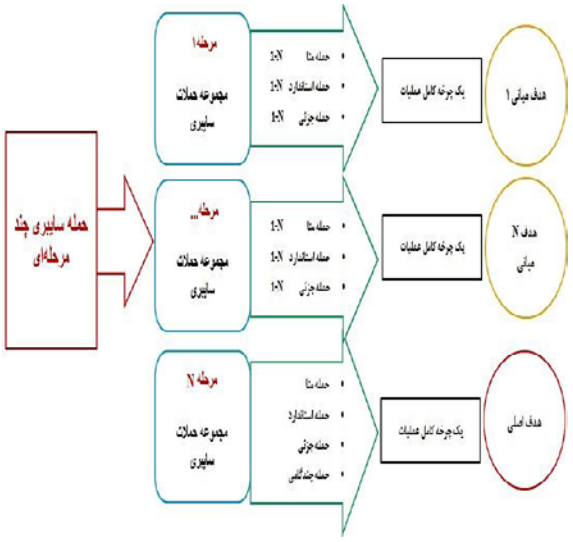
مجموعه‌ای از حملات مختلف هستند که برای رسیدن به هدف خود در یک مرحله طرح‌ریزی و اجرا می‌شوند.

[1] Single - stage attacks
[2] Meta
[3] Standard
[4] Detailed
[5] Multi-step attacks

### ۳-۸- حملات چندمرحله‌ای [1]

اگر مراحل یک حمله سایبری از سطح دسترسی تاکتیکی (پائین) به سطح دسترسی عملیاتی (میانی) و سپس به سطح دسترسی راهبردی (بالا) ارتقاء یابد و در این مسیر، اهداف اولیه (در سطح تاکتیکی) و میانی (در سطح عملیات) گام‌های لازم برای دستیابی به هدف نهایی (در سطح راهبرد) باشند آن را حمله سایبری چندمرحله‌ای می‌نامیم.

حملات سایبری چندمرحله‌ای، مجموعه‌ای از روندهای مخفیانه، درعین‌حال پابرجا و پیچیده‌ای از حملات هستند که برای رسیدن به هدف اصلی خود از چند مرحله مختلف تشکیل شده‌اند، مهاجم برای رسیدن به هدف اصلی و نهایی خود باید حملات متعددی را انجام دهد؛ هر یک از مراحل حمله چندمرحله‌ای به‌خودی‌خود یک حمله کامل محسوب می‌گردند؛ یعنی هر مرحله یک فرآیند کامل عملیات را دارد. سرمنشأ این حملات به‌جای یک شخص یا گروه، سازمان‌های بزرگ و در مواردی دولت‌ها هستند و اهدافشان به‌جای یک یا چند شبکه باانگیزه مادی، ضربه زدن به زیرساخت‌های حیاتی یک کشور باانگیزه‌های سیاسی، نظامی، اقتصادی و یا فرهنگی است. فرآیندهای حمله چندمرحله‌ای در شکل (۱) نمایش داده شده است.




**شکل (۱):** حمله چندمرحله‌ای.

### ۳-۹- حملات پاک [2]

در این نوع حملات از هیچ روش و یا فنی برای مخفی بودن حملات استفاده نشده است؛ این نوع حملات به‌راحتی توسط سامانه‌های تشخیص نفوذ قابل‌شناسایی هستند [۶].

### ۳-۱۰- مبهم‌سازی

لفظ مبهم‌سازی [3] 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.

مبهم‌سازی در سه سطح نویز، اقدام [4] و حمله قابل‌اجرا است.

### ۳-۱۱- سطح نویز

حمله‌ی 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].

### ۳-۱۲- مبهم‌سازی کد [5]

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 [۱۱]. یکی از تلاش‌های معروف جهت مبهم‌سازی کد اجرایی تبدیل یا تغییر کد است. مانند افزودن کدهای مرده، جابجایی دستورالعمل‌های پرش با برخی کدهای خطادار 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.

### ۳-۱۳- مبهم‌سازی سطح اقدام

مبهم‌سازی در سطح اقدام به معنی انجام فنونی در اجرای اقدام و فعالیت‌های مقدماتی 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.

### ۳-۱۴- مبهم‌سازی 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

[1] Multi - stage attacks
[2] Clean
[3] Obfuscation
[4] Action-level
[5] Code-level

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:

### ۳-۱۴-۱- 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.

### ۳-۱۴-۲- فن حذف حمله

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

### ۳-۱۴-۳- فن جایگزین حمله

تغییر یا جایگزینی حمله می‌تواند دنباله مشابهی از حملات واقعی ایجاد نماید، این دنباله 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.

## ۴- مدل پیشنهادی

در این بخش، یک مدل احتمالاتی برای حملات چندمرحله‌ای مبهم ارائه می‌کنیم. در مدل ما، حملات سایبری در شرایط زیر قابل‌تشخیص نیستند:

- مرحله‌ای کردن حمله سایبری
- مبهم‌سازی مراحل حمله با فن‌های ترکیبی
- استفاده از نرخ مبهم‌سازی ۱۰۰ درصدی

مدل پیشنهادی حملات سایبری چندمرحله‌ای مبهم مطابق شکل (۲) است. این مدل از پنج مرحله تشکیل شده است:

### مرحله یک؛ طرح‌ریزی و انتخاب حملات پاک

مهاجم در این بخش با توجه به طرح‌ریزی که قبلاً انجام داده است، تمام حملات پاک موردنیاز حمله خود را شامل: حملات متا، حملات استاندارد، حملات جزئی خود را انتخاب می‌کند.

### مرحله دوم؛ مبهم‌سازی حملات پاک

مهاجم بر اساس نرخ مبهم‌سازی و نوع فن مبهم‌سازی، حملات پاک انتخاب‌شده از مرحله قبل را به هراندازه که بخواهد، مبهم می‌نماید. این بخش متشکل از تعدادی حمله پاک و تعدادی حمله مبهم است.

### مرحله سوم؛ تولید مجموعه (دنباله) حملات پاک

مهاجم در این بخش با توجه به فرصت‌ها، قابلیت‌ها و راهبردی‌های انتخابی دنباله حمله پاک خود را که به‌صورت زمان‌دار و مرحله‌ای می‌خواهد اجرا کند، تولید می‌سازد.

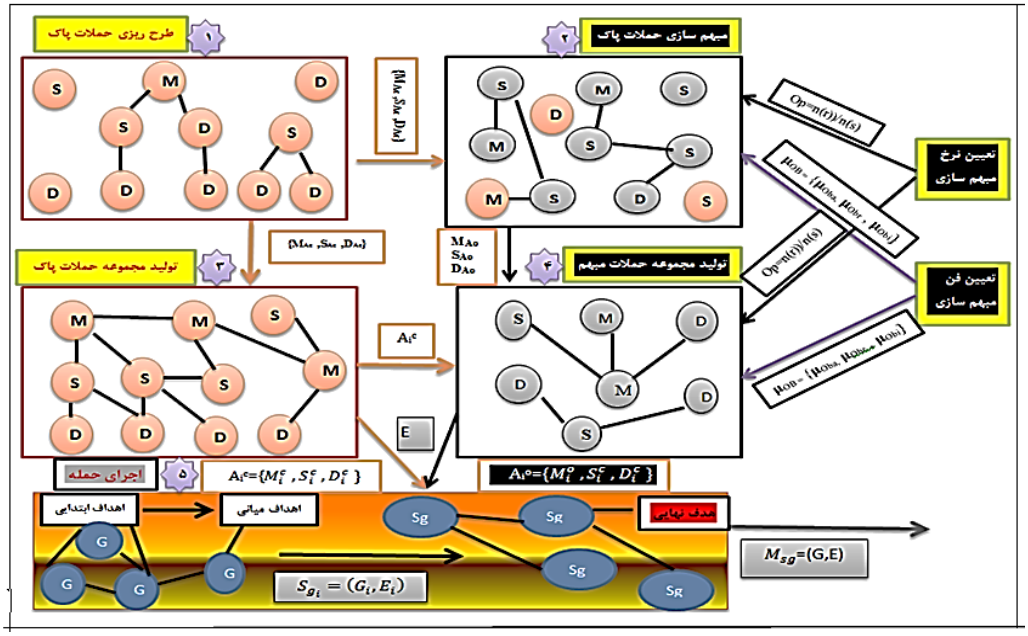
### مرحله چهارم؛ تولید مجموعه (دنباله) حملات مبهم

در این بخش با در نظر گرفتن زمان و ترتیب اجرا، مجموعه حملات بخش قبل انتخاب می‌کند. سپس این دنباله حملات بر اساس نرخ مبهم‌سازی و فن موردنظر مهاجم (اضافه حمله، حذف حمله و جایگزین حمله) مبهم‌سازی شده و دنباله حملات مبهم تولید می‌شود.

### مرحله پنجم؛ اجرای حملات

این بخش اجرای حملات نامیده می‌شود و از دو ماهیت یا ویژگی وابسته به هم تشکیل شده است.

۱- ماهیت اهداف **G** شامل: اهداف اصلی و فرعی
۲- ماهیت راه‌کارها **E** شامل: نحوه رسیدن به اهداف اصلی و فرعی

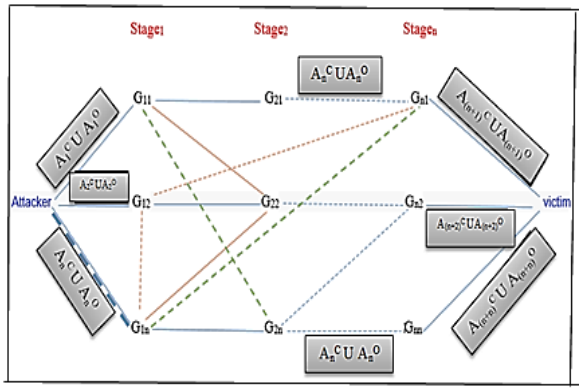



**شکل (۲)**: مدل پیشنهادی حملات سایبری چندمرحله‌ای مبهم.

مهاجم در این بخش به‌منظور دست‌یابی به اهداف فرعی ( ابتدایی و میانی) با توجه به دنباله حملات پاک و دنباله حملات مبهم به‌دست‌آمده، حملات دنباله‌داری را در زمان‌های مختلف اجرا می‌کند، سپس در ادامه دسترسی‌ها و امتیازات خود را ارتقاء داده و برای رسیدن به اهداف اصلی (نهائی)، مراحل حمله خود را اجرا می‌کند. تا زمانی که مهاجم به هدف نهایی خود نرسد، این حملات مستمر، پیچیده و مخفی ادامه می‌یابند. بدیهی است طول دنباله حملات چندمرحله‌ای مبهم براساس مدل مبهم مورد نظر مهاجم و حملات پاک به‌دست می‌آید. پیچیدگی روابط بین حملات پاک و حملات مبهم براساس مدل مبهم، فن‌های مختلف مبهم‌سازی و مراحل حمله انتخابی توسط مهاجم تعیین می‌شود.

چون هدف از مبهم‌سازی حمله، کاهش نرخ طبقه‌بندی درست دنباله حملاتی است که منجر به کاهش احتمال تشخیص حملات مبهم نسبت به حملات پاک می‌گردد، لذا احتمال تشخیص مبهم‌سازی حملات با شانس موفقیت مهاجم ارتباط معکوس دارد. بنابراین، محور اصلی این پژوهش ارائه یک مدل تحلیلی برای حملات سایبری چندمرحله‌ای مبهم است.

برای روشن شدن بیشتر مدل پیشنهادی یک مدل ساده‌تر با جریان اجرای حمله چندمرحله‌ای مبهم در شکل (۳) نشان داده شده است. همان‌طور که در شکل (۳) ملاحظه میشود مهاجم[1] حمله خود را به سمت قربانی[2] در چند مرحله (مرحله ۱ تا مرحله n) انجام می‌دهد که هر مرحله شامل تعدادی راه‌کار است.




**شکل (۳)**: مدل ساده حملات چندمرحله‌ای مبهم

### ۴-۶- تعریف مسئله

در این بخش مسئله موردنظر و تمام متغیرها برای طرح‌ریزی و اجرای حملات سایبری چندمرحله‌ای مبهم بیان می‌گردد.

نمادهای استفاده‌شده در مدل‌سازی حمله در جدول (۱) آورده شده است.

[1] Attacker
[2] victim

**جدول (۱):** نمادهای استفاده‌شده در مدل‌سازی حمله.

| مفهوم | نماد | مفهوم | نماد |
|---|---|---|---|
| طول دنباله حملات پاک | Lc | مجموعه فضای حمله | Ω |
| طول دنباله حملات مبهم | Lo | حملات چندمرحله‌ای | $M_{Sg}$ |
| طول دنباله حملات نویز | $L_N$ | احتمال موفقیت نهائی مهاجم | P(E) |
| حمله پاک | X | حملات چندمرحله‌ای مبهم | $M_{sg}^{O}$ |
| حمله مبهم | Y | هدف نهائی | G |
| مدل‌های حمله | ℧ | راه‌کارهای حملات | E |
| مجموعه حملات مبهم | $A^O$ | احتمال موفقیت تک‌مرحله‌ای مهاجم | $P(E_i)$ |
| طول دنباله حمله مشاهده‌شده | N | مجموعه حملات پاک | $A^C$ |
| نرخ مبهم‌سازی | $O_p$ | احتمال تشخیص مبهم‌سازی حمله | $P^o(Y\|X)$ |

اگر G معرف هدف اصلی مهاجم باشد و E معرف راه‌کارهای (حملات) در اختیار مهاجم باشد، آن‌گاه $M_{sg}^{o}$ معرف حمله سایبری چندمرحله‌ای مبهم است، این تعریف در رابطه (۱) بیان‌شده است. مهاجم برای رسیدن به هر هدف باید مراحلی[1] از حمله را طرح‌ریزی و اجرا کند، هر مرحله از حمله $S_{g_i}$ نیز دارای هدف فرعی $G_i$ با سطوح پائین‌تر است، اجرای مراحل ابتدایی و میانی برای رسیدن به هدف فرعی، پیش‌نیازی ضروری برای رسیدن به هدف اصلی است.

$$M_{sg}=\{G,E\} \qquad (۱)$$

$$S_{g_i}=\{G_i,E_i:\ i=1,2,\dots,n\} \qquad (۲)$$

اگر Ω فضای تمام حملات سایبری باشد و $A^c$ نمایانگر مجموعه حملات سایبری پاک و $A^o$ به معنی مجموعه حملات سایبری مبهم باشند آن‌گاه داریم:

$$\Omega=A^c \cup A^o \qquad (۳)$$

در این نوع حملات یکی از مراحل حمله با طول دنباله (سازگار) به‌عنوان نقطه شروع انتخاب و اجرا می‌شود. مهاجم با اجرای راه‌کارهای مختلف خود به اهداف خود می‌رسد. در مرحله اول به هدف ابتدایی خود می‌رسد و بقیه راه‌کارها به‌عنوان مراحل بعدی حمله هستند که توسط مهاجم در حین و یا پس از حمله مرحله اول مشخص می‌شوند، هم‌چنین مهاجم ممکن است راه‌کارهایش را طول اجرای حمله، تغییر دهد تا بتواند به هدف نهایی خود برسد، بر همین اساس مهاجم با توجه به راهبردهایش می‌تواند این دنباله حملات مرحله‌ای را تشکیل دهد. هر راه‌کار E شامل مجموعه‌ای از راه‌کارهای سطوح پائین‌تر است، که برای هر راه‌کار $E_i$ مجموعه طراحی‌شده‌ای از دنباله حملات پاک $A_i^C$ و مجموعه طراحی‌شده‌ای از دنباله حملات مبهم $A_i^o$ وجود دارد. مجموعه کلیه نتایج ممکنه برای یک حمله انتخابی طبق رابطه (۴) است.

$$E_i=\{E_{i1},E_{i2},\dots E_{in}:\ i=1,2,\dots,n\} \qquad (۴)$$

$$E_i = A_i^C \cup A_i^o$$

برای به‌دست آوردن راه‌کارهای یک مرحله از حمله چندمرحله‌ای مبهم از روابط (۲)، (۳)، (۴) استفاده می‌کنیم.

$$A_i^C=\{A_{i1}^C, A_{i2}^C, \dots, A_{in}^C : i=1,2,\dots n\}$$

$$A_i^o=\{A_{i1}^o, A_{i2}^o, \dots, A_{in}^o : i=1,2,\dots n\}$$

$$A_i^C \cap A_i^o = \phi$$

$$A_1^c \cup A_1^o = \{ x \mid x \in A_1^C \vee x \in A_1^o \}$$

$$E_1=A_1=\{ (A_{11}^C \cup A_{11}^o) \cup \dots \cup (A_{1n}^C \cup A_{1n}^o) \} \qquad (۵)$$

$$E_n= A_n=\{ (A_{n1}^C \cup A_{n1}^o) \cup \dots \cup (A_{nn}^C \cup A_{nn}^o) \} \qquad (۶)$$

با توجه به این‌که $E_1, E_2, \dots, E_n$، پیشامدهای راه‌کار مهاجم برای اجرای مراحل مختلف رسیدن به اهداف فرعی هستند، اجتماع این پیشامدها، حمله چندمرحله‌ای مبهم را شکل می‌دهد و طبق رابطه (۷) داریم:

$$\cup_{i=1}^{n} E_i = \{x|(x \in E_1) \vee (x \in E_2) \vee \dots, \dots, \vee (x \in E_n)\} \qquad (۷)$$

اگر $P(E)$ احتمال موفقیت نهائی مهاجم از انجام حملات چندمرحله‌ای مبهم و G هدف نهایی او باشد، مطابق رابطه (۸) داریم:

$$P(E) = P(\cup E_i) = \sum_{i=1}^{n} P(E_i) - \sum\sum_{i\neq j} P(E_i \cap E_j) - \sum\sum\sum_{i\neq j\neq k} P(E_i \cap E_j \cap E_k) + \dots + (-1)_{n+1} P(E_1 \cap \dots \cap E_n) \qquad (۸)$$

برای به‌دست آوردن $P(\text{Stage i} = E_i)$ احتمال موفقیت فرعی مهاجم برای هر راه‌کار (یک مرحله از حملات چندمرحله‌ای مبهم) اگر $G_i$ اهداف فرعی او باشد و $P(E_i^c)$ احتمال موفقیت مهاجم در حملات تک‌مرحله‌ای پاک و $P(E_i^c)$ احتمال موفقیت مهاجم در حملات تک‌مرحله‌ای مبهم باشد، از رابطه (۹) استفاده می‌کنیم:

[1] Stage

$$P(\text{موفقیت مرحله‌ای مهاجم}) = P(\text{Stage i}) = P(E_i) = P(E_i^c \cup E_i^c) = P(A_i^c \cup A_i^c) \quad (۹)$$

$$P(E_i) = P\{(A_1^C \cup A_1^O) \cup (A_2^C \cup A_2^O) \cup \ldots \cup (A_n^C \cup A_n^O)\},\ i=1,2,\ldots\ldots n \quad (۱۰)$$

در رابطه (۱۰) $A_i^o$ وابستگی شرطی به $A_i^c$ دارد $P(A_i^c \mid A_i^o)$ رابطه بین دنباله حملات پاک و حملات مبهم را نشان می‌دهد. بر اساس مدل‌های طراحی‌شده توسط مهاجم در طول دنباله حمله، رابطه بین دنباله حملات پاک $A_i^c$ و دنباله حملات مبهم $A_i^o$ متفاوت خواهد بود.

$$P(A_i^C \cap A_i^o) = P(A_i^c \mid A_i^o)\, P(A_i^o \quad (۱۱)$$

اگر $P(A_i^C)$ احتمال تشخیص دنباله حملات پاک و $P(A_i^O)$ احتمال تشخیص دنباله حملات مبهم باشد، توجه به عدم استقلال رخدادها و سازگاری آن‌ها در یک مرحله از حمله چندمرحله‌ای مبهم داریم:

$$P(A_i^C \cup A_i^o) = P(A_i^C) + P(A_i^o) - P(A_i^C \cap A_i^o) \quad (۱۲)$$

مجموعه دنباله حملات $A_i$ شامل دنباله‌ای از حملات $X_i$ هستند، که طبق رابطه (۱۳) به‌دست می‌آید:

$$A_i = \{Xi: i = 1,2, \ldots 9\} \quad (۱۳)$$

این دسته حملات دنباله‌ای $X_i$ طبق رابطه (۱۴) شامل حملات پاک متا $M_i^C$، حملات مبهم متا $M_i^o$، حملات پاک استاندارد $S_i^C$، حملات مبهم استاندارد $S_i^O$، حملات پاک جزئی $D_i^C$ و حملات مبهم جزئی $D_i^0$ است.

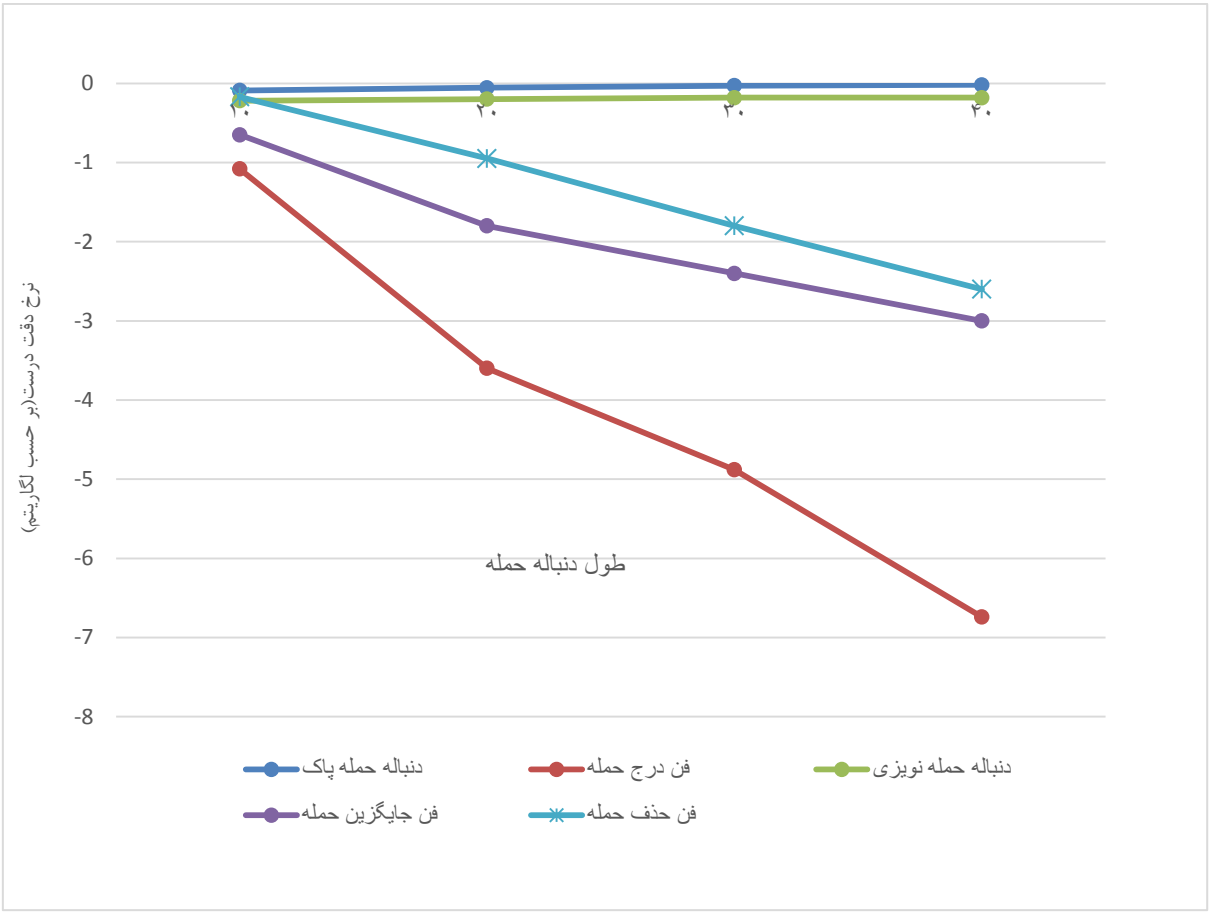
$$X_i = \{(M_1^C, S_1^C, D_1^C), \ldots, (M_n^C, S_n^C, D_n^C), (M_1^o, S_1^O, D_1^o), \ldots, (M_n^o, S_n^o, D_n^o)\} \quad (۱۴)$$

$$X_i = \{(M_1^C, \ldots, M_n^C) \cup (S_1^C, \ldots, S_n^C) \cup (D_1^C, \ldots, D_n^C) \cup (M_1^o, \ldots, M_n^o) \cup (S_1^o, \ldots, S_n^C) \cup (D_1^o, \ldots, D_n^o)\}$$

برای روشن شدن نحوه عملکرد مبهم‌سازی حملات تک‌مرحله‌ای با توجه به شبیه‌سازی انجام‌گرفته، یک مثال ارائه نموده‌ایم. مدل پیشنهادی در این مطالعه موردی بر اساس مدل‌سازی احتمالی ارزیابی و نتایج حاصله مورد تجزیه‌وتحلیل قرار گرفته است و با تحقیقات دیگران مقایسه شده است. محاسبات بر اساس الگوریتم بیزین انجام گرفته است. در جدول (۲) شبیه‌سازی برای حملات سایبری تک‌مرحله‌ای وابسته به همدیگر و نرخ مبهم‌سازی ۴۰ برای دنباله حمله شامل حمله نویزی، حمله پاک، حمله مبهم شده با فن اضافه حمله، حمله مبهم شده با فن حذف حمله، حمله مبهم شده با فن جایگزین حمله محاسبه و بیان شده است.

**جدول (۲)**: مثالی از نحوه عملکرد مبهم‌سازی حملات تک‌مرحله‌ای

| ردیف | Lc | Lo | فن مبهم‌سازی | نتیجه (برحسب لگاریتم) |
|---|---|---|---|---|
| ۱ | ۴۰ | ۴۰ | حمله نویز | طبقه‌بندی درست حملات برابر ۰/۲۲- $L_N$ =۱۰<br>طبقه‌بندی درست حملات برابر۰/۲- $L_N$ =۲۰<br>طبقه‌بندی درست حملات برابر۰/۱۸- $L_N$ =۳۰<br>طبقه‌بندی درست حملات برابر۰/۱۸- $L_N$ =۴۰ |
| ۲ | ۴۰ | ۴۰ | حمله پاک | طبقه‌بندی درست حملات برابر۰/۰۹- $L_C$ =۱۰<br>طبقه‌بندی درست حملات برابر۰/۰۵- $L_C$ =۲۰<br>طبقه‌بندی درست حملات برابر۰/۰۳- $L_C$ =۳۰<br>طبقه‌بندی درست حملات برابر۰/۰۲- $L_C$ =۳۰ |
| ۳ | ۲۰ | ۴۰ | اضافه حمله | طبقه‌بندی درست حملات برابر۱/۰۸- $L_o$ =۱۰<br>طبقه‌بندی درست حملات برابر۳/۶- $L_o$ =۲۰<br>طبقه‌بندی درست حملات برابر۴/۸۸- $L_o$ =۳۰<br>طبقه‌بندی درست حملات برابر ۶/۷۴ - $L_o$ =۴۰ |
| ۴ | ۴۰ | ۲۰ | حذف حمله | طبقه‌بندی درست حملات برابر ۰/۱۷- $L_o$ =۱۰<br>طبقه‌بندی درست حملات برابر۰/۹۵- $L_o$ = ۲۰<br>طبقه‌بندی درست حملات برابر۸/ ۱- $L_o$ =۳۰<br>طبقه‌بندی درست حملات برابر۲/۶ - $L_o$ =۴۰ |
| ۵ | ۴۰ | ۴۰ | جایگزین حمله | طبقه‌بندی درست حملات برابر /۶۵- $L_o$ =۱۰<br>طبقه‌بندی درست حملات برابر ۱/۸- $L_o$ =۲۰<br>طبقه‌بندی درست حملات برابر ۲/۴- $L_o$ =۳۰<br>طبقه‌بندی درست حملات برابر۳ - $L_o$ =۴۰ |




**نمودار (۱):** مقایسه دقت مبهم‌سازی مدل پیشنهادی برای فنون مختلف با حملات پاک

همان‌طور که در نمودار (۱) مشاهده می‌گردد، دقت طبقه‌بند برای مدل‌های با نرخ مبهم‌سازی بیشتر، کمتر است چون هر چه دنباله حملات مبهم‌تر باشد، تشخیص آن توسط طبقه بند سخت‌تر است و باعث ایجاد خطا در سامانه‌های تشخیص نفوذ می‌شود. (سامانه‌های‌تشخیص نفوذ از طبقه‌بند برای مدل‌سازی و ذخیره‌سازی الگوهای حمله استفاده می‌کند، تا در صورت ورود حمله مشابه، آن حمله را با الگوهای حمله از قبل تعریف‌شده، که توسط طبقه‌بند به‌دست‌آمده‌اند، تطبیق داده و به‌عنوان نفوذ شناسایی کند). همان‌طور که در جدول (۲) ملاحظه می‌شود سامانه‌های تشخیص نفوذ حملات پاک را به‌خوبی تشخیص داده‌اند ولی با نویزی کردن دنباله حملات پاک، تشخیص حمله با خطا مواجه می‌شود ولی در طول دنباله ۴۰ سامانه‌های تشخیص نفوذ به‌خوبی حملات را خوشه‌بندی می‌کنند و اثر نویزی را خنثی می‌کنند ولی با فنون مبهم‌سازی پیشنهادی با روش حمله متناظر، مبهم‌سازی دنباله حملات به‌درستی انجام شده و طبقه‌بندی درست حملات توسط سامانه‌های تشخیص نفوذ به سمت صفر میل کرده و در تشخیص حمله با خطای خیلی زیاد مواجه می‌شوند. لذا با روش پیشنهادی می‌توان چالش افزایش ذنباله حمله، را برطرف کرد.

## ۵- بررسی مدل پیشنهادی

برای بررسی درستی‌یابی[1] مدل پیشنهادی از روش صوری استفاده می‌کنیم، با توجه به تعاریف بیان‌شده و بهره‌گیری از سه فن مختلف مبهم‌سازی برای مخفی کردن دنباله حملات چندمرحله‌ای به اثبات قضایا و گزاره‌ها می‌پردازیم.

همچنین برای اثبات اعتبارسنجی[2] مدل پیشنهادی می‌توان به حملات راهبردی انجام شده مانند: رجین[3]، استاکس نت[4] اشاره کرد.

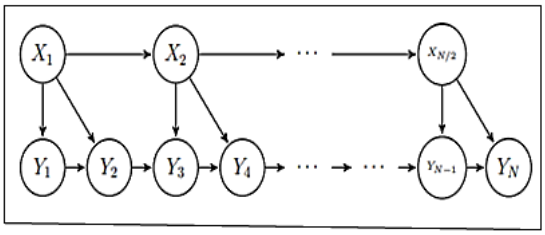
[1] Verification
[2] Validation
[3] Rogin
[4] Stux Net

**لم[1] ۱:** اگر مهاجم حملات خود را با فن افزایش حمله، مبهم‌سازی کند، آنگاه احتمال موفقیت وی افزایش می‌یابد.

**اثبات:**

فرض کنید $X=\{X_1,X_2,\ldots,X_{N/2}\}$ بردار دنباله حملات پاک و $Y=\{y_1,y_2,\ldots,y_N\}$ بردار دنباله حملات مبهم شده توسط فن افزایش حمله باشد، بنابراین، طبق شکل (۴) باید نشان دهیم:

$$P^c(Y|X) > P^O(Y|X)$$



**شکل (۴):** مدل دنباله حمله مبهم با فن افزایش حمله.

در این مدل حمله مبهم $Y_i$ به حمله مبهم قبلی خود یعنی $Y_{i-1}$ و حمله پاک $X_{i-1}$ وابسته خواهد بود. با توجه به سازگاری و ارتباط حملات مبهم با حملات پاک داریم:

$$P^O(Y|X) = P(Y_1|X_1)P(Y_2|Y_1,X_1)\prod_{i=1}^{\frac{N}{2}} P(Y_{2i-1}|Y_{2i-2},X_i)\ P(Y_{2i}|Y_{2i-1},X_i) \qquad (۱۵)$$

چون هر حمله X دارای چند اقدام اثرگذاری بر موجودیت‌های قربانی است و برخی از این اقدام‌های اثرگذار با حمله دیگر مشترک(مشابه) هستند لذا:

$$P^O(Y2i-1|Y2i-2 \cap Xi) = (P(Y2i-1 \cap Y_{2i-1} \cap Xi))/(P(Y2i-1 \cap Xi))$$
$$= \frac{n(Y2i-1 \cap (Y2i-2 \cap Xi))/n(s)}{n(Y2i-2 \cap Xi)/n(s)} \qquad (۱۶)$$

$$= \frac{n(Y2i-1 \cap (Y2i-2 \cap Xi))}{n(Y2i-2 \cap Xi)}$$

$$P^O(Y2i|Y2i-1,Xi) = \frac{P(Y2i \cap (Y2i-1 \cap Xi))}{P(Y2i-1 \cap Xi)} \qquad (۱۷)$$

$$= \frac{n(Y2i \cap (Y2i-1 \cap Xi))/n(s)}{n(Y2i-1 \cap Xi)/n(s)}$$

$$= \frac{n(Y_{2i} \cap Y_{2i-1} \cap Xi)}{n(Y_{2i-1} \cap Xi)}$$

مخرج کسر رابطه $P(Y_{2i}|Y_{2i-1} \cap X_i)$ ، از اجتماع تعداد اقدامات $x_i$ و $y_{2i-1}$ از یک گروه و صورت کسر، اشتراک تعداد گام‌های(اقدامات) $y_{2i}$ با اجتماع تعداد گام‌های $x_i$ و $y_{2i-1}$ است. به همین ترتیب برای رابطه‌ی $P(Y_{2i}|Y_{2i-1} \cap X_i)$ 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 شناسه‌ی حمله‌ی 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 حمله‌ی 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 دنباله‌ی حمله، از رابطه کلی (۱۸) محاسبه می‌شود:

$$P^O(Yi|Xi) = \frac{P(Yi \cap Xi)}{P(Xi)} = \frac{n(Yi \cap Xi)/n(s)}{n(Xi)/n(r)} = \frac{n(Yi \cap Xi)n(r)}{n(Xi)n(s)} \qquad (۱۸)$$

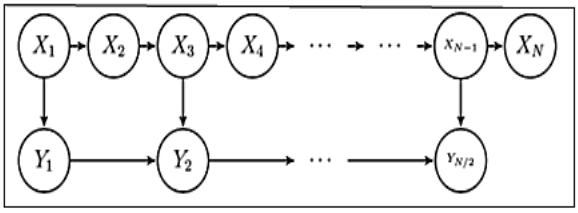
در رابطه مذکور $n(s)$ تعداد کل اقدامات دنباله حمله پاک و $n(r)$ تعداد کل اقدامات دنباله حملات مبهم است. با توجه به ثابت بودن مخرج کسر(تعداد حملات پاک) مدافع سعی دارد تعداد شباهت‌ها بین **Y** و **X** را تشخیص دهد که هر چه شباهت‌ها کمتر باشد شانس تشخیص مبهم‌سازی مدافع کاهش می‌یابد و درنتیجه احتمال موفقیت مهاجم افزایش می‌یابد.

**لم ۲:** اگر مهاجم حملات خودش را با فن حذف حمله، مبهم‌سازی کند، آنگاه احتمال موفقیت وی افزایش می‌یابد.

**اثبات:**

اگر $X=\{X_1,X_2,\ldots,X_N\}$ بردار دنباله حملات پاک و $Y=\{y_1,y_2,\ldots,Y_{N/2}\}$ بردار دنباله حملات مبهم شده توسط فن حذف حمله باشد، بنابراین، طبق شکل(۵) باید نشان دهیم:

$$P^c(Y|X) > P^O(Y|X)$$



**شکل (۵):** نمایش مدل گرافیکی ۲ برای حذف حمله.

[1] lemma

در این مدل حمله مبهم $Y_i$ به حمله مبهم قبلی خود یعنی $Y_{i-1}$ وابسته خواهد بود، لذا با توجه به سازگاری و ارتباط حملات مبهم با حملات پاک داریم :

$$P^o(Y|X) = P(X_1)P(Y_1|X_1)\ P(\ (X_1)\prod_{i-1}^{N-1} P(X_{i+1} + 1|\ Xi)(P(Y_1|\ X_1, X_2)\prod_{i-2}^{\frac{N}{2}} P(Yi|\ Y_{i-1}, X_{2i-1}, X2i) \prod_{i-1}^{N-1} P(Y_{i+1}|\ Yi))\ (۱۹)$$

$$P^o(Y_i|X_i, X_{i+1}) = \frac{P(Yi \cap (Xi \cap Xi+1))}{P(Xi \cap Xi+1)} = \frac{n(Yi \cap (Xi \cap Xi+1))/n(s)}{n(Xi \cap Xi+1)/n(r)}$$

$$= \frac{n(Yi \cap (Xi \cap xi+1)n(r)}{n(Xi \cap xi+1)n(s)} \qquad (۲۰)$$

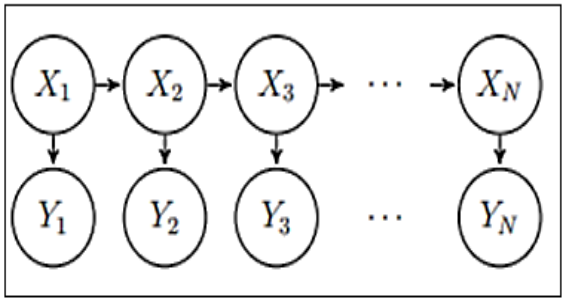
ملاحظه می‌گردد هر چه مهاجم بتواند تعداد شباهت بین حملات $\{Yi \cap (Xi \cap X_{i+1})\}$ را کاهش دهد، احتمال مبهم‌سازی $P^o(Y|X)$ کاهش می‌یابد . لذا با کاهش احتمال مبهم‌سازی در دنباله حملات، شانس تشخیص حمله توسط مدافعین امنیتی سخت‌تر خواهد شد و درنتیجه احتمال موفقیت مهاجم P(E) افزایش می‌یابد.

**لم ۳:** اگر مهاجم حملات خود را با فن حذف حمله، مبهم‌سازی کند، آنگاه احتمال موفقیت وی افزایش می‌یابد.

**اثبات:**

اگر $X=\{X_1,X_2,...,X_N\}$ بردار دنباله حملات پاک و $Y=\{Y_1,Y_2,....Y_N\}$ بردار دنباله حملات مبهم شده توسط فن حذف حمله باشد، بنابراین طبق شکل (۶) باید نشان دهیم:

$$P^c(Y|X) > P^o(Y|X)$$




**شکل(۶):** مدل مخفی مارکوف برای فن جایگزین حمله

در این مدل حمله مبهم $Y_i$ به حمله مبهم قبلی خود یعنی $Y_{i-1}$ وابسته نخواهد بود و فقط به حمله پاک $X_i$ وابستگی دارد، لذا با توجه به سازگاری و ارتباط حملات مبهم با حملات پاک داریم :

$$P^o(Y|X) = \frac{n(Yi \cap (Yi \cap Xi)n(r)}{n(Yi \cap Xi)n(s)} \qquad (۲۱)$$

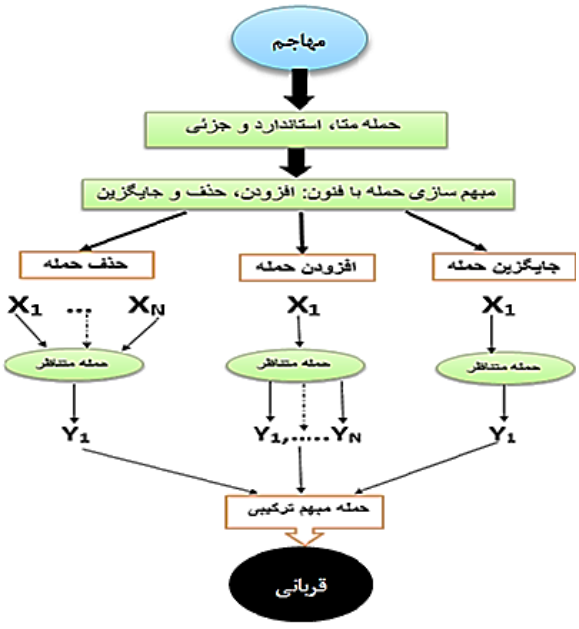
در این فن مانند دو فن قبلی مبهم‌سازی ملاحظه می‌گردد هر چه مهاجم بتواند تعداد شباهت بین حملات $Yi \cap (Yi \cap Xi)$ را کاهش دهد، احتمال مبهم‌سازی $P^o(Y|X)$ کاهش می‌یابد. لذا با کاهش احتمال مبهم‌سازی در دنباله حملات، احتمال تشخیص حمله توسط مدافعین امنیت شبکه سخت‌تر خواهد شد و درنتیجه شانس موفقیت مهاجم P(E) افزایش می‌یابد.

**قضیه ۱:** اگر مهاجم در دنباله حملاتش از فنون مبهم‌سازی استفاده کند آنگاه احتمال موفقیت وی افزایش می‌یابد.

**اثبات:**

اگر $E^c=\{E_1^c, E_2^c,..., E_N^c\}$ بردار دنباله مجموعه حملات پاک برای حملات تک‌مرحله‌ای و $E^o=\{E_1^o, E_2^o,..., E_N^o\}$ بردار دنباله مجموعه حملات مبهم شده توسط سه فن حذف، اضافه و جایگزین حمله برای حملات تک‌مرحله‌ای باشد، بنابراین طبق شکل (۷) باید نشان دهیم:

$$P(E_i^o) \geq P(E_i^c)$$




**شکل (۷):** مدل‌سازی احتمالی دنباله حملات مبهم

با توجه به برهان‌های کمکی ۱ و ۲ و ۳ برای مبهم‌سازی حملات سایبری اثبات گردید:

رابطه شرطی $\frac{P(Yi \cap Xi)}{P(Xi)}$ اثرگذاری یکسانی برای فنون مختلف مبهم‌سازی دارد لذا با توجه به ثابت بودن مخرج کسر (تعداد حملات پاک) مدافع سعی دارد تعداد شباهت‌ها بین

**Y** و **X** را تشخیص دهد که هر چه شباهت‌ها کمتر باشد شانس تشخیص مبهم‌سازی مدافع کاهش می‌یابد و درنتیجه احتمال موفقیت مهاجم افزایش می‌یابد.

**لم ۴:** اگر مهاجم حملات خود را به‌صورت مرحله‌ای اجرا کند آنگاه احتمال موفقیت وی بیشتر می‌گردد.

**اثبات:**

اگر E مجموعه تمام راه‌کارها و $E_i$ راه‌کار i–ام باشد که:

$$E=\bigcup_{i=1}^{n} E_i = E_1 \cup E_2 \cup \dots \cup E_n \qquad (۲۲)$$

بنابراین، باید نشان دهیم:

$$P(E) \geq P(E_i)$$

چون $E_i \subseteq E = \bigcup_{i=1}^{n} E_i$ درنتیجه داریم:

$$P(E_i) \leq P(E)$$

**قضیه ۲:**

اگر مهاجم در دنباله حملاتش از حملات چندمرحله‌ای مبهم استفاده کند آنگاه احتمال موفقیت وی بیشتر است.

**اثبات:**

فرض کنید $E_i^c$ مجموعه راه‌کارها برای حملات تک‌مرحله‌ای پاک باشد و E مجموعه راه‌کارهای حملات چندمرحله‌ای پاک و مبهم باشد. بنابراین، باید نشان دهیم:

$$P(E_i^c) \leq P(E)$$

با توجه به قضیه ۱ و لم ۴ برای حملات سایبری داریم:

$$P(E_i^c) \leq P(E_i^o)$$

همچنین

$$P(E_i^o) \leq P(E_i)$$

چون

$$P(E) = \sum_{i=1}^{\infty} P(E_i)$$

و

$$E_i \subseteq E$$

درنتیجه:

$$P(E_i^c) \leq P(E)$$

## ۶- نتیجه‌گیری

با طراحی مراحل مختلف حمله در حملات چندمرحله‌ای، می‌توان همبستگی بین دنباله حملات مشاهده‌شده را کاهش داد؛ درنتیجه باعث کمتر شدن دقت طبقه‌بندی حملات توسط سامانه‌های تشخیص نفوذ گردید و همچنین این‌که با انجام مبهم‌سازی ترکیبی در مراحل حمله باعث سخت‌تر شدن تشخیص حملات گردید. به‌این‌ترتیب با ارایه مدل احتمال پیشنهادی حملات چند مرحله‌ای نشان داده شده که اثر مبهم‌سازی در دنباله و مراحل حملات با اجرای چندمرحله‌ای حملات هم‌افزا شده و مدل حمله را برای مدافعین شبکه پیچیده و سخت‌تر خواهد کرد.

## ۷- مراجع


[1] F. Iserhani, et al., “MARS: multi-stage attack recognition system,” in 24th IEEE International Conference on Advanced Information Networking and Applications, 2010.

[2] S. T. Eckmann, G. Vigna, and R. A. Kemmerer, “STATL: An attack language for state-based intrusion detection,” Journal of computer security, pp. 71-103, 2002.

[3] K. K. Thompson, “Not like an Egyptian: Cybersecurity and the Internet kill switch debate,” p. 465, 2011.

[4] P. Disso and F. Jules, “A novel intrusion detection system (IDS) architecture,” Attack detection based on snort for multistage attack scenarios in a multi-cores environment, University of Bradford, 2011.

[5] S. Noel and S. Jajodia, “Optimal ids sensor placement and alert prioritization using attack graphs,” Journal of Network and Systems Management, pp. 259-275, 2008.

[6] H. Du, “Probabilistic Modeling and Inference for Obfuscated Network Attack Sequences,” 2014.

[7] H. Du and S. J. Yang, “Sequential modeling for obfuscated network attack action sequences,” in IEEE Conference on Communications and Network Security (CNS), 2013.

[8] R.Goyal, et al., “Obfuscation of stuxnet and flame malware. Latest Trends in Applied Informatics and Computing,” pp. 150-154, 2012.

[9] S. Andersson, A. J. Clark, and G. M. Mohay, “Detecting network-based obfuscated code injection attacks using sandboxing,” 2005.

[10] B. Barak, et al., “On the (im) possibility of obfuscating programs. Journal of the ACM (JACM),” 2012.

[11] 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 Persion).

[12] D. M. Farid and M. Z. Rahman, “Attribute weighting with adaptive NBTree for reducing false positives in intrusion detection,” 2010.

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

[14] 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 Persion).

[15] 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 Persion).

[16] 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 Persion).

**Journal of Electronical & Cyber Defence**
**Vol. 8, No. 2, 2020, Serial No. 30**

# Probabilistic Modeling of Obfuscated Multi- Stage cyber Attacks

K. Shoushian, A. J. Rashidi*, A. R. Mirghadri

*Malek Ashtar University of Technology

(Received: 12/06/2019, Accepted: 23/10/2019)

**ABSTRACT**

*One of the most important threats for computer systems and cyber space in recent years are cyber attacks, particularly the emerging obfuscated cyber attacks. Obfuscation at the attack level means change of attack, without change in the behavior and type of impact of attack on the victim. So the highlighted problems are the complexity and ambiguity of these attacks and the difficulty in detecting and issueing alarms on time. This paper suggests the acquisition and deployment of a new model of multi - stage cyber - attacks that enables network security defenders to create a deterrent to enemies in addition to timely diagnosis of cyber attacks. Using this model of attack to multi stage and obfuscate attacks, the attacker can imply false classification in the attack sequence and break the dependence between the attack warnings, actions,steps and strategies, thus making changes in the sequence of attacks. As a result, network security managers cannot easily recognize the ultimate goal of the attacker. To assess the presented model, we have used the Bayesian algorithm.The results of the research and implementation of the model indicate that the accuracy of classification (in terms of log) for the best case of clean attacks is -0.04 whilst for multi-stage obfuscate attacks it reduces to -35. This indicates that the proposed model for multi - stage obfuscate cyber attacks is more efficient than the obfuscate logic of single - stage attacks, because of the ability to deceive intrusion detection systems and make uncertainties in penetration warnings.*

**Keywords:** Probabilistic Modeling, Cyber Attacks, Multi – Stage, Attacks Obfuscation, Attack Sequence

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