مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۳، پاییز ۱۳۹۷، ص ۳۴-۱۳

چارچوبی آینده‌نگر برای سامانه‌های پاسخ به نفوذ در شبکه‌های رایانه‌ای

محمد قاسمی‌گل
استادیار، گروه مهندسی کامپیوتر، دانشگاه بیرجند، بیرجند
(دریافت: ۹۵/۱۲/۲۲، پذیرش: ۹۶/۰۸/۱۰)

چکیده

امروزه افزایش هشدارهای صادرشده توسط سامانه‌های محافظ امنیت منجر به بروز چالش جدیدی برای مدیران امنیت شبکه شده است. اصولاً مدیریت و پاسخگویی به این حجم زیاد هشدارها کار دشواری است. از این‌رو، مدیریت هشدار و سامانه پاسخ را می‌توان به عنوان اساسی‌ترین بخش‌های سامانه‌های محافظ امنیت از جمله سامانه‌های تشخیص نفوذ در نظر گرفت. در سال‌های اخیر، بیشتر تحقیقات صورت‌گرفته به طور مجزا به بحث مدیریت هشدار و سامانه پاسخ پرداخته‌اند، درحالی‌که این دو بخش لازم و ملزوم یکدیگر هستند و عملکردشان بر روی یکدیگر تأثیرگذار است. بخش مدیریت هشدارها بایستی به گونه‌ای طراحی شود که اطلاعات لازم در مورد حملات رخ داده را متناسب با نوع سامانه پاسخ در اختیار آن قرار دهد. این اطلاعات به همراه اطلاعات مستخرج از منابع شبکه، وضعیت فعلی شبکه را برای سامانه پاسخ ترسیم می‌کنند. با این‌حال، چنانچه تصمیمات اتخاذشده در سامانه پاسخ تنها براساس اطلاعات وضعیت فعلی شبکه باشد، مجموع هزینه‌های شبکه در طول زمان افزایش می‌یابد. از این‌رو، می‌توان با کمک مفهوم آینده‌نگری از کلیه اطلاعات موجود و قابل دسترس برای شناسایی وضعیت فعلی شبکه و کلیه وضعیت‌های پیش رو استفاده نمود و فرآیند تصمیم‌گیری در سامانه پاسخ را با این نگاه بهبود بخشید. در این مقاله هدف ما ارائه یک رویکرد آینده‌نگر جهت یافتن پاسخ‌های بهینه برای مقابله با حملات رخ داده و حملات محتمل آینده است. برای این منظور معماری پیشنهادی شامل دو بخش کلی ۱) مدل‌سازی هشدارها و حملات و ۲) مدل‌سازی پاسخ می‌باشد. در بخش نخست با تحلیل هشدارهای مستخرج از سامانه‌های تشخیص نفوذ سعی کرده‌ایم ورودی مناسب برای سامانه پاسخ خودکار فراهم شود. همچنین به منظور پیش‌بینی حملات آینده روش‌هایی جهت تحلیل حملات به صورت پویا ارائه شده است تا از این طریق، انتخاب پاسخ مناسب با دید آینده‌نگر انجام گیرد. در بخش دوم نیز ابتدا با ارائه یک مدل بازنمایی مناسب به تحلیل مجموعه پاسخ‌ها پرداخته‌ایم. سپس با بررسی شرایط فعلی و آتی شبکه، هزینه‌ها و سودمندی‌های هر پاسخ به طور دقیق محاسبه شده است. درنهایت، مدل‌هایی جهت انتخاب پاسخ‌های مناسب با کمک روش‌های تصمیم‌سازی ارائه شده است. نتایج حاصل از شبیه‌سازی با سناریوهای مختلف نشان می‌دهد با کمک آینده‌نگری در سامانه پاسخ می‌توان هزینه‌های ناشی از وقوع حمله به شبکه و اعمال پاسخ را تا حد زیادی کاهش داد و شبکه را به سوی وضعیت‌هایی با هزینه کم هدایت نمود.

کلید واژه‌ها: سامانه پاسخ به نفوذ، آینده‌نگری، مدیریت هشدار، گراف حمله آگاه به عدم قطعیت، گراف وابستگی‌های شبکه، فرآیند تصمیم‌سازی مارکوف.

۱- مقدمه

امروزه افزایش هشدارهای صادرشده توسط ابزارهای محافظ شبکه منجر به بروز چالش‌های جدیدی برای مدیران امنیت شبکه شده است. اصولاً بررسی و پاسخگویی به این حجم زیاد هشدارها کار دشواری است. در راستای مواجهه با این چالش، بخش عمده‌ای از تحقیقات صورت‌گرفته به‌دنبال ارائه روش‌های مختلفی جهت مدیریت هشدارها هستند تا از این طریق حجم هشدارهای صادرشده را کاهش دهند. با این‌حال، همچنان شیوه پاسخگویی به حملات شناسایی‌شده، امر دشواری است و در بیشتر سامانه‌های تشخیص نفوذ شناخته‌شده سامانه پاسخ دستی مورد استفاده قرار می‌گیرد [۱].

از این‌رو، در دو دهه اخیر تلاش‌هایی جهت ارائه سامانه‌های پاسخ به نفوذ خودکار به‌عنوان یکی از بخش‌های اساسی سامانه‌های محافظ امنیت صورت گرفته است. وظیفه اصلی این سامانه‌ها اعمال پاسخ‌های مناسب در مقابل حملات شناسایی شده است. به‌گونه‌ای که یا مانع از وقوع حمله شود و یا با استفاده از فنون مناسب خسارت ناشی از حمله را تا حد امکان کاهش دهد و

* رایانامه نویسنده مسئول: ghasemigol@birjand.ac.ir

شبکه را به وضعیت قبل حمله بازگرداند. هشدارهای صادرشده، ورودی اصلی سامانه‌های پاسخ به نفوذ هستند و خروجی آن‌ها نیز زیرمجموعه‌ای از پاسخ‌های مناسب انتخاب‌شده می‌باشد. از آن‌جایی‌که اعمال هر پاسخ هزینه‌هایی را به منابع و سرویس‌های شبکه تحمیل می‌کند، هدف یافتن پاسخ‌هایی است که هزینه کمتری را در پی داشته باشند.

در این‌جا فرض می‌کنیم بر روی یک شبکه مجموعه‌ای از گره‌ها وجود دارند که با یکدیگر در ارتباط بوده و در هر یک از آن‌ها تعدادی آسیب‌پذیری موجود است. همچنین، در این شبکه حملات مختلفی می‌توانند به‌طور همزمان شکل گرفته به‌طوری‌که هر حمله یک دامنه فعالیت (تخریب) مشخصی دارد. از سوی دیگر، مجموعه‌ای از پاسخ‌ها توسط مسئول شبکه طراحی شده که هر کدام از این پاسخ‌ها بر روی بخشی از شبکه تاثیرگذار خواهند بود. محدوده اجرایی هر حمله و یا هر پاسخ شامل بخشی از منابع موجود در گره‌های مختلف شبکه است. با بهره‌برداری از آسیب‌پذیری‌های موجود در گره‌های مختلف شبکه حملات شکل خواهند گرفت. همچنین، پاسخ‌ها نیز برای مقابله با حملات موجود و یا محتمل بر روی گره‌های شبکه مورد استفاده قرار می‌گیرند و در مواردی منجر به افزودن هزینه اضافی بر منابع شبکه و کاربران خواهند شد. بر این اساس، شرایط زیر بر فضای مسئله حاکم خواهد بود:

- شبکه حاوی مجموعه‌ای از گره‌هاست.
- در هر گره تعدادی آسیب‌پذیری شناسایی شده وجود دارد. براساس این آسیب‌پذیری‌ها حملات محتمل بر روی شبکه با کمک گراف حمله قابل شناسایی است.
- هر حمله می‌تواند با احتمالی مشخص زیرمجموعه‌ای از آسیب‌پذیری‌های شبکه را مورد بهره‌برداری قرار دهد.
- در پی وقوع هر حمله یک یا مجموعه‌ای از هشدارها توسط سامانه تشخیص نفوذ صادر می‌شود.
- در پی وقوع حمله میزان مشخصی خسارت به بخشی از شبکه تحمیل خواهد شد.
- مجموعه‌ای از پاسخ‌های ممکن توسط مدیر شبکه تعریف می‌شود.
- هر پاسخ توانایی برطرف‌نمودن زیرمجموعه‌ای از حملات شبکه را دارد، درحالی‌که هزینه‌ای را به برخی از منابع و کاربران شبکه تحمیل می‌کند.
- هر یک از گره‌ها و منابع مختلف شبکه اهمیت خاص خود را دارند.
- هزینه پاسخ و میزان خسارت حمله می‌تواند متأثر از پارامترهای زیادی مانند شرایط شبکه، تعداد کاربران و نوع منابع باشند.

حال هدف فعال‌کردن و یا غیرفعال‌کردن زیرمجموعه بهینه‌ای از پاسخ‌ها در وضعیت فعلی است که با درنظرگرفتن حملات رخ داده شده، حملات محتمل آینده و هزینه پاسخ‌های فعال، منجر به کاهش هزینه‌های شبکه در یک بازه زمانی مشخص شود. به‌عبارت دیگر، به دنبال پاسخ‌هایی هستیم که هزینه‌های شبکه را با دید آینده‌نگر کاهش دهند. از این‌رو، نوآوری اصلی این تحقیق ارائه یک مدل پاسخ حساس به هزینه و آینده‌نگر برای سامانه‌های تشخیص نفوذ به منظور یافتن پاسخ‌های مناسب برای مقابله با حملات رخ داده و حملات محتمل آینده است. در این مدل به وابستگی‌ها و ارتباطات میان هشدارها و ارتباطات میان پاسخ‌ها توجه شده است. همچنین، به کمک این مدل می‌توان بهترین پاسخ‌های ممکن را در هر لحظه با توجه به وضعیت جاری شبکه و وضعیت‌های آتی آن شناسایی نمود.

ساختار این مقاله به شرح ذیل است: در بخش دوم به بررسی مختصر روش‌های مدیریت هشدار پرداخته می‌شود. در بخش سوم سامانه‌های پاسخ به نفوذ را از جنبه‌های مختلف بررسی می‌شود. در بخش چهارم روش‌های تحلیل حملات شبکه بیان شده است. معماری پیشنهادی برای چارچوب پاسخ آینده‌نگر در بخش پنجم به طور مشروح بررسی می‌شود. در بخش ششم نتایج شبیه‌سازی رویکرد پیشنهادی مورد بررسی و تحلیل قرار گرفته‌اند. در بخش انتهایی مقاله جمع‌بندی نتایج به‌دست‌آمده از این تحقیق و فهرست کارهای پیشنهادی برای ادامه آن بیان شده است.

۲- مدیریت هشدارها

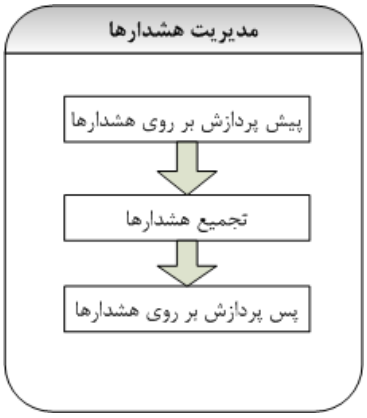
مدیریت هشدارها دربرگیرنده مجموعه اقدامات لازم جهت مدیریت حجم زیادی از هشدارها است که منجر به تجمیع آن‌ها می‌شود و در عین حال، هشدارهای تجمیع‌شده با ایجاد یک نمای سطح بالا از وضعیت امنیتی شبکه تحت نظارت، اطلاعات بهتری را در زمینه حملات صورت‌گرفته در اختیار مدیر شبکه قرار می‌دهد [۲]. همان‌طور که در شکل (۱) نمایش داده شده است، سامانه مدیریت هشدارها شامل بخش‌های زیر است:

- پیش‌پردازش هشدارها: اولین کار در این راستا یکسان‌نمودن فرمت هشدارهایی است که توسط حسگرهای مختلف شناسایی شده‌اند. در سامانه‌های تشخیص نفوذ این کار با استفاده از پیام‌هایی با فرمت استاندارد انجام می‌گیرد (IDMEF[1]) [۳].
- تجمیع و هم‌بسته‌سازی هشدارها: هدف از این بخش شناسایی هشدارهای مشابه و یافتن روابط بین هشدارها

1- Intrusion Detection Message Exchange Format

است تا از این طریق بتوان تعداد هشدارهای صادرشده را کاهش داد و بررسی آن‌ها را تسهیل نمود [۴].

- پس‌پردازش هشدارها: که شامل اولویت‌دهی به هشدارهای تجمیع شده است [۶-۵].



شکل (۱): بخش‌های مختلف یک سامانه مدیریت هشدار [۲].

۳- سامانه پاسخ

با افزایش شمار حملات و هشدارهای صادرشده، اعمال پاسخ دستی توسط مدیران امنیتی شبکه بسیار دشوار است. از این‌رو، تلاش‌های زیادی برای ارائه سامانه‌های پاسخ به نفوذ خودکار صورت گرفته است. با این وجود، به‌دلیل امکان بروز خطا و اعمال پاسخ‌های نامناسب، همچنان در بیشتر سامانه‌های تشخیص نفوذ شناخته‌شده سامانه پاسخ دستی مورد استفاده قرار می‌گیرد [۱]. انتخاب پاسخ‌های مناسب به عوامل فراوانی مرتبط است که بایستی مورد توجه قرار گیرند. به‌طوری‌که علاوه‌بر مجموعه پاسخ‌ها و حملات صورت‌گرفته بایستی به جنبه‌های دیگری از فضای مسئله نیز توجه نمود. در ادامه این بخش با سامانه‌های پاسخ به نفوذ پیشین و چالش‌های موجود در آن‌ها آشنا خواهیم شد.

در حوزه سامانه پاسخ، دسته‌بندی‌های مختلفی ارائه شده است [۹-۷]. در سال ۱۹۹۶ میلادی اولین دسته‌بندی سامانه‌های پاسخ تحت عنوان Fisch DC&A ارائه شد که در آن پاسخ را در دو حوزه بررسی کرده بود:

۱) زمان تشخیص : قبل از وقوع حمله یا پس از وقوع حمله
۲) هدف پاسخ : کنترل خسارت به صورت فعال، کنترل خسارت به صورت غیرفعال، بررسی خسارت و ترمیم خسارت

در سال ۲۰۰۴ دسته‌بندی دیگری در زمینه سامانه‌های پاسخ و ترمیم ارائه شد که براساس آن دسته‌های مختلف پاسخ به شرح زیر است [۱۰]:

- بازگشت به آخرین وضعیت امن قبلی[۱]
- رفتن به اولین وضعیت امن بعدی[۲]
- حصر جزء معیوب[۳]
- پیکربندی مجدد[۴]
- بازگشت به وضعیت اولیه[۵]

Wang و همکارانش نیز در دسته‌بندی نسبتاً متفاوتی که 5W2H نام گرفت، سامانه پاسخ را در ۷ بعد بررسی نموده اند [۱۱]:

۱) بعد زمان[۶]
۲) پتانسیل تخریب[۷]
۳) مکان حمله‌کننده[۸]
۴) نوع حمله[۹]
۵) هدف حمله[۱۰]
۶) نوع حمله‌کننده[۱۱]
۷) نقشه حمله[۱۲]

مشهورترین دسته‌بندی ارائه‌شده از سامانه‌های پاسخ توسط Stakhanova در سال ۲۰۰۷ میلادی مطرح شد و از آن به بعد در بسیاری از منابع مبنای مقایسه سامانه‌های پاسخ قرار گرفته است [۱]. شکل (۲) دسته‌بندی انواع سامانه‌های پاسخ را از دیدگاه‌های مختلف نشان می‌دهد. براساس این دسته‌بندی ارائه‌شده از دیدگاه میزان خودکارسازی، سامانه‌های پاسخ را می‌توان به سه دسته زیر تقسیم بندی نمود:

۱) سامانه‌های اخطار دهنده[۱۳]: هدف سامانه‌های اخطاردهنده ارائه اطلاعات نفوذ به مدیر شبکه است تا به کمک آن پاسخ‌های مناسب را انتخاب کند. اصولاً این سامانه‌ها هنگام تشخیص حمله هشدارهایی صادر می‌کنند که شامل اطلاعات مربوط به حمله مانند نوع حمله، زمان حمله، IP مبدأ، IP مقصد، نوع پروتکل و ... می‌باشند. بیشتر سامانه‌های پاسخ بر این مبنا کار می‌کنند. بزرگترین مشکل این روش تأخیر بین حمله و اعمال پاسخ از سوی مدیر شبکه است.
۲) سامانه‌های پاسخ دستی[۱۴]: سامانه‌های پاسخ دستی سطح بالاتری از خودکارسازی را نسبت به سامانه‌های اخطاردهنده

1- Rollback
2- Rollforward
3- Isolation
4- Reconfiguration
5- Reinitialization
6- When (as a dimension of time)
7- How serious (potential of destruction)
8- Where (location of attacker)
9- How (type of attack)
10- What (a target or victim)
11- What (type of attacker)
12- Why (plan of attack)
13- Notification systems
14- Manual response systems

فراهم می‌کنند. این سامانه‌ها به مدیر شبکه امکان می‌دهند که براساس اطلاعات حمله از میان مجموعه پاسخ‌های از پیش تعریف‌شده یکی را انتخاب کند.

۳) سامانه‌های پاسخ خودکار[1]: برخلاف دو مورد قبلی، سامانه‌های پاسخ خودکار امکان اعمال پاسخ‌های فوری را با استفاده از یک فرآیند تصمیم‌سازی خودکار فراهم می‌کنند. با وجود این‌که امروزه بیشتر سامانه‌های تشخیص به صورت خودکار عمل می کنند، اما هنوز سامانه‌های پاسخ خودکار بسیار محدودی وجود دارد. بزرگترین مشکل این سامانه‌ها این است که در آن‌ها احتمال اعمال پاسخ‌های نامناسب وجود دارد.

از دیدگاه نوع اعمال پاسخ، سامانه‌های پاسخ در دو دسته زیر تقسیم‌بندی می‌شوند:

۱) سامانه‌های پاسخ غیرفعال[2]: در سامانه‌های پاسخ غیرفعال هیچ تلاشی برای کاهش میزان خسارت حمله و یا جلوگیری از حملات بیشتر صورت نمی‌گیرد. هدف اصلی این سامانه‌ها آگاهی‌دادن به مدیر شبکه در مورد اطلاعات حمله است. بیشتر سامانه‌های پاسخ به‌صورت غیرفعال کار می‌کنند.

۲) سامانه‌های پاسخ فعال[3]: سامانه‌های پاسخ فعال برخلاف سامانه‌های پاسخ غیرفعال به‌دنبال کم‌کردن خسارت حمله و انجام پاسخ متقابل در برابر حمله‌کننده هستند.

از منظر توانایی سازگاری، سامانه‌های پاسخ را می‌توان به دو دسته زیر تقسیم‌بندی نمود:

۱) سامانه‌های پاسخ ایستا[4]: در بیشتر سامانه‌های پاسخ، شیوه انتخاب پاسخ در مدت حمله ثابت است و تغییر نمی‌کند. این سامانه‌ها بایستی به صورت دوره‌ای توسط مدیر شبکه ارتقاء یابند.

۲) سامانه‌های پاسخ تطبیقی[5]: توانایی انطباق‌پذیری سامانه‌های پاسخ بدین معنی است که شیوه انتخاب پاسخ به صورت پویا بوده و با توجه به تغییرات محیط در مدت حمله تنظیم می‌شود. این قابلیت انطباق می‌تواند به صورت‌های مختلف نمایش داده شود. به عنوان مثال، توجه به میزان موفقیت و اشتباه در پاسخ‌هایی که تاکنون توسط سامانه اعمال شده که ممکن است ناشی از عملکرد غلط سامانه تشخیص و یا انتخاب پاسخ‌های نامناسب توسط سامانه پاسخ باشد [۱۲].

1- Automatic Response Systems
2- Passive
3- Active
4- Static
5- Adaptive

از دید زمان پاسخ، سامانه‌های پاسخ در دو دسته زیر تقسیم‌بندی می‌شوند:

۱) پیشگویانه[6]: سامانه‌های پاسخ پیشگویانه به ما امکان پیش بینی حمله قبل از وقوع آن را می‌دهند. این پیشگویی عموماً دشوار بوده و مبتنی بر احتمالات و آنالیز کاربران فعلی و رفتار سامانه است [۱۲-۱۹]. سامانه‌های پاسخ پیشگویانه نیازمند ارتباط نزدیک شیوه تشخیص و شیوه پاسخ است به طوری‌که به محض تشخیص حمله پاسخ صادر شود. اگرچه پاسخ پیشگویانه یک ویژگی مطلوب برای مدیر شبکه است اما در هنگام اعمال پاسخ پیشگویانه، با توجه به اینکه درستی و صحت وقوع حمله تضمین نمی‌شود، ممکن است پاسخ‌های نامناسبی انتخاب شود.

۲) انفعالی[7]: اعمال پاسخ تا زمانی که وقوع حمله قطعی شود به تأخیر می‌افتد. معمولاً اطمینان لازم برای وقوع حمله از طریق تعیین معیارهای اطمینان برای سامانه تشخیص نفوذ و یا از طریق مطابقت کامل امضای حمله با شرایط موجود است. اگرچه بیشتر سامانه‌های پاسخ به صورت انفعالی عمل می‌کنند اما این روش برای کاربردهای حیاتی و حساس نمی‌تواند مورد استفاده قرار گیرد. در این روش زمان بیشتری در اختیار حمله کننده قرار می‌گیرد و به وی اجازه داده می‌شود خسارت بیشتری به سامانه وارد کند.

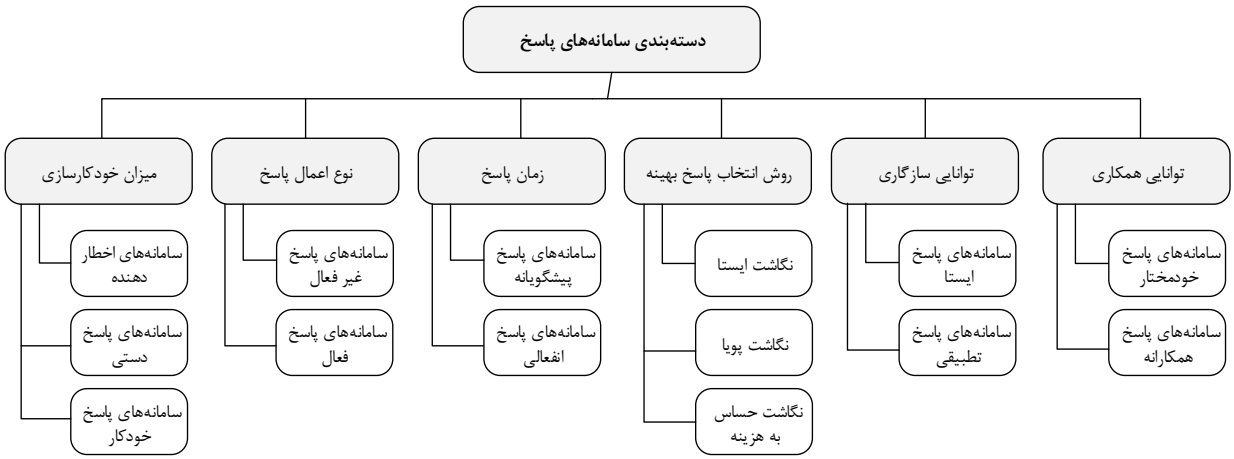
از جنبه توانایی همکاری، سامانه‌های پاسخ را می‌توان به دو دسته زیر تقسیم بندی نمود:

۱) سامانه‌های پاسخ خودمختار[8]: سامانه‌های پاسخ خودمختار به‌طور مستقل به بررسی یک نفوذ در سطح تشخیص داده شده می‌پردازند. به‌عنوان مثال، یک سامانه تشخیص نفوذ مبتنی بر میزبان در هنگام تشخیص یک نفوذ در سطح میزبان، یک پاسخ محلی (مانند خاتمه‌دادن به یک پردازش و یا خاموش‌کردن میزبان) صادر می‌کند.

۲) سامانه‌های پاسخ همکارانه[9]: سامانه‌های پاسخ همکارانه به مجموعه‌ای از سامانه‌های پاسخ اطلاق می‌شود که با همکاری یکدیگر یک پاسخ را در مقابله با حمله اعمال می‌کنند. به‌عبارت دیگر، سامانه‌های پاسخ همکارانه متشکل از تعدادی سامانه پاسخ خودمختار است که قادر به تشخیص و اعمال پاسخ به‌صورت محلی هستند. هرچند راه‌برد نهایی پاسخ به‌صورت سراسری انتخاب می‌شود. اگرچه سامانه‌های پاسخ همکارانه پاسخ کاراتری را نسبت

6- Proactive (Preemptive)
7- Reactive
8- Autonomous
9- Cooperative

به سامانه‌های پاسخ خودمختار ارائه می‌دهند اما معمولاً پیچیده بوده و نیازمند هماهنگی و ارتباطات قوی میان بخش‌های مختلف هستند.



شکل (۲): دسته‌بندی سامانه‌های پاسخ بر اساس دیدگاه‌های مختلف

از نظر روش انتخاب پاسخ، سامانه‌های پاسخ در سه دسته زیر تقسیم‌بندی می‌شوند:

۱) نگاشت ایستا[1]: نگاشت ایستا اصولاً برای سامانه‌های پاسخ دستی مورد استفاده قرار می‌گیرد که در آن یک نگاشت ثابت بین هشدارها و پاسخ‌های از پیش تعیین‌شده صورت می‌گیرد. پیاده‌سازی و نگهداری این دسته از سامانه‌های پاسخ آسان است. یکی از معایب این روش این است که رفتار سامانه پاسخ در آن قابل پیش‌بینی است و حمله‌کننده می‌تواند سامانه پاسخ را دور بزند. عیب دیگر این روش عدم استفاده از وضعیت فعلی سامانه در نگاشت هشدارها به پاسخ‌هاست.

۲) نگاشت پویا[2]: سامانه‌های پاسخ نگاشت پویا نسبت به سامانه‌های پاسخ نگاشت ایستا پیشرفته‌تر بوده و در انتخاب پاسخ براساس سنجه‌های حمله (اطمینان، شدت حمله و ...) عمل می‌کنند. در تنظیمات نگاشت پویا یک هشدار به مجموعه‌ای از پاسخ‌ها مرتبط می‌شود. پاسخ‌های مناسب در زمان واقعی براساس ویژگی‌های حمله انتخاب می‌شود.

۳) نگاشت حساس به هزینه[3]: تنها سامانه‌های پاسخی هستند که هدفشان برقراری تعادل بین هزینه پاسخ و خسارت حمله است. بر این اساس، پاسخ‌های مناسب براساس عوامل مربوط به حمله مانند شدت مخاطره و عوامل مربوط به پاسخ مانند میزان هزینه انتخاب خواهد شد. مهم‌ترین چالش فراروی روش‌های حساس به هزینه اندازه‌گیری دقیق این فاکتورها و به‌روزرسانی آن‌هاست.

در ادامه دسته‌بندی سامانه‌های پاسخ و براساس رساله دکترای آقای شاملی سه نوع مدل هزینه پاسخ نیز می‌توان درنظر گرفت [۲۰]:

۱) مدل هزینه ایستا[4]: هزینه ایستای پاسخ با استفاده از تخصیص یک مقدار ثابت براساس نظر خبره به‌دست می‌آید. بنابراین، یک مقدار ثابت برای هزینه هر پاسخ درنظر گرفته می‌شود (RCs = CONSTANT).

۲) مدل هزینه ارزیابی‌شده ایستا[5]: در این روش، هزینه ارزیابی‌شده ایستا با استفاده از یک سازوکار ارزیابی برای هر پاسخ به‌دست می‌آید. هزینه پاسخ در اکثر مدل‌های موجود به این صورت ارزیابی می‌شود. یک راه‌حل معمول برای این منظور بررسی اثرات مثبت پاسخ‌ها، براساس نتیجه محرمانگی، یکپارچگی، دسترس‌پذیری و معیارهای عملکرد می‌باشد. برای بررسی اثرات منفی پاسخ‌ها می‌توان دیگر منابع را از لحاظ دسترسی و عملکرد مورد بررسی قرار داد. به‌عنوان مثال، بعد از اجرای پاسخ، دیگر وب سرور مورد حمله در معرض خطر نیست، اما دسترسی به سرویس‌ها کاهش پیدا می‌کند. بعد از ارزیابی اثرات مثبت و منفی هر پاسخ، باید هزینه پاسخ را مشخص کنیم. یک راه‌حل در معادله ۱ نشان داده شده است [۲۱]. بدیهی است که بالاترین مقدار RC، بهترین پاسخ را نشان می‌دهد.

$$RC_{se} = \frac{\text{Positive effect}}{\text{Negative impact}} \qquad (۱)$$

1- Static Mapping
2- Dynamic Mapping
3- Cost-Sensitive
4- Static Cost Model
5- Static Evaluated Cost Model

۳) مدل هزینه ارزیابی‌شده پویا[1]: این مدل براساس وضعیت شبکه می‌باشد (RC_{de}) و به کمک آن می‌توان هزینه پاسخ را به صورت برخط، براساس وابستگی بین منابع و کاربران برخط ارزیابی کرد. براساس این مدل چنانچه هزینه خاتمه‌دادن به یک فرآیند بالا باشد، شاید بتوان پاسخ دیگری را انتخاب نمود. هزینه ارزیابی پاسخ به وابستگی منابع، تعداد کاربران برخط و سطح امتیاز کاربران مرتبط است. این مدل ما را به سمت داشتن یک سامانه پاسخ حساس به هزینه سوق می‌دهد.

۴- تحلیل حملات آینده

تحلیل حملات شبکه یکی از عواملی است که تأثیر فراوانی بر روی انتخاب پاسخ مناسب در مقابله با حملات دارد. به‌طور کلی، حملات شبکه را می‌توان از جنبه‌های مختلفی ازقبیل الگوی حملات، تعداد مسیرهای حمله، میزان خسارت حمله و احتمال وقوع آن مورد تحلیل قرار داد. به منظور دستیابی به الگوی حملات می‌توان از تحلیل روابط بین آسیب‌پذیری‌های شبکه [۲۲] و یا تحلیل وابستگی بین فراخوانی‌های سامانه [۲۳] استفاده نمود. گراف حمله به‌عنوان یکی از مشهورترین ابزارهای موجود جهت تحلیل حملات شبکه است که از طریق آن می‌توان کلیه مسیرهای حمله و احتمالات مربوطه را محاسبه نمود [۲۷-۲۴]. به منظور تخمین میزان خسارت حملات نیز بایستی سیاست‌های امنیتی شبکه را مورد بررسی قرار داد. یکی از روش‌های مرسوم در این حوزه نیز به‌کارگیری گراف وابستگی شبکه است [۲۰]. از این‌رو، در ادامه این بخش به بررسی اجمالی گراف حمله و گراف وابستگی خواهیم پرداخت.

۴-۱- تحلیل حملات شبکه با گراف حمله

گراف‌های حمله اطلاعاتی را در رابطه با آسیب‌پذیری‌ها، ارتباطات بین آن‌ها و اتصالات شبکه مشخص می‌کنند. از این جهت، ابزارهای مهمی برای مقاوم‌سازی شبکه هستند. یک گراف حمله عموماً با آسیب‌پذیری‌ها و شرایط امنیتی نشان داده می‌شود. یک آسیب‌پذیری زمانی می‌تواند مورد بهره‌برداری قرار گیرد که تمام پیش‌شرط‌های مورد نیاز برای بهره‌برداری آن در شبکه موجود باشد. هر مسیر در یک گراف حمله می‌تواند مجموعه‌ای از آسیب‌پذیری‌های بهره‌برداری شده است که می‌تواند سامانه را به یک وضعیت نامطلوب ببرد. با داشتن گراف حمله یا شبکه می‌توان به سوالات زیر پاسخ داد [۲۸]:

- از گراف حمله چه اطلاعاتی به‌دست می‌آید؟
- حملات ممکن در شبکه کدام هستند؟
- برای حمله به یک نقطه در شبکه، مهاجم چند راه مختلف می‌تواند طی کند؟
- مدیر شبکه باید چه اقداماتی انجام دهد تا شبکه را در برابر حمله مقاوم نماید؟

گراف‌های حمله در حوزه‌های مختلف امنیت شبکه ازجمله، تشخیص نفوذ، اعمال سیاست‌های امنیتی و ارائه پاسخ به نفوذ قابل استفاده هستند. یک گراف حمله می‌تواند تمامی دنباله‌های ممکن از آسیب‌پذیری‌هایی که مهاجم می‌تواند بهره‌برداری کند را مشخص نماید. به‌طور کلی، یک گراف حمله تمام دنباله‌های ممکنی که مهاجم ممکن است برای نفوذ در شبکه از آن بهره گیرد را مشخص می‌سازد.

Mulval ابزاری مبتنی بر برنامه‌نویسی منطقی برای تولید گراف حمله است [۲۴]. در این ابزار از زبان Datalog برای نمایش اجزای شبکه و تعاملات امنیتی میان آن‌ها استفاده می‌شود. Datalog از نظر نحوی زیرمجموعه زبان prolog است و مشخصات روشنی از منطق استدلالی مهیا می‌کند. Mulval شامل تعداد مختصری از قوانین Datalog، سناریوهای حمله عمومی شامل بهره‌برداری از انواع مختلف آسیب‌پذیری‌های نرم‌افزاری، سیستم عامل‌ها و پیکربندی می‌باشد. موتور استدلال، ورودی‌ها را از ابزارهای مختلف و مدیران شبکه دریافت می‌کند و تحلیل را در سطح شبکه انجام می‌دهد تا نشان دهد که آیا آسیب‌پذیری‌های موجود بر روی هریک از میزبان‌ها، می‌تواند به یک حمله بزرگتر برای شبکه تبدیل شود یا خیر. Mulval پس از استنتاج و کشف مسیر حمله، گراف حمله را به‌صورت بصری تولید می‌کند.

۴-۲- تحلیل حملات شبکه با گراف وابستگی

در گراف حمله تنها به ارتباطات موجود میان آسیب‌پذیری‌های شبکه و مسیرهای حمله می‌پردازیم. درحالی‌که سایر وابستگی‌های موجود میان گره‌ها و سرویس‌های شبکه نیز تأثیر فراوانی در تحلیل حملات شبکه و اعمال پاسخ‌های مناسب دارند. Gruschke برای اولین بار با استفاده از مفهوم گراف وابستگی رخداد، به مدیریت و هم‌بسته‌سازی رخدادهای شبکه پرداخت [۲۹]. Zhai و همکارانش نیز با ردیابی وابستگی‌های اشیاء در سطح سیستم عامل (مانند فرآیندها و عملیات بر روی فایل‌ها) و ساخت درخت رخدادهای سامانه، روشی جهت تجمیع هشدارهای شبکه ارائه دادند [۳۰].

Toth و Kruegel نیز برای اولین بار از مفهوم گراف وابستگی سرویس در سامانه‌های پاسخ به نفوذ استفاده کردند [۳۱]. یک‌سال بعد Balepin و همکارانش از گراف وابستگی منابع برای ایجاد یک سامانه پاسخ به نفوذ خودکار بهره گرفتند که با ارزیابی وضعیت فعلی شبکه و توجه به سه عامل هزینه حمله، هزینه پاسخ و سود پاسخ اقدام به انتخاب پاسخ مناسب می‌کرد [۳۲]. در

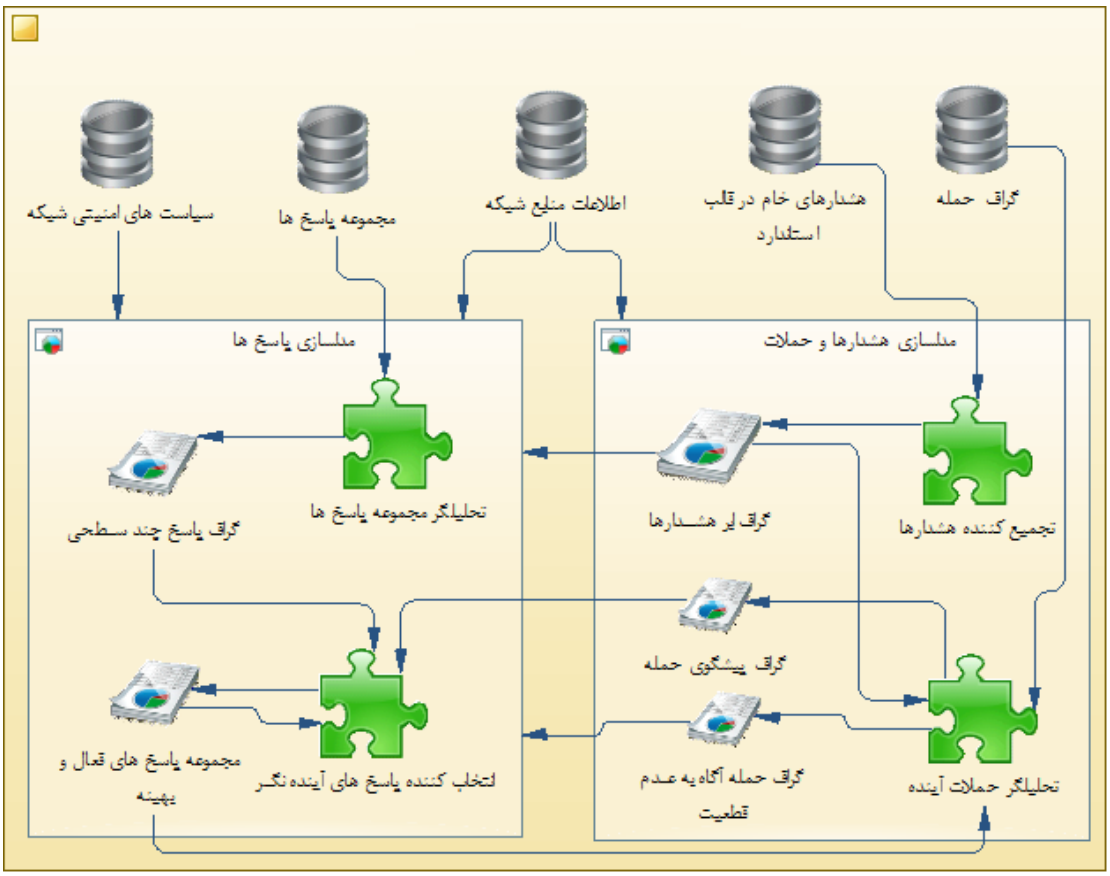
1- Dynamic Evaluated Cost Model

پژوهشی دیگر، Kheir و همکارانش با ارائه یک مدل وابستگی سرویس برای سامانه‌های پاسخ به نفوذ حساس به هزینه، اهمیت وابستگی‌های موجود میان سرویس‌های شبکه در مقایسه حملات شبکه و تخمین هزینه پاسخ را نشان دادند [۱۸]. اخیراً نیز شاملی و همکارانش از گراف وابستگی سرویس برای ارزیابی هزینه پاسخ در سامانه پاسخ به نفوذ پیشنهادی خودشان استفاده کرده‌اند [۳۳]. از این‌رو، تحلیل حملات شبکه به کمک گراف وابستگی تأثیر فراوانی در فرآیند مدیریت هشدارها و انتخاب پاسخ مناسب دارد.

۵- چارچوب پیشنهادی

در این بخش یک چارچوب پاسخ حساس به هزینه و آینده‌نگر برای سامانه‌های تشخیص نفوذ به منظور یافتن پاسخ‌های مناسب برای مقابله با حملات رخ داده و حملات محتمل آینده ارائه‌شده است. در این چارچوب به وابستگی‌ها و ارتباطات میان هشدارها و ارتباطات میان پاسخ‌ها توجه شده است. همچنین، به کمک این معماری می‌توان بهترین پاسخ‌های ممکن را در هر لحظه با توجه به وضعیت جاری شبکه و وضعیت‌های آتی آن شناسایی نمود.

با توجه به این‌که هشدارهای صادرشده توسط سامانه‌های تشخیص نفوذ به‌عنوان ورودی اصلی مسئله انتخاب پاسخ بهینه مطرح هستند، معماری پیشنهادی شامل دو بخش کلی ۱) مدل‌سازی هشدارها و حملات و ۲) مدل‌سازی پاسخ می‌باشد. همچنین، معماری پیشنهادی نمایش دادهشده در شکل (۳) به منظور انتخاب پاسخ به صورت آینده‌نگر طراحی شده است. نوآوری‌های اصلی این مقاله پیرامون بخش‌های مختلف این معماری شکل گرفته و مواردی از قبیل هشدارهای خام، گراف حمله، سیاست‌های امنیتی، مجموعه پاسخ‌ها و منابع شبکه به‌عنوان ورودی‌های مسئله در نظر گرفته شده‌اند.



شکل (۳): چارچوب پیشنهادی برای سامانه پاسخ به نفوذ آینده‌نگر

۵-۱- تجمیع‌کننده هشدارها

در بخش تجمیع‌کننده هشدارها هدف ما استخراج اطلاعات مفید موجود در جریان هشدارهای شبکه است تا از این طریق بتوان با شناسایی بخش‌های مخرب، فرآیند پاسخگویی را بهبود داد.

برای این منظور، بایستی در ابتدا هشدارهای مشابه که دربرگیرنده اطلاعات یکسانی هستند، شناسایی شوند. سپس هشدارهای مشابه به شکل مناسبی و در قالب ابرهشدار بازنمایی گردند. همچنین، بایستی به‌منظور نمایش ارتباطات بین ابرهشدارها از یک ساختار گرافیکی مناسب استفاده شود. بر این اساس، روش

تجمیع پیشنهادی در این بخش به صورت مبتنی بر شباهت رفتار می‌کند با این تفاوت که در نهایت ارتباطات علت و معلولی بین ابرهشدارهای تولیدی را نیز بازگو خواهد کرد.

در این بخش، به منظور شناسایی هشدارهای مشابه که دربرگیرنده اطلاعات یکسانی هستند از مفهوم بی‌نظمی جزئی استفاده شده است [۳۴]. بر این اساس، بی‌نظمی جزئی هشدارهای صادرشده توسط سامانه تشخیص نفوذ به شکل زیر تعریف می‌شود:

تعریف (بی‌نظمی هشدار) [۳۴]: فرض کنید مجموعه هشدارها را به صورت $\psi = \{A_1, A_2, ..., A_n\}$ و مجموعه ویژگی‌های هر هشدار شامل برچسب زمانی، آدرس مبدأ، آدرس مقصد، پروتکل، پورت مبدأ، پورت مقصد و ... را با $F = \{F_1, F_2, ..., F_k\}$ نمایش دهیم. در این صورت هر ویژگی F_j را می‌توان به‌عنوان یک متغیر تصادفی گسسته درنظر گرفت. حال فرض می‌کنیم برخی از این ویژگی‌ها مانند $F_d \in F$ مستقل نیستند و به مقدار ویژگی F_j وابسته هستند. بر این اساس، برای هر هشدار $A_i = [f_{i1}, f_{i2}, ..., f_{id}, ..., f_{ik}]$ بی‌نظمی جزئی به صورت زیر محاسبه می‌شود:

$$\begin{aligned} H_P(\psi = A_i) &= H_P([F_1, F_2, ..., F_d, ..., F_k] = [f_{i1}, f_{i2}, ..., f_{id}, ..., f_{ik}]) \\ &= [H_P(F_1 = f_{i1}), H_P(F_2 = f_{i2}), ... \\ &\quad , H_P(F_d = f_{id} \mid F_j = f_{ij}), ..., H_P(F_k = f_{ik})] \end{aligned} \quad (۲)$$

بر این اساس، می‌توان ماتریس بی‌نظمی جزئی هشدار (APE) را به صورت زیر تعریف نمود:

$$\begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{matrix} \begin{bmatrix} H_P(F_1 = f_{11}) & \cdots & H_P(F_d = f_{1d} \mid F_j = f_{1j}) & \cdots H_P(F_k = f_{1k}) \\ H_P(F_1 = f_{21}) & \cdots & H_P(F_d = f_{2d} \mid F_j = f_{2j}) & \cdots H_P(F_k = f_{2k}) \\ \vdots & \vdots & \vdots & \vdots \cdots \quad \vdots \\ H_P(F_1 = f_{n1}) & \cdots & H_P(F_d = f_{nd} \mid F_j = f_{nj}) & \cdots H_P(F_k = f_{nk}) \end{bmatrix} \quad (۳)$$

با کمک قانون زنجیره‌ای می‌توان وابستگی‌های پیچیده‌تر را نیز به کمک روابط بیان‌شده پشتیبانی نمود. از آن‌جایی‌که هشدارهای مشابه در بردارنده اطلاعات یکسانی هستند، بردار بی‌نظمی جزئی آن‌ها نیز مشابه خواهد بود و می‌توان با استفاده از یک روش خوشه‌بندی مناسب هشدارهای شبیه به هم را شناسایی نمود و در یک خوشه قرار داد. برای این منظور، از الگوریتم خوشه‌بندی مشهور DBSCAN[1] استفاده شده است [۳۵]. همچنین، برای بازنمایی هشدارهای قرارگرفته در یک خوشه از ساختار تعمیم سلسله مراتبی ویژگی‌های هشدار استفاده شده است [۳۶]. در این ساختار با ایجاد یک درخت برای هریک از ویژگی‌های هشدار، می‌توان به‌راحتی هشدارهای موجود در یک خوشه را به شکل مناسبی بازنمایی نمود. روابط بین ابرهشدارها را نیز می‌توان به کمک یک ساختار گرافی مناسب بازنمایی نمود. برای این منظور، گراف ابرهشدار را به‌صورت زیر تعریف می‌کنیم:

تعریف (گراف ابرهشدارها) [۳۴]: یک گراف جهت‌دار است که با ۳-تایی $HG = \langle Ha, E_{Ha}, L \rangle$ نمایش داده می‌شود که در آن:

- Ha مجموعه گره‌های گراف را نمایش می‌دهد که در قالب ابرآدرس‌ها[2] (آدرس مبدأ و یا مقصد به‌صورت تعمیم‌یافته و یا غیرتعمیم‌یافته) تعریف می‌شوند.
- $E_{Ha} = \{e_{Ha_1}, ..., e_{Ha_m}\}$ مجموعه یال‌های گراف بوده و گویای جریان هشدارهای موجود بین ابرآدرس‌ها است.
- $L = \{l_1, ..., l_m\}$ نیز مجموعه برچسب‌های الصاق‌شده به یال‌های گراف در قالب $l_i = < NoEA, Pro, Sp, Dp, vulID, NoIA >$ است که در آن:
  - $NoEA$ بیان‌گر تعداد هشدارهای خروجی صادرشده از ابرآدرس مبدأ
  - Pro بیان‌گر نوع پروتکل(ها)
  - Sp بیان‌گر شماره پورت(های) مبدأ
  - Dp بیان‌گر شماره پورت(های) مقصد
  - $vulID$ بیان آسیب‌پذیری(های) مورد بهره‌برداری قرارگرفته
  - $NoIA$ بیان‌گر تعداد هشدارهای ورودی واردشده به ابرآدرس مقصد است.

براساس مطالب بیان‌شده، تجمیع‌کننده هشدارهای پیشنهادی شامل فعالیت‌های زیر است:

- گام اول: مدل‌سازی و بازنمایی مجموعه هشدارها با کمک ماتریس APE
- گام دوم: اجرای الگوریتم خوشه‌بندی DBSCAN بر روی ماتریس APE به منظور شناسایی هشدارهای مشابه
- گام سوم: بازنمایی هشدارهای قرارگرفته در هر خوشه در قالب ابرهشدارها
- گام چهارم: یک مرحله اختیاری جهت کاهش تعداد ابرهشدارها درصورت زیادبودن آن‌ها
- گام پنجم: تولید گراف ابرهشدارها به منظور ایجاد یک شمای کلی از هشدارهای صادرشده

۵-۲- تحلیل‌گر حملات آینده

به‌طور کلی، پیش‌بینی حملات آینده امر دشواری است. با این حال، کسب اطلاعاتی در مورد حملات پیش رو می‌تواند در تحلیل امنیت شبکه و فرآیند پاسخگویی به حملات در وضعیت فعلی

1- Density-Based Spatial Clustering of Applications with Noise

2- Hyper-Addresses

بسیار موثر باشد. در این بخش رویکردی نوین جهت پیش‌بینی حملات آتی و تخمین احتمال وقوع هریک از آن‌ها ارائه شده است [۳۷]. پیش‌بینی صورت‌گرفته برمبنای تجمیع اطلاعات دریافتی از گراف حمله، مجموعه هشدارها، پاسخ‌های فعال و گراف وابستگی شبکه می‌باشد. همچنین، به‌منظور افزایش کارایی، احتمال حملات به صورت بازه‌ای محاسبه شده‌اند. در الگوریتم (۱) رویکرد پیشنهادی جهت پیشگویی حملات آینده ارائه شده است.

Input: Uncertainty-aware Attack graph, Hyper-alerts graph, Multi-level Response Graph, Dependency Graph
Output: Forecasting Attack Graph

Step 1. *Calculate the initial probability of nodes in the uncertainty-aware Attack Graph*

$$\underline{P}^{(old)}(n_i)=\arg\min_{\forall C}\sum_{n_i\in N}\hat{P}(n_i)$$

$$\overline{P}^{(old)}(n_i)=\arg\max_{\forall C}\sum_{n_i\in N}\hat{P}(n_i)$$

Step 2. *Update the probability of nodes in the uncertainty-aware attack graph*

for each attack graph node (n_i) **do**

Update the probability of nodes in the uncertainty- aware attack graph according to hyper-alerts

for each Hyper-alert (ha_x) **do**

$$\theta = Hsimilarity(ha_x, n_i)$$

$$\underline{P}^{(H)}(n_i)=\left(1-\underline{P}^{(old)}(n_i)\right)\times\theta+\underline{P}^{(old)}(n_i)$$

$$\overline{P}^{(H)}(n_i)=\left(1-\overline{P}^{(old)}(n_i)\right)\times\theta+\overline{P}^{(old)}(n_i)$$

$$\hat{P}^{(H)}(n_i)=<\underline{P}^{(H)}(n_i),\overline{P}^{(H)}(n_i)>$$

end for

Update the probability of nodes in the uncertainty-aware attack graph according to the active responses

for each response (r_y) **do**

$$\omega = Rsimilarity(r_y, n_i)$$

$$\underline{P}^{(R)}(n_i)=-\underline{P}^{(H)}(n_i)\times\omega+\underline{P}^{(H)}(n_i)$$

$$\overline{P}^{(R)}(n_i)=-\overline{P}^{(H)}(n_i)\times\omega+\overline{P}^{(H)}(n_i)$$

$$\hat{P}^{(R)}(n_i)=<\underline{P}^{(R)}(n_i),\overline{P}^{(R)}(n_i)>$$

end for

end for

$$\hat{P}^{(new)}(n_i)=\hat{P}^{(R)}(n_i)$$

Step 3. *Find the probability of attacks* $Att_g^{(jl)}$ *on service and/or process* sp_j *in host* h_l *and generate the Forecasting Attack Graph using Dependency Graph or Uncertainty-aware Attack Graph*

الگوریتم (۱): رویکرد پیشنهادی جهت پیش‌بینی حملات آینده

در گام اول هدف ما ساخت گراف حمله آگاه به عدم قطعیت و محاسبه احتمالات گره‌های آن است. گراف حمله آگاه به عدم قطعیت یکی از اجزای اصلی رویکرد پیشنهادی است که به کمک آن احتمال بهره‌برداری از آسیب‌پذیری‌های شبکه با درنظرگرفتن عدم قطعیت موجود در اندازه‌گیری محاسبه می‌شود. به‌طور رسمی، گراف حمله آگاه به عدم قطعیت به صورت زیر تعریف می‌شود:

تعریف (گراف حمله آگاه به عدم قطعیت) [۳۷]: یک گراف مبتنی بر گراف حمله است که به‌صورت ۶-تایی $UAG=\langle N,E_N,D,\Pr,C,G\rangle$ تعریف می‌شود. که در آن:

- $N=\{n_1,n_2,\ldots,n_k\}$، مجموعه نودهای گراف حمله
- E_N، مجموعه یال‌های گراف حمله
- D مجموعه‌ای از دوتایی‌های $<n_i,d_i>, i=1,\ldots k$ است که $d_i\in\{LEAF,AND,OR\}$ نمایان‌گر نوع گره‌های موجود در گراف است.
- $\Pr=\{\hat{P}(n_1),\hat{P}(n_2),\ldots,\hat{P}(n_k)\}$ مجموعه احتمالات نادقیق وابسته به هر گره است که در آن، $\underline{P}(n_i)=\sup\{P(n_i):P\in\rho\}$ نشان‌دهنده حد پایین و $\overline{P}(n_i)=\inf\{P(n_i):P\in\rho\}$ نشان‌دهنده حد بالای احتمال است. ρ نیز معرف مجموعه توزیع احتمالات موجود است.
- C مجموعه محدودیت‌های تعریف‌شده برروی نودهای گراف حمله است. برخی از این محدودیت‌ها را می‌توان براساس ساختار گراف حمله استخراج نمود. به‌عنوان مثال، برای گره‌های برگ، محدودیت‌ها می‌توانند از جنس تساوی باشند ($\hat{P}(n_i)=<1,1>$) و برای گره‌های عطفی و فصلی می‌توان محدودیت‌هایی از جنس نامساوی براساس گره‌های والد به صورت زیر تعریف نمود:
  - $\hat{P}(n_i)\le\prod\hat{P}(Parent(n_i))$ چنانچه n_i یک گره AND باشد.
  - $\hat{P}(n_i)\le 1-\prod\left(1-\hat{P}(Parent(n_i))\right)$ چنانچه n_i یک گره OR باشد.

همچنین برخی از محدودیت‌ها نیز با استفاده از دانش شخص خبره و ویژگی‌های شبکه تعریف می‌شوند.

- $G\subseteq N$ نیز مجموعه گره‌های هدف و زیرهدف مورد استفاده توسط حمله‌کننده را نشان می‌دهند.

به‌منظور محاسبه حد بالا و پایین احتمالات در هر گره می‌توان مسائل بهینه‌سازی زیر را حل نمود:

$$\underline{P}(n_i)=\arg\min_{\forall C}\sum_{n_i\in N}\hat{P}(n_i) \qquad (۴)$$

$$\bar{P}(n_i)=\arg\max_{\forall C}\sum_{n_i\in N}\hat{P}(n_i) \quad (۵)$$

در گام دوم با کمک ابرهشدارهای تولیدشده و مجموعه پاسخ‌های فعال، احتمالات حاصل را به‌روزرسانی می‌کنیم. طریقه به‌روزرسانی به گونه‌ای است که ابرهشدارهای صادرشده تأثیر افزایشی برروی احتمالات موجود خواهند گذاشت و مجموعه پاسخ‌های فعال نیز تأثیر کاهشی خواهند داشت. در گام سوم نیز هدف تولید گراف پیشگوی حملات با استفاده از اطلاعات حاصل از گام‌های قبل و گراف وابستگی شبکه و یا گراف حمله آگاه به عدم قطعیت است.

تعریف (گراف پیشگوی حمله) [۳۷]: یک گراف جهت‌دار است که به‌صورت ۳-تایی $FAG=\langle Att_g, E_{Att}, L\rangle$ نمایش داده می‌شود که در آن:

- Att_g بیان‌گر مجموعه گره‌های گراف بوده و شامل حملات محتمل در شبکه است.
- E_{Att} بیان‌گر مجموعه یال‌های گراف بوده و روابط موجود میان حملات شبکه را نشان می‌دهد.
- $L=\langle P_A, NT, PI\rangle$ بیان‌گر برچسب گره‌های گراف پیشگوی حمله است که حاوی احتمال حمله، نوع گره (عطفی، فصلی و یا برگ) و اطلاعات مستخرج از مسیر حمله (آسیب‌پذیری‌ها، سرویس‌ها، فرآیندها، برنامه‌ها، فایل‌ها و کاربران مرتبط با حمله) است.

۵-۳- تحلیل‌گر مجموعه پاسخ‌ها

یکی از مهم‌ترین چالش‌های پیش رو در حوزه سامانه‌های پاسخ به نفوذ، عدم وجود مجموعه استانداردی از پاسخ‌ها است. در اغلب پژوهش‌های صورت‌گرفته، بررسی و ارزیابی سامانه پیشنهادی تنها با کمک تعریف مجموعه محدودی از پاسخ‌ها انجام می‌گیرد. از سوی دیگر، تاکنون هیچ ساختار استانداردی برای نمایش مجموعه پاسخ‌ها ارائه نشده است. از این‌رو، در این بخش هدف ما ارائه یک شیوه مناسب برای دسته‌بندی و بازنمایی مجموعه پاسخ‌هاست به نحوی که فرآیند محاسبه هزینه پاسخ و انتخاب پاسخ بهینه تسهیل شود [۳۸].

۵-۳-۱- مدل چندسطحی برای دسته‌بندی پاسخ‌ها

در این بخش یک مدل چندسطحی جهت دسته‌بندی مجموعه پاسخ‌ها ارائه شده است. مطابق مدل پیشنهادی، مجموعه پاسخ‌ها را می‌توان براساس میزان تأثیرگذاری آن‌ها بر روی منابع به ۸ دسته زیر تقسیم‌بندی نمود.

۱) پاسخ در سطح اطلاع‌رسانی[1]: از دید میزان تأثیر بر روی منابع شبکه پایین‌ترین سطح پاسخ‌ها به شمار می‌روند. در این نوع پاسخ‌ها در صورت بروز حمله، با روش‌های مختلفی (ثبت در فایل وقایع سامانه، ارسال ایمیل، ارسال پیام کوتاه و ...) مدیر شبکه در جریان وقوع حمله قرار می‌گیرد.

۲) پاسخ در سطح حمله‌کننده[2]: این نوع پاسخ‌ها به طور مستقیم بر روی حمله‌کننده تأثیر خواهند گذاشت (مانند مسدودکردن آدرس IP حمله‌کننده در دیواره آتش).

۳) پاسخ در سطح آسیب‌پذیری[3]: این دسته از پاسخ‌ها جهت مرتفع‌نمودن آسیب‌پذیری‌های شناخته‌شده اعمال می‌شوند. به عنوان مثال، برای از بین‌بردن آسیب‌پذیری CVE-2009-1918 که در سرویس مرورگر مایکروسافت قرار دارد بایستی نسخه فعلی را ارتقاء داد و نسخه ۹ و یا بالاتر این مرورگر را نصب نمود.

۴) پاسخ در سطح فایل[4]: کلیه پاسخ‌هایی که به طور مستقیم بر روی فایل‌های شبکه تأثیر می‌گذارند (از قبیل مسدودکردن یک فایل و یا هرگونه اعمال تغییرات در مجوزهای دسترسی آن) در این سطح دسته‌بندی می‌شوند.

۵) پاسخ در سطح کاربر[5]: این سطح کلیه پاسخ‌هایی را شامل می‌شود که به طور مستقیم بر روی کاربران شبکه تأثیر می‌گذارند (مانند مسدودکردن یک کاربر و یا تغییر مجوزهای دسترسی وی).

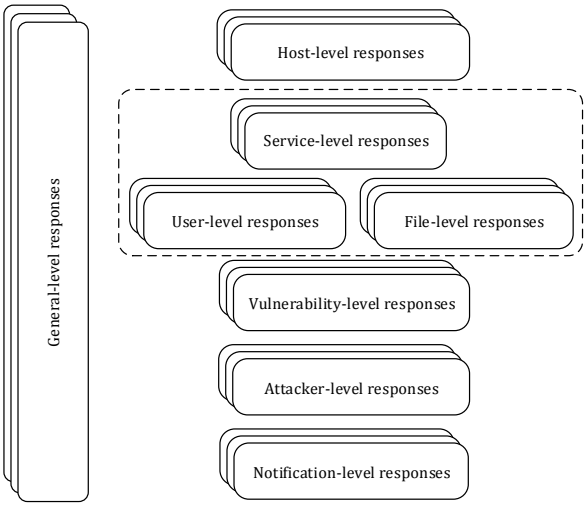
۶) پاسخ در سطح سرویس[6]: پاسخ‌های اعمال‌شده بر روی فرآیندها، سرویس‌ها، پورت‌ها و برنامه‌های کاربردی در این دسته قرار می‌گیرند (مانند مسدودنمودن پورت ۲۳ در سرورها).

۷) پاسخ در سطح میزبان[7]: شدیدترین نوع پاسخ‌ها در این سطح دسته‌بندی می‌شوند. پاسخ‌های موجود در این سطح بر روی یک میزبان تأثیر می‌گذارند (مانند خاموش‌کردن و یا راه‌اندازی مجدد یک میزبان).

۸) پاسخ در سطح کلی[8]: برخی از پاسخ‌های موجود جنبه عام داشته و در هیچ یک از دسته‌های فوق قرار نمی‌گیرند. به عنوان مثال، راه‌اندازی یک سامانه تشخیص نفوذ و یا یک دیواره آتش اضافی می‌تواند در این سطح قرار گیرد. به‌طور کلی، هدف این دسته از پاسخ‌ها بالابردن سطح ایمنی شبکه است.

1- Notification-Level Response

2- Attacker-Level Response
3- Vulnerability-Level Response
4- File-Level Response
5- User-Level Response
6- Service-Level Response
7- Host-Level Response
8- General-Level Response



شکل (۴): مدل چند سطحی ارائه شده جهت دسته‌بندی مجموعه پاسخ‌ها [۳۸]

۵-۳-۲- مدل آینده‌نگر تخمین هزینه پاسخ

اعمال هر پاسخ بر روی منابع شبکه هزینه‌هایی را به دنبال خواهد داشت. برآورد دقیق این میزان هزینه در انتخاب پاسخ‌های مناسب بسیار مفید است. از این‌رو، در این بخش رویکرد جدیدی برای محاسبه هزینه پاسخ به صورت آینده‌نگر ارائه شده است که در آن از کلیه اطلاعات مربوط به مجموعه پاسخ‌ها، منابع شبکه، حملات رخ‌داده و حملات محتمل آتی استفاده کرده‌ایم. همچنین، در مدل پیشنهادی به عدم قطعیت موجود در برآورد هزینه پاسخ توجه شده و هزینه پاسخ در دو حالت خوش‌بینانه و بدبینانه محاسبه می‌شود.

به منظور محاسبه هزینه کلی پاسخ، تأثیرات منفی و تأثیرات مثبت آنرا به‌صورت مجزا درنظر می‌گیریم. تأثیرات منفی پاسخ به هزینه‌های تحمیل‌شده به منابع شبکه اشاره دارد درحالی‌که تأثیرات مثبت پاسخ، میزان تأثیر پاسخ بر روی حملات موجود را شامل می‌شود. سایر ورودی‌های مورد نیاز جهت تخمین تأثیرات منفی و مثبت پاسخ‌ها عبارتند از: سیاست‌های امنیتی، گراف حمله آگاه به عدم قطعیت، گراف ابرهشدارها و گراف وابستگی‌های کلی شبکه[1].

تعریف (گراف وابستگی‌های کلی شبکه) [۳۸]: یک گراف جهت‌دار است که به صورت ۳-تایی $GNDG = \langle \mathrm{H}, E_{\mathrm{H}}, L \rangle$ نمایش داده می‌شود که در آن:

۱) $\mathrm{H} = \{\eta_1, \eta_2, \ldots \eta_m\}$ بیان‌گر مجموعه گره‌های گراف بوده و شامل اجزای مختلف شبکه از قبیل: سرویس‌ها، فرآیندها، برنامه‌های کاربردی، فایل‌ها، کاربران و آسیب‌پذیرها است.

۲) $E_{\mathrm{H}} = \{e_1, \ldots, e_{|E_{\mathrm{H}}|}\}$ بیان‌گر مجموعه یال‌های گراف بوده و روابط موجود میان اجزای مختلف شبکه را نشان می‌دهد.

۳) $L = \{l_1, \ldots, l_{|E_{\mathrm{H}}|}\}$ بیان‌گر مجموعه برچسب‌های متصل به یال‌های گراف است که در آن $l_i \in \{\textbf{confidentiality, integrity, availability}\}$.

تأثیرات مثبت و منفی پاسخ با کمک روابط زیر محاسبه می‌شود:

$$\textbf{Impact}_{+}(R_i, Att_k) = \sum_{M \in \{C,I,A\}} \left\{ G(M, R_i, Att_k) . \sum_{j=1}^{m} \tilde{D}(M, Att_k, \eta_j) \right\} \quad (۶)$$

$$\textbf{Impact}_{-}(R_i) = \tilde{C}_{op}(R_i) + \sum_{M \in \{C,I,A\}} \sum_{j=1}^{m} \tilde{\omega}(M, \eta_j) . \tilde{C}_{im}(M, R_i, \eta_j) \quad (۷)$$

که در آن‌ها، $\tilde{D}(M, Att_k, \eta_j)$ تابعی است جهت تخمین خسارت حمله Att_k بر روی هریک از معیارهای امنیتی موجود در گره η_j گراف وابستگی‌های کلی شبکه. همچنین، تابع $G(M, R_i, Att_k)$ جهت محاسبه میزان سودمندی پاسخ R_i بر روی حمله Att_k در رابطه با معیار امنیتی M استفاده می‌شود. $\tilde{C}_{op}(R_i) = \langle \underline{C}_{op}(R_i), \overline{C}_{op}(R_i) \rangle$ نیز بیان‌گر حداقل و حداکثر هزینه عملیاتی‌شدن پاسخ است که براساس دانش شخص خبره تعیین می‌شود. $\tilde{\omega}(M, \eta_j)$ تابعی است که به کمک آن وزن هریک از معیارهای امنیتی بر روی گره η_j مشخص می‌شود. همچنین، تابع $\tilde{C}_{im}(M, R_i, \eta_j)$ جهت محاسبه میزان هزینه پاسخ R_i بر روی معیار امنیتی M در گره η_j استفاده می‌گردد. سپس هزینه نهایی پاسخ را در دو حالت خوش‌بینانه و بدبینانه به صورت زیر تعریف می‌کنیم:

$$\textbf{Optimistic\_Cost}^{(t)}(R_i) = \sum_{k=1}^{l} \left\{ \frac{\left(1 - \underline{P}^{(t)}(Att_k)\right)\left(\textbf{Impact}_{-}(R_i)\right)}{\underline{P}^{(t)}(Att_k)\left(\textbf{Impact}_{+}(R_i, Att_k)\right)} \right\} \quad (۸)$$

$$\textbf{Pessimistic\_Cost}^{(t)}(R_i) = \sum_{k=1}^{l} \left\{ \frac{\left(1 - \overline{P}^{(t)}(Att_k)\right)\left(\textbf{Impact}_{-}(R_i)\right)}{\overline{P}^{(t)}(Att_k)\left(\textbf{Impact}_{+}(R_i, Att_k)\right)} \right\} \quad (۹)$$

که در آن، $\underline{P}^{(t)}(Att_k)$ و $\overline{P}^{(t)}(Att_k)$ کمترین و بیشترین میزان احتمال وقوع حملات را در لحظه t نمایش می‌دهند که از طریق گراف حمله آگاه به عدم قطعیت قابل استخراج می‌باشند.

۵-۴- انتخاب‌کننده پاسخ‌های آینده‌نگر

در این بخش به دنبال ارائه روشی آینده‌نگر برای انتخاب پاسخ‌های مناسب هستیم به گونه‌ای که کمترین میزان هزینه به شبکه تحمیل شود. برای این منظور، دو رویکرد کلی زیر پیشنهاد شده است:

1- Global Network Dependency Graph

۱) مدل‌سازی مسئله با کمک روش‌های مرسوم تصمیم‌سازی[1]: در این رویکرد ابتدا وزن هریک از معیارهای تصمیم که شامل معیارهای امنیتی محرمانگی، جامعیت و در دسترس‌پذیری است به کمک مدیر شبکه محاسبه می‌شود. سپس امتیاز هر پاسخ با کمک تخمین هزینه پاسخ بر روی هریک از معیارهای امنیتی به‌دست می‌آید. به منظور تخمین هزینه پاسخ نیز از مدل آینده‌نگر بیان‌شده در بخش قبل استفاده می‌کنیم. درنهایت، رتبه کلی هر پاسخ در وضعیت فعلی شبکه با ترکیب نتایج قبلی محاسبه می‌شود.

۲) مدل‌سازی مسئله با کمک روش‌های مرسوم تصمیم‌سازی در شرایط عدم قطعیت: در این رویکرد به عدم قطعیت موجود در وضعیت شبکه نیز توجه می‌شود. این عدم قطعیت ناشی از وقوع (عدم وقوع) حملات و یا اعمال (عدم اعمال) پاسخ‌های ممکن در شبکه است. از این‌رو، برای انتخاب پاسخ‌های مناسب با یک فرآیند تصادفی مواجه خواهیم بود. در این‌جا بایستی ابتدا کلیه وضعیت‌های شبکه را شناسایی کرده، سپس احتمال انتقال بین وضعیت‌های مختلف از طریق احتمال وقوع (عدم وقوع) حملات و اعمال (عدم اعمال) پاسخ قابل محاسبه است. همچنین با انتقال بین وضعیت‌های مختلف شبکه می‌توان میزان سودمندی مشخصی را به‌دست آورد.

به منظور توسعه رویکرد اول مسئله انتخاب پاسخ‌های مناسب را می‌توان با کمک الگوریتم تصمیم‌سازی AHP[2] مدل کرد [۳۹]. بر این اساس، پاسخ‌هایی که هزینه‌های آن‌ها به صورت آینده‌نگر محاسبه شده‌اند، با توجه به میزان اهمیت هریک از معیارهای تصمیم، رتبه‌بندی می‌شوند. همچنین، در راستای توسعه رویکرد دوم می‌توان از فرآیند تصمیم‌سازی مارکوف[3] بهره گرفت. در این بخش به دلیل عدم قطعیت موجود در ساختار مسئله انتخاب پاسخ بهینه از استفاده شده است.

برای این منظور وضعیت امنیتی شبکه را با استفاده از اطلاعات مستخرج از گراف پیشگوی حمله و مجموعه پاسخ‌های ممکن بازنمایی می‌کنیم. به‌طوری‌که وضعیت امنیتی شبکه ترکیبی از حملات صورت‌گرفته و پاسخ‌های فعال در شبکه است. بر این اساس، مسئله انتخاب پاسخ آینده‌نگر با کمک MDP به صورت چندگانه $\langle S, \Re, P_{S\Re}, \gamma, R \rangle$ مدل می‌شود که در آن:

۱) $S = \{R_1,\ldots,R_n, a_1,\ldots,a_m\}$, $R_i \in \{0,1\}, a_j \in \{0,1\}$ بیان‌گر مجموعه وضعیت‌های امنیتی شبکه از دید حملات رخداده و پاسخ‌های فعال است.

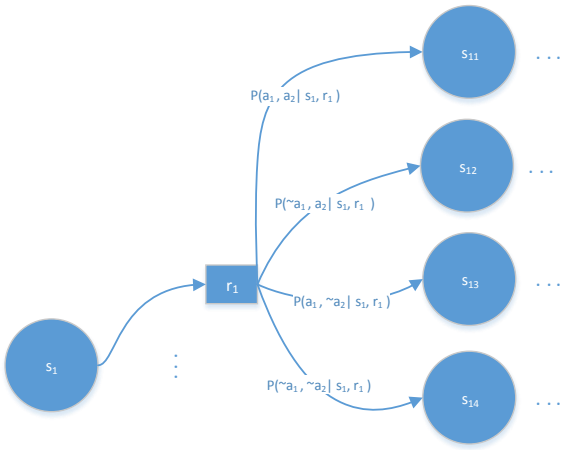
۲) $\Re = \{r_1,\ldots,r_n\}$ بیان‌گر مجموعه پاسخ‌های ممکن در شبکه است.

۳) $P_{S\Re}$ تابعی است که بیان‌گر احتمالات گذر بین وضعیت‌های مختلف امنیتی شبکه است. در این‌جا این تابع میزان احتمال وقوع هر حمله را با توجه به وضعیت فعلی و پاسخ انتخاب‌شده مشخص می‌کند (مقادیر این احتمالات به کمک CVSS قابل محاسبه است).

۴) $\gamma \in [0,1)$ معرف ضریب کاهش است.

۵) $R: S \times A \times S \rightarrow \mathbf{R}$ بیان‌گر تابع پاداش است. در این‌جا با توجه به تغییر وضعیت صورت‌گرفته، گراف حمله پیشگوی حمله به‌روزرسانی می‌شود و با کمک تفاوت احتمالات جدید و قدیم و همچنین میزان هزینه پاسخ، سودمندی هر پاسخ محاسبه می‌شود.

در این حالت با فرض وجود دو حمله نمونه‌ای از گذر بین وضعیت‌های مختلف به صورت شکل (۵) خواهد بود. مطابق این شکل، چنان‌چه شبکه در وضعیت s_1 باشد و پاسخ r_1 فعال شود با احتمال $P(a_1, a_2 \mid s_1, r_1)$ حملات a_1 و a_2 به وقوع خواهند پیوست و شبکه به وضعیت s_{11} خواهد رفت و یا با احتمال $P(\sim a_1, a_2 \mid s_1, r_1)$ حمله a_2 رخ می‌دهد و حمله a_1 اتفاق نخواهد افتاد و شبکه به وضعیت S_{12} خواهد رفت. به طور مشابه T برای سایر حملات محتمل و پاسخ‌های ممکن می‌توان احتمال گذر از وضعیت فعلی را محاسبه نمود.



شکل (۵): نمونه‌ای از گذر بین وضعیت‌های مختلف در مدل انتخاب پاسخ آینده‌نگر مبتنی بر حمله

۶- شبیه‌سازی

در این بخش جهت ارزیابی عملکرد سامانه آینده‌نگر پیشنهادی، آن‌را در یک محیط شبیه‌سازی‌شده تحت سناریوهای مختلف تحت بررسی قرار داده‌ایم. برای این منظور، بخش‌های مختلف این سامانه در نرم‌افزار Matlab پیاده‌سازی شده است. همچنین، به منظور امکان مقایسه نتایج در دو حالت آینده‌نگر و غیرآینده‌نگر،

1- Decision Making
2- Analytic Hierarchy Process
3- Markov Decision Process (MDP)

یک سامانه پاسخ به نفوذ حساس به هزینه و غیرآینده‌نگر مطابق مدل شاملی [۲۰] طراحی و پیاده‌سازی شد. سامانه پاسخ به نفوذ غیرآینده‌نگر طراحی‌شده برخلاف سامانه آینده‌نگر، تنها از اطلاعات موجود در وضعیت فعلی برای محاسبه پاسخ بهینه بهره می‌گیرد. از این‌رو، تنها به سود لحظه‌ای پاسخ اهمیت می‌دهد و به پاداش مورد انتظار در آینده توجهی ندارد.

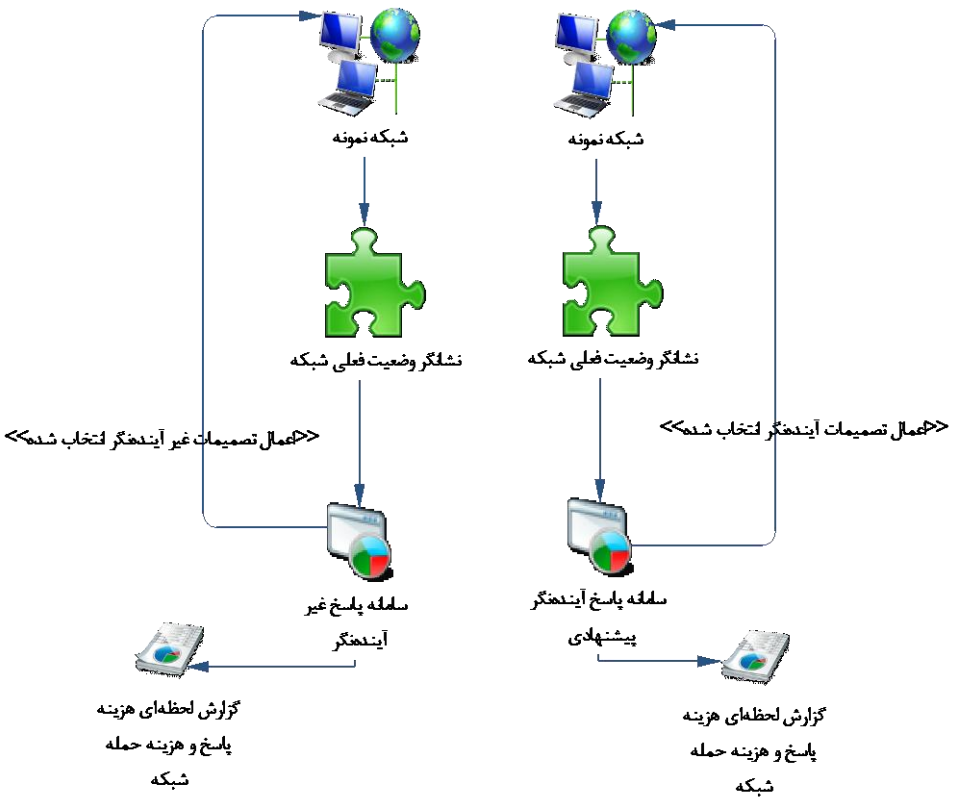
پس از فراهم‌شدن بستر شبیه‌سازی مطابق شکل (۶)، عملکرد سامانه آینده‌نگر و غیرآینده‌نگر را بر روی شبکه نمونه در یک بازه زمانی مشخص مورد ارزیابی قرار می‌دهیم. در ابتدا سامانه پاسخ آینده‌نگر و سامانه پاسخ غیرآینده‌نگر، مطابق اطلاعات مستخرج از شبکه نمونه ساخته می‌شوند. بر این اساس، ابتدا مجموعه تصمیمات بهینه در کلیه وضعیت‌های ممکن شبکه نمونه در دو حالت آینده‌نگر و غیرآینده‌نگر جهت انتخاب پاسخ استخراج می‌شوند. سپس وضعیت امنیتی شبکه از دید حملات رخ داده (یا آسیب‌پذیری‌های مورد بهره‌برداری قرارگرفته) و پاسخ‌های اعمال‌شده شناسایی می‌شود. درنهایت، براساس وضعیت جاری شبکه و مجموعه پاسخ‌های استخراج‌شده، تصمیمات بهینه در وضعیت جاری در دو حالت آینده‌نگر و غیرآینده‌نگر انتخاب و اعمال می‌شود.

جهت اجرای شبیه‌سازی مطابق سه سناریوی پیشنهادی زیر عمل شده است:

۱) سناریوی اول (سناریوی واقع‌گرا): در ابتدا کلیه وضعیت‌های شبکه شناسایی شده و یک وضعیت آغازین انتخاب می‌شود. در وضعیت جاری یک عدد تصادفی تولید می‌شود (با درنظرگرفتن میزان احتمال وقوع هر حمله و یا میزان احتمال بهره‌برداری از هر آسیب‌پذیری) و بر اساس آن وضعیت بعدی شبکه مشخص می‌شود. این فرآیند تا انتهای بازه شبیه‌سازی تکرار می‌شود.

۲) سناریوی دوم (سناریوی خوش‌بینانه): در ابتدا کلیه وضعیت‌های شبکه شناسایی شده و یک وضعیت به عنوان وضعیت آغازین انتخاب می‌شود. در وضعیت جاری محتمل‌ترین حمله به وقوع می‌پیوندد و یا محتمل‌ترین آسیب‌پذیری مورد بهره‌برداری قرار می‌گیرد و بر اساس آن، وضعیت بعدی شبکه مشخص می‌شود. این فرآیند تا انتهای بازه شبیه‌سازی تکرار می‌شود.

۳) سناریوی سوم (سناریوی بدبینانه): در ابتدا کلیه وضعیت‌های شبکه شناسایی شده و یک وضعیت به عنوان وضعیت آغازین انتخاب می‌شود. در وضعیت جاری غیرمحتمل‌ترین حمله به وقوع می‌پیوندد و یا غیر محتمل‌ترین آسیب‌پذیری مورد بهره‌برداری قرار می‌گیرد و براساس آن، وضعیت بعدی شبکه مشخص می‌شود. این فرآیند تا انتهای بازه شبیه‌سازی تکرار می‌شود.



شکل (۶): معماری بستر شبیه‌سازی

۶-۱- معیارهای ارزیابی

به‌منظور ارزیابی رویکرد آینده‌نگر در سامانه پاسخ، نیازمند شبیه‌سازی در طول یک بازه زمانی هستیم. از این‌رو، در این بخش معیارهای جدیدی برای محاسبه هزینه‌های شبکه در یک بازه زمانی مشخص معرفی شده است.

هزینه پاسخ در واحد زمان: به کمک این معیار می‌توان هزینه کل پاسخ‌های اعمال‌شده در یک بازه زمانی مشخص را محاسبه نمود. به منظور محاسبه هزینه پاسخ در واحد زمان از رابطه زیر استفاده می‌کنیم.

$$C_R = \sum_{t=1}^{l} \left(C_{aR}^{(t)} + C_{sR}^{(t)} \right) \qquad (۱۰)$$

که در آن، $C_{aR}^{(t)}$ مجموع هزینه پاسخ‌های فعال و $C_{sR}^{(t)}$ هزینه پاسخ انتخاب شده در زمان t است.

هزینه حمله در واحد زمان: به کمک این معیار می‌توان هزینه کل حملات رخ داده‌شده و محتمل را در یک بازه زمانی مشخص محاسبه نمود. برای محاسبه هزینه حمله در واحد زمان رابطه زیر مورد استفاده قرار می‌گیرد:

$$C_A = \sum_{t=1}^{l} \left(C_{oA}^{(t)} + C_{pA}^{(t)} \right) \qquad (۱۱)$$

که در آن، $C_A^{(t)}$ هزینه حملات فعال و $C_T^{(t)}$ هزینه مربوط به تهدیدات (حملات محتمل) در زمان t است

هزینه کل در واحد زمان: به کمک این معیار می‌توان هزینه کل شبکه در یک بازه زمانی مشخص را محاسبه نمود. برای محاسبه هزینه کل در واحد زمان کافی است مجموع هزینه حمله و هزینه پاسخ را محاسبه کنیم.

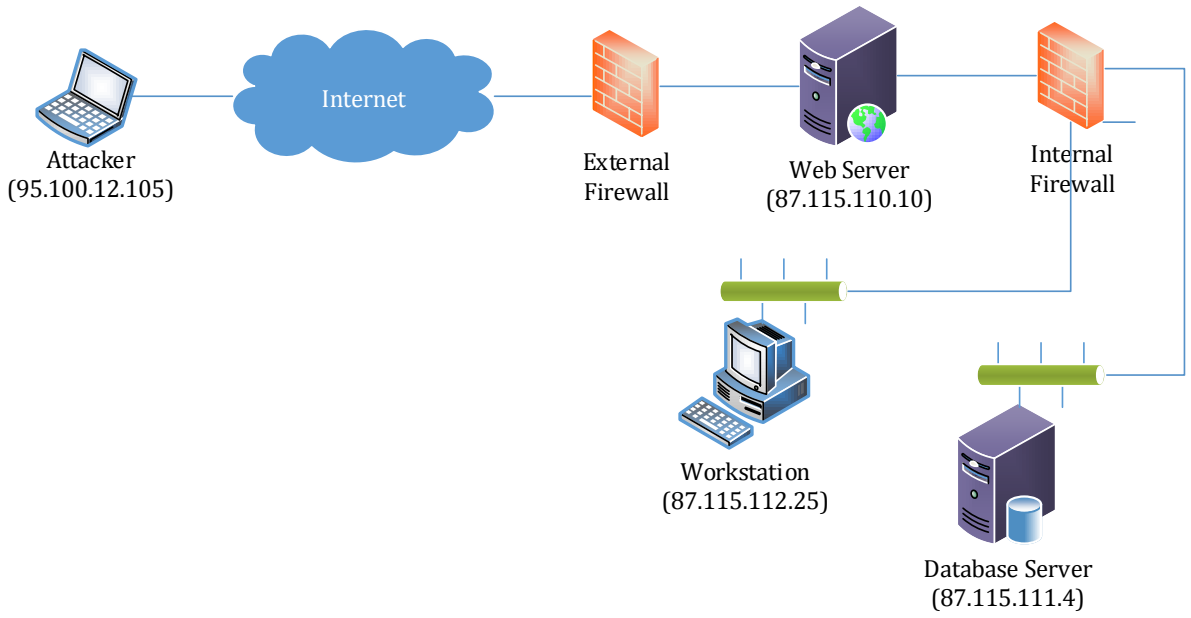
$$C_{total} = C_R + C_A \qquad (۱۲)$$

علاوه‌بر معیارهای فوق و به منظور بررسی روند تغییرات هزینه شبکه می‌توان معیارهای زیر را نیز تعریف نمود.

نمودار نرخ هزینه پاسخ در واحد زمان: این نمودار نشان دهنده نرخ هزینه پاسخ‌ها در واحد زمان است. به کمک این نمودار هزینه‌های تحمیل‌شده به شبکه توسط پاسخ‌های فعال در هر زمان قابل مشاهده است.

نمودار نرخ هزینه حملات در واحد زمان: این نمودار نشان‌دهنده نرخ هزینه حملات در واحد زمان است. به کمک این نمودار هزینه‌های تحمیل‌شده به شبکه توسط حملات رخ داده و حملات محتمل در هر زمان قابل مشاهده است.

نمودار نرخ هزینه کل در واحد زمان: این نمودار نشان‌دهنده نرخ کل هزینه‌های شبکه در واحد زمان است.



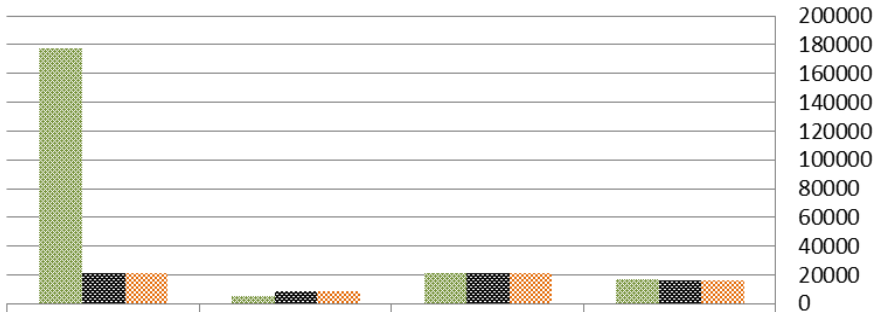
شکل (۷): ساختار شبکه نمونه

جدول (۱): مجموعه پاسخ‌های تعریف‌شده بر روی شبکه نمونه شکل (۷)

Response -level	Response ID	Response-location	Response-action	Response-target	User	File	Process/ Program/ Service	Port	Protocol	Vulnerability	Operational cost (±0.001)
Notification-level	R1-NL-workStation	workStation	Alarm	Attacker	secretary	N/A	N/A	N/A	N/A	N/A	0.01
	R13-NL-dbServer	Database server	Alarm	Attacker	N/A	N/A	mySQL	dbPort	dbProtocol	N/A	0.01
	R7-NL-WebServer	Web server	Notification	Attacker	N/A	N/A	Httpd	Httpport	httpprotocol	N/A	0.01
Attacker-level	R2-AL-workStation	workStation	Block	Attacker	N/A	N/A	N/A	N/A	N/A	N/A	0.01
	R14-AL-dbServer	Database server	Block	Attacker	N/A	N/A	mySQL	dbPort	dbProtocol	N/A	0.01
	R8-AL-WebServer	Web server	Block	Attacker	N/A	N/A	Httpd	HttpPort	httpProtocol	N/A	0.01
Vulnerability-level	R3-VL-workStation	workStation	Remove	workStation	N/A	N/A	N/A	N/A	N/A	CVE-2009-1918	0.2
	R15-VL-dbServer	Database server	Remove	DBserver	N/A	N/A	N/A	N/A	N/A	CVE-2009-2446	0.2
	R9-VL-WebServer	Web server	Remove	Webserver	N/A	N/A	N/A	N/A	N/A	CVE-2006-3747	0.2
User-level	R4-UL-workStation	workStation	Block	workStation	secretary	N/A	N/A	N/A	N/A	N/A	0.1
	R16-UL-dbServer	Database server	Block	workStation	secretary	N/A	N/A	N/A	N/A	N/A	0.1
	R10-UL-WebServer	Web server	Block	workStation	secretary	N/A	N/A	N/A	N/A	N/A	0.1
Service-level	R5-SL-workStation	workStation	Remove	workStation	N/A	N/A	'IE'	N/A	N/A	N/A	0.1
	R17-SL-dbServer	Database server	Block	DBserver	N/A	N/A	mySQL	dbPort	dbProtocol	N/A	0.1
	R11-SL-WebServer	Web server	Block	Webserver	N/A	N/A	Httpd	HttpPort	httpProtocol	N/A	0.1
Host-level	R6-HL-workStation	workStation	Shutdown	Webserver	N/A	N/A	N/A	N/A	N/A	N/A	0.01
	R18-HL-dbServer	Database server	Shutdown	DBserver	N/A	N/A	N/A	N/A	N/A	N/A	0.01
	R12-HL-WebServer	Web server	Shutdown	Webserver	N/A	N/A	N/A	N/A	N/A	N/A	0.01

۶-۲- اجرای شبیه‌سازی بر روی شبکه نمونه

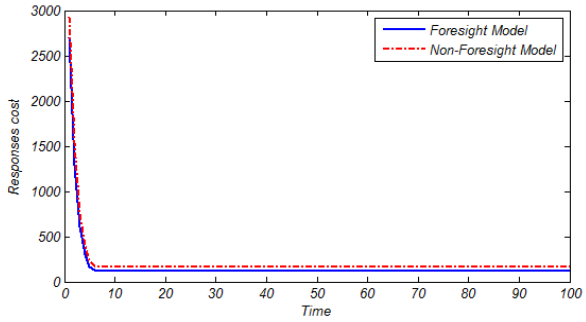
در این‌جا بر روی شبکه نمونه شکل (۷) متمرکز می‌شویم. این شبکه شامل سه آسیب‌پذیری است و احتمال رخدادن سه حمله بر روی نودهای Workstation، WebServer و DbServer وجود دارد. میزان احتمال بهره‌برداری از هر آسیب‌پذیری و یا احتمال وقوع هریک از این حملات با استفاده از گراف حمله آگاه به عدم قطعیت و گراف پیشگوی حمله (مراجعه به پیوست) قابل استخراج است. همچنین، مجموعه پاسخ‌های تعریف‌شده بر روی این شبکه در جدول (۱) نمایش داده شده است. با بهره‌گیری از اطلاعات موجود و الگوریتم پیشنهادی، وضعیت‌های مجاز شبکه را که در حالت به‌کارگیری مدل انتخاب پاسخ آینده‌نگر مبتنی بر حمله تعداد آن‌ها معادل ۵۲۲۹ است، شناسایی و استخراج می‌کنیم. سپس، با کمک مدل‌های آینده‌نگر پیشنهادی و مدل‌های غیرآینده‌نگر موجود هزینه پاسخ محاسبه شده و بهترین پاسخ ممکن در هر وضعیت شناسایی می‌شود. بخشی از تصمیمات بهینه آینده‌نگر و غیرآینده‌نگر به‌دست‌آمده در وضعیت‌های امنیتی مختلف شبکه نمونه، در جدول (پ-۳) پیوست نمایش داده شده است. حال این شبکه را در یک بازه زمانی مشخص (شامل ۱۰۰ گذر وضعیت) مطابق سناریوهای تعریف‌شده در بخش قبل در دو حالت آینده‌نگر و غیرآینده‌نگر شبیه‌سازی می‌کنیم. در این حالت هزینه پاسخ، هزینه حمله و هزینه کل برای هریک از سناریوهای مذکور مطابق شکل (۸) است. همان‌طورکه در شکل (۸) مشاهده می‌شود، کلیه هزینه‌ها در مدل آینده‌نگر در مقایسه با مدل غیرآینده‌نگر به مراتب کمتر است. مدل غیرآینده‌نگر به صورت حریصانه عمل کرده و در هر وضعیت بهترین پاسخ با حداکثر پاداش لحظه‌ای را انتخاب می‌کند، درحالی‌که مدل آینده‌نگر در هر وضعیت علاوه‌بر پاداش لحظه‌ای به پاداش مورد انتظار آینده نیز توجه می‌کند.



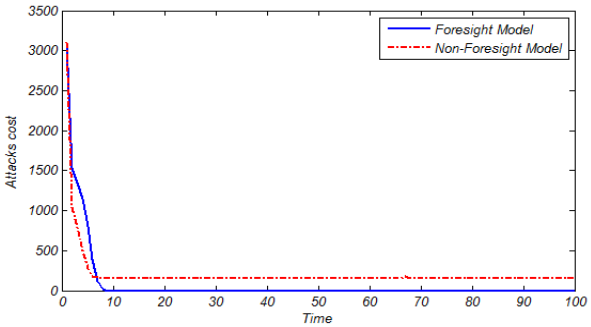
	Total Attack Cost(Non-Foresight)	Total Attack Cost(Foresight)	Total Response Cost(Non-Foresight)	Total Response Cost(Foresight)
Scenario 1	21328.99244	8439.125937	21295.81609	16333.51459
Scenario 2	21322.00594	8483.567937	21295.81609	16332.14957
Scenario 3	177477.4082	5266.177437	21491.88352	16580.00718

شکل (۸): هزینه پاسخ، هزینه حمله و هزینه کل برای هر یک از سناریوهای شبیه‌سازی در دو مدل آینده‌نگر و غیرآینده‌نگر برای شبکه نمونه شکل (۷)

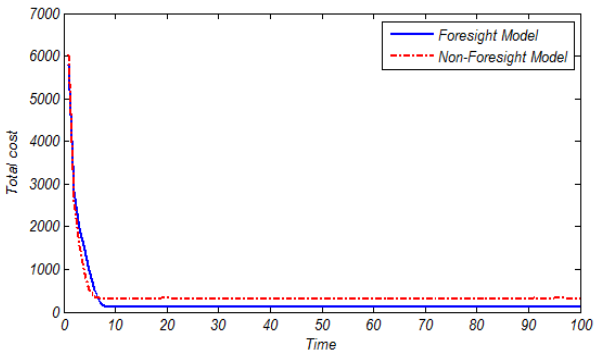
در ادامه آزمایشات نمودارهای نرخ هزینه پاسخ، هزینه حمله و هزینه کل شبکه در سناریوی اول به‌دست آمده است. همان‌طورکه در شکل (۹) مشاهده می‌شود، هزینه پاسخ در دو مدل آینده‌نگر و حریصانه با شروع شبیه‌سازی روند کاهشی دارد و در یک سطح مشخص تقریباً ثابت می‌شود. دلیل این امر نیز جابه‌جایی وضعیت شبکه در میان وضعیت‌هایی با هزینه پاسخ کمتر است. مطابق شکل (۱۰)، هزینه حمله در مدل آینده‌نگر پس از مدتی به صفر کاهش می‌یابد درحالی‌که در مدل غیرآینده‌نگر، هزینه حمله نیز مانند هزینه پاسخ با جابه‌جایی در بین وضعیت‌های غیربهینه در سطح بالاتری نسبت به مدل آینده‌نگر قرار می‌گیرد. بر این اساس، مطابق شکل (۱۱)، کل هزینه‌های شبکه در هر دو مدل آینده‌نگر و غیرآینده‌نگر روند کاهشی دارد با این تفاوت که مدل آینده‌نگر شبکه را به سمت بهترین وضعیت‌های ممکن سوق می‌دهد که در آن‌ها هزینه شبکه کمتر است. با اجرای شبیه‌سازی مطابق سناریوی دوم نیز نتایج مشابهی حاصل می‌شود. همان‌طورکه در اشکال (۱۴-۱۲) مشاهده می‌شود، روند کاهشی هزینه‌های شبکه در مدل آینده‌نگر بهتر از مدل غیرآینده‌نگر است.



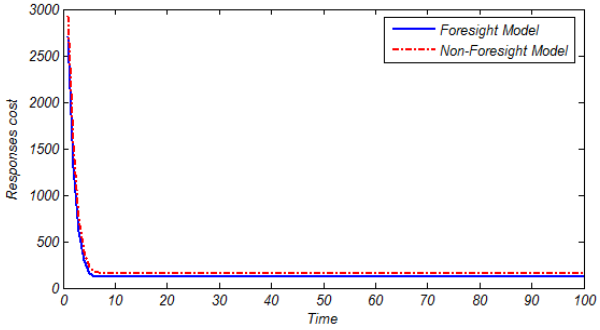
شکل (۹): نمودار نرخ هزینه پاسخ برای سناریوی اول شبیه‌سازی در شبکه نمونه شکل (۷)



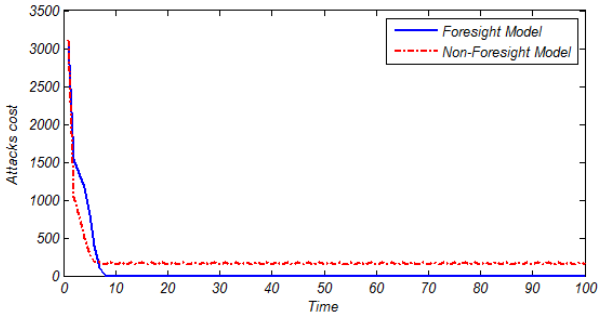
شکل (۱۰): نمودار نرخ هزینه حمله برای سناریوی اول شبیه‌سازی در شبکه نمونه شکل (۷)



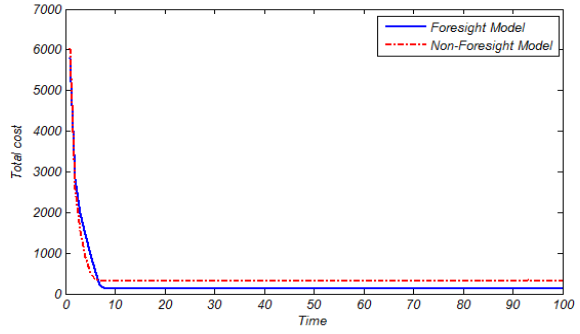
شکل (۱۱): نمودار نرخ هزینه کل برای سناریوی اول شبیه‌سازی در شبکه نمونه شکل (۷)



شکل (۱۲): نمودار نرخ هزینه پاسخ برای سناریوی دوم شبیه‌سازی در شبکه نمونه شکل (۷)

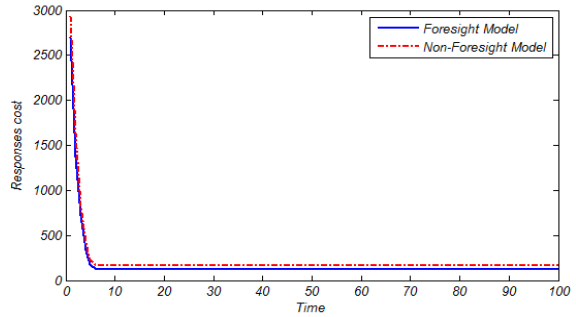


شکل (۱۳): نمودار نرخ هزینه حمله برای سناریوی دوم شبیه‌سازی در شبکه نمونه شکل (۷)

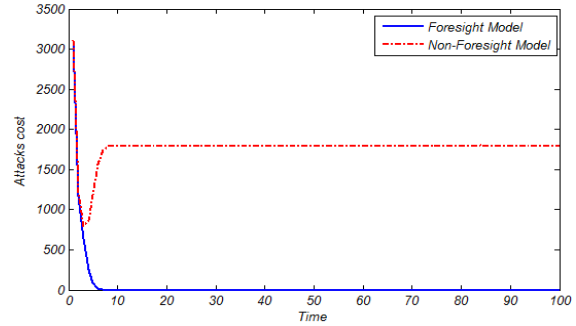


شکل (۱۴): نمودار نرخ هزینه کل برای سناریوی دوم شبیه‌سازی در شبکه نمونه شکل (۷)

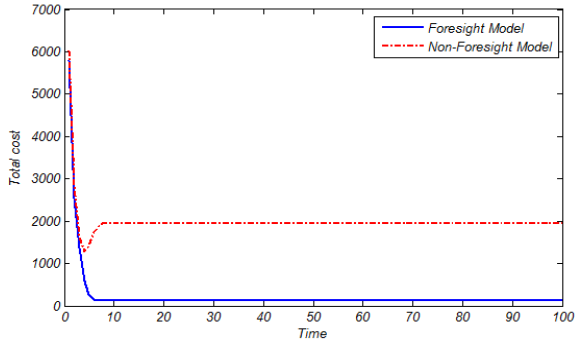
درنهایت، با اجرای شبیه‌سازی مطابق سناریوی سوم نتایج جالبی حاصل می‌شود. همان‌طورکه در شکل (۱۵) مشاهده می‌کنید، هزینه پاسخ تقریباً مشابه سناریوهای قبلی است با این تفاوت که قدری افزایش یافته است. اما در مورد هزینه حمله شرایط متفاوت است و با وقوع رخدادهای غیر محتمل روند کاهشی هزینه حمله در مدل غیر آینده‌نگر تحت تأثیر قرار گرفته است. شکل (۱۶) نشان می‌دهد که مدل آینده‌نگر قادر به تحمل شرایط رخ داده شده است و بر خلاف مدل غیر آینده‌نگر در صورت وقوع رخدادهای غیر محتمل نیز شبکه را به سمت وضعیت‌هایی با هزینه کم هدایت می‌کند. از این رو نرخ کل هزینه‌های شبکه مطابق سناریوی سوم مطابق شکل (۱۷) می‌شود.



شکل (۱۵): نمودار نرخ هزینه پاسخ برای سناریوی سوم شبیه‌سازی در شبکه نمونه شکل (۷)



شکل (۱۶): نمودار نرخ هزینه حمله برای سناریوی سوم شبیه‌سازی در شبکه نمونه شکل (۷)



شکل (۱۷): نمودار نرخ هزینه کل برای سناریوی سوم شبیه‌سازی در شبکه نمونه شکل (۷)

۷- نتیجه‌گیری

در این مقاله رویکرد آینده‌نگر را برای توسعه سامانه‌های پاسخ مورد بررسی قرار دادیم. در این رویکرد از کلیه اطلاعات مفید و قابل دسترس (منابع شبکه و میزان اهمیت آن‌ها، وابستگی‌های منابع، هشدارهای شبکه که نشان‌دهنده حملات صورت‌گرفته در وضعیت فعلی هستند، حملات آتی شبکه و احتمال وقوع آن‌ها، هزینه پاسخ و خسارت حمله، و ارتباطات میان حملات و پاسخ‌ها) جهت پاسخگویی به حملات رخ داده و حملات محتمل آینده استفاده می‌کنیم. هدف رویکرد آینده‌نگر کاهش هزینه‌های شبکه در یک بازه زمانی است به نحوی که در انتهای بازه، شبکه در وضعیت مطلوب قرار گیرد. برای این منظور، چارچوب پیشنهادی شامل دو بخش اساسی مدل‌سازی هشدارها و حملات و مدل‌سازی پاسخ می‌باشد. در بخش نخست هشدارهای شبکه مدیریت می‌شود تا از این طریق بتوانیم حمله‌کننده و نقاط مورد حمله را شناسایی کنیم. شناسایی این نقاط و خروجی این بخش می‌تواند در انتخاب پاسخ‌های مناسب بسیار مفید باشد. همچنین، با بررسی و تحلیل گراف حمله آگاه به عدم قطعیت و گراف وابستگی‌های شبکه می‌توان حملات آینده شبکه را پیش‌بینی کرده و احتمال وقوع آن‌ها را محاسبه نمود. دانستن احتمال وقوع حملات تأثیر به سزایی در انتخاب پاسخ‌های مناسب و پیشگیری از وقوع این حملات در آینده دارد. در بخش دوم معماری پیشنهادی، در ابتدا با مشکل عدم وجود مجموعه استانداردی از پاسخ‌ها مواجه بودیم. برای این منظور یک مدل پاسخ چندسطحی برای بازنمایی مجموعه پاسخ‌ها ارائه شد که از طریق آن تحلیل مجموعه پاسخ‌ها تسهیل می‌شود. همچنین، با ارائه مدل‌های آینده‌نگر هزینه هر پاسخ محاسبه شده و در هر وضعیت شبکه بهترین پاسخ ممکن با توجه به شرایط فعلی و آینده شبکه انتخاب می‌شود. براساس نتایج شبیه‌سازی صورت‌گرفته، رویکرد آینده‌نگر در پاسخگویی به حملات منجر به کاهش هزینه‌های شبکه (هزینه حمله و هزینه پاسخ) در طول یک بازه زمانی مشخص خواهد شد. زیرا در رویکرد آینده‌نگر علاوه‌بر اطلاعات مستخرج از وضعیت فعلی شبکه، کلیه وضعیت‌های محتمل آینده نیز بررسی می‌شود و براساس آن‌ها بهترین پاسخ ممکن انتخاب می‌گردد. همچنین، درصورت وقوع رخدادهای غیرمحتمل نیز مدل آینده‌نگر قابلیت تطبیق با شرایط پیش‌آمده را دارد و باز هم شبکه را به سمت وضعیت‌هایی با کمترین هزینه سوق می‌دهد. به منظور ادامه کار و تکمیل این تحقیق می‌توان بر روی استخراج و به‌کارگیری ویژگی‌ها، توانایی‌ها و رفتار حمله‌کننده، ارائه روش خودکار جهت تولید گراف وابستگی‌های شبکه، ارائه روش خودکار جهت استخراج پاسخ‌های ممکن بر روی شبکه و مدل‌سازی شبکه‌های بزرگ با کمک GMDP فعالیت نمود.

۸- منابع

[1] N. Stakhanova, S. Basu, and J. Wong, "A Taxonomy of Intrusion Response Systems," International Journal of Information and Computer Security, vol. 1, no. 1/2, pp. 169-184, 2007.

[2] A. A. Ghorbani, W. Lu, and M. Tavallaee, "Network Intrusion Detection and Prevention Concepts and Techniques," Springer US, 2009.

[3] M. M. Siraj and S. Z. M. Hashim, "Modeling Intrusion Alerts using IDMEF Data Model," University Technology of Malaysia, 2008.

[4] H. T. Elshousha and I. M. Osman, "Alert correlation in collaborative intelligent intrusion detection systems—A survey," Appl. Soft Comput., vol. 11, pp. 4349–4365, 2011.

[5] K. A. Alsubhi, "A Fuzzy-logic based Alert Prioritization Engine for IDSs: Architecture and Configuration," University of Waterloo, 2008.

[6] K. Alsubhi, I. Aib, and R. Boutaba, "FuzMet: a fuzzy-logic based alert prioritization engine for intrusion detection systems," Int J Netw Manag, vol. 22, no. 4, pp. 263-284, 2012.

[7] H. Q. Wang, G. F. Wang, Y. Lan et al., "A new automatic intrusion response taxonomy and its application," in The 8th Asia-Pacific Web Conference and Workshops (APWeb 2006), Harbin, People R China, pp. 999-1003, 2006.

[8] A. Avizienis, J. C. Laprie, B. Randell et al., "Basic concepts and taxonomy of dependable and secure computing," IEEE Trans Dependable Secure Comput, vol. 1, no. 1, pp. 11-33, 2004.

[9] G. Idowu, O. Enikuomehin, and S. Olasanoye, "Intrusion Response Systems: An Overview," Asian Journal of Information Technology ,vol. 10, no. 5, pp. 192-200, 2011.

[10] S. A. Zonouz, "Game-theoretic intrusion response and recovery," University of Illinois at Urbana-Champaign, 2011.

[11] N. B. A. Jumaat, "Incident prioritisation for intrusion response systems," Plymouth University, 2012.

[12] N. Stakhanova, S. Basu, and JohnnyWong, "A Cost-Sensitive Model for Preemptive Intrusion Response Systems," in 21st International Conference on Advanced Networking and Applications, Niagara Falls, ON, Canada, pp. 428-435, 2007.

[13] B. Foo, Y.-S. Wu, Y.-C. Mao et al., "ADEPTS: Adaptive intrusion response using attack graphs in an e-commerce environment," in The 2005 International Conference on Dependable Systems and Networks, Yokohama, Japan, pp. 508–517, 2005.

[14] M. E. Locasto, K. Wang, A. D. Keromytis et al., "FLIPS: Hybrid adaptive intrustion prevention," in The 8th international conference on Recent Advances in Intrusion Detection (RAID), Seattle, WA, USA, pp. 82-101, 2005.

[15] K. Haslum, A. Abraham, and S. Knapskog, "DIPS : A framework for distributed intrusion prediction and prevention using hidden markov models and online fuzzy risk assessment," in the 3rd International Symposium on Information Assurance and Security, Manchester, United Kingdom, pp. 183-188, 2007.

[16] Z. Zhang, P.-H. Ho, and L. He, "Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach," Comput. Secur., vol. 28, pp. 605-614, 2009.

[17] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, et al., "Risk-Aware Framework for Activating and Deactivating Policy-Based Response," in The Fourth International Conference on Network and System Security, Melbourne, VIC, pp. 207-215, 2010.

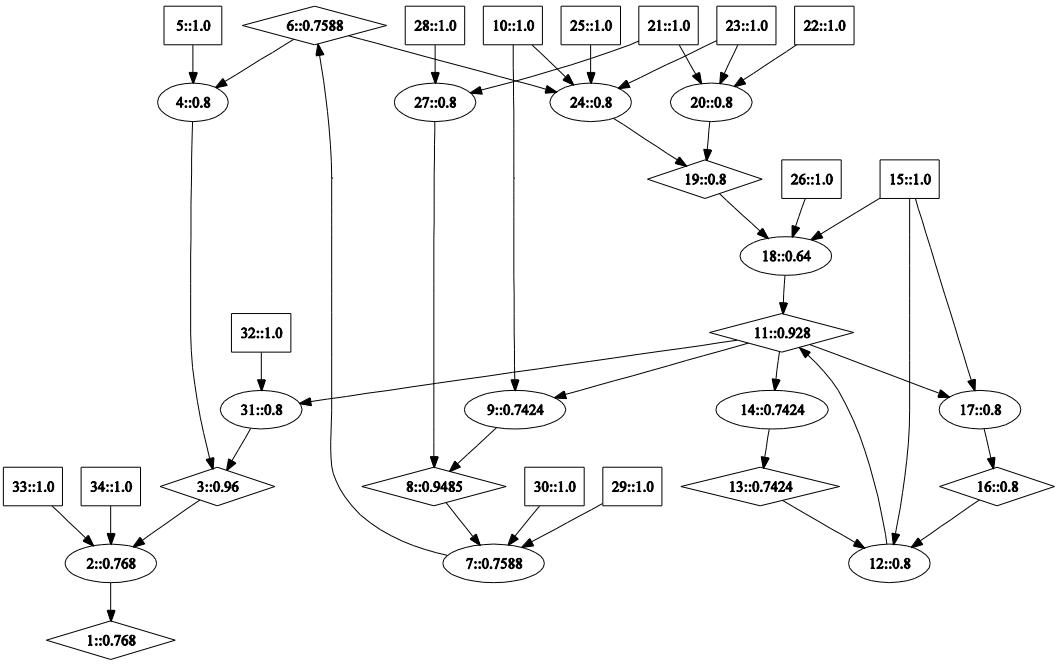
[18] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, et al., "A service dependency model for cost sensitive intrusion response," in The 15th European Conference on Research in Computer Security, Athens, Greece, pp. 626-642, 2010.

[19] A. Shameli-Sendi, J. Desfossez, M. Dagenais, et al., "A Retroactive-Burst Framework for Automated Intrusion Response System," Journal of Computer Networks and Communications, 2013.
[20] A. Shameli-Sendi, "System health monitoring and proactive response activation," Université de Montréal, Canada, 2013.
[21] C. Mu and Y. Li, "An intrusion response decision-making model based on hierarchical task network planning," Expert. Syst. Appl., vol. 37, no. 3, pp. 2465-2472, 2010.
[22] H. W. Njogu, L. Jiawei, J. N. Kiere, et al., "A comprehensive vulnerability based alert management approach for large networks," Future Generat Comput. Syst., vol. 29, pp. 27-45, 2013.
[23] S. Parsa, H. Saifi, and M.-H. Alaeian, "Providing a New Approach to Discovering Malware Behavioral Patterns Based on the Dependency Graph Between System Calls," Journal Of Electronical & Cyber Defence, vol. 4, no. 3, 2016 (In Persian).
[24] X. Ou, S. Govindavajhala, and A. W. Appel, "MulVAL: A Logic-based Network Security Analyzer," in USENIX Security, 2005.
[25] K. Kaynar, "A taxonomy for attack graph generation and usage in network security," Journal of Information Security and Applications, vol. 29, pp. 27-56, 2016.
[26] S. Wu, Y. Zhang, and W. Cao, "Network security assessment using a semantic reasoning and graph based approach," Comput. Electr. Eng., 2017.
[27] H. Li, Y. Wang, and Y. Cao, "Searching Forward Complete Attack Graph Generation Algorithm Based on Hypergraph Partitioning," Procedia Computer Science, vol. 107, pp. 27-38, 2017.
[28] M. Keramati, "Using Attack Graph for Improving Intrusion Response Systems in Computer Networks," Iran University of Science and Technology, 2011. (In Persian).
[29] B. Gruschke, "Integrated event management: Event correlation using dependency graphs," in Proceedings of the 9th IFIP/IEEE International Workshop on Distributed Systems: Operations & Management (DSOM 98), pp. 130-141, 1998.
[30] Y. Zhai, P. Ning, and J. Xu, "Integrating IDS Alert Correlation and OS-Level Dependency Tracking," in The 4th IEEE international conference on Intelligence and Security Informatics, pp. 272-284, 2006.
[31] T. Toth, and C. Kruegel, "Evaluating the impact of automated intrusion response mechanisms," in The 18th Annual Computer Security Applications Conference, Las Vegas, Nevada, pp. 301-310, 2002.
[32] I. Balepin, S. Maltsev, J. Rowe, et al., "Using specification-based intrusion detection for automated response," in The 6th International Symposium on Recent Advances in Intrusion Detection (RAID), Pittsburgh, PA, USA, 2003.
[33] A. Shameli-Sendi, and M. Dagenais, "ORCEF: Online response cost evaluation framework for intrusion response system," J. Netw. Comput. Appl., vol. 55, pp. 89-107, 2015.
[34] M. GhasemiGol and A .Ghaemi-Bafghi, "E-correlator: an entropy-based alert correlation system," Secur. Comm. Network, vol. 8, no. 5, pp. 822–836, 2015.
[35] M. Ester, H.-P. Kriegel, J. Sander, et al., "A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise," in 2nd International Conference on Knowledge Discovery and Data Mining (KDD-96), 1996.
[36] K. Julisch, "Clustering intrusion detection alarms to support root cause analysis," ACM Trans Inform Syst Secur, vol. 6, no. 4, pp. 443-471, 2003.
[37] M. GhasemiGol, A. Ghaemi-Bafghi, and H. Takabi, "A comprehensive approach for network attack forecasting," Comput. Secur., vol. 58, pp. 83-105, 2016.
[38] M. GhasemiGol, H. Takabi, and A. Ghaemi-Bafghi, "A foresight model for intrusion response management," Comput. Secur., vol. 62, pp. 73-94, 2016.
[39] T. L. Saaty, "Decision making with the analytic hierarchy process," Int J Serv Sci, vol. 1, no. 1, pp. 83-98, 2008.

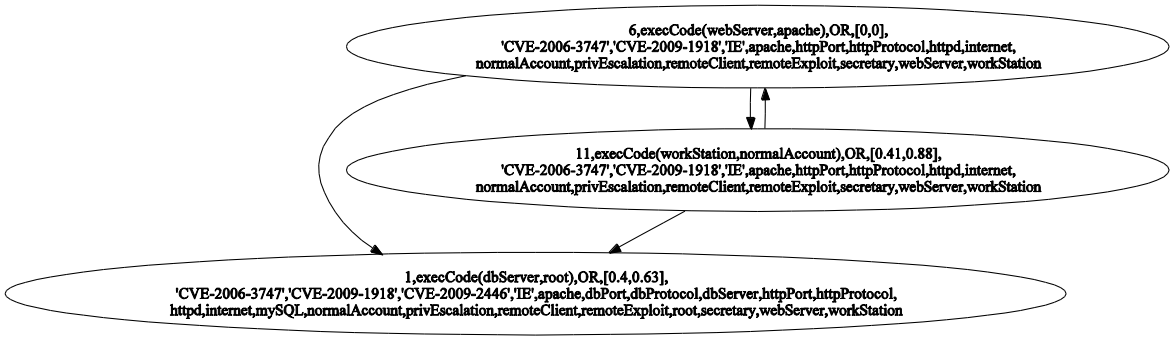
پیوست

جدول (پ-۱): جزئیات گره‌های موجود در گراف حمله شکل (۱۸)

1,"execCode(dbServer,root)","OR",0.768
2,"RULE 2 (remote exploit of a server program)","AND",0.768
3,"netAccess(dbServer,dbProtocol,dbPort)","OR",0.96
4,"RULE 5 (multi-hop access)","AND",0.8
5,"hacl(webServer,dbServer,dbProtocol,dbPort)","LEAF",1.0
6,"execCode(webServer,apache)","OR",0.7588
7,"RULE 2 (remote exploit of a server program)","AND",0.7588
8,"netAccess(webServer,httpProtocol,httpPort)","OR",0.9485
9,"RULE 5 (multi-hop access)","AND",0.7424
10,"hacl(workStation,webServer,httpProtocol,httpPort)","LEAF",1.0
11,"execCode(workStation,normalAccount)","OR",0.928
12,"RULE 0 (When a principal is compromised any machine he has an account on will also be compromised)","AND",0.8
13,"canAccessHost(workStation)","OR",0.7424
14,"RULE 8 (Access a host through executing code on the machine)","AND",0.7424
15,"hasAccount(secretary,workStation,normalAccount)","LEAF",1.0
16,"principalCompromised(secretary)","OR",0.8
17,"RULE 12 (password sniffing)","AND",0.8
18,"RULE 3 (remote exploit for a client program)","AND",0.64
19,"accessMaliciousInput(workStation,secretary,'IE')","OR",0.8
20,"RULE 22 (Browsing a malicious website)","AND",0.8
21,"attackerLocated(internet)","LEAF",1.0
22,"hacl(workStation,internet,httpProtocol,httpPort)","LEAF",1.0
23,"inCompetent(secretary)","LEAF",1.0
24,"RULE 24 (Browsing a compromised website)","AND",0.8
25,"isWebServer(webServer)","LEAF",1.0
26,"vulExists(workStation,'CVE-2009-1918','IE',remoteClient,privEscalation)","LEAF",1.0
27,"RULE 6 (direct network access)","AND",0.8
28,"hacl(internet,webServer,httpProtocol,httpPort)","LEAF",1.0
29,"networkServiceInfo(webServer,httpd,httpProtocol,httpPort,apache)","LEAF",1.0
30,"vulExists(webServer,'CVE-2006-3747',httpd,remoteExploit,privEscalation)","LEAF",1.0
31,"RULE 5 (multi-hop access)","AND",0.8
32,"hacl(workStation,dbServer,dbProtocol,dbPort)","LEAF",1.0
33,"networkServiceInfo(dbServer,mySQL,dbProtocol,dbPort,root)","LEAF",1.0
34,"vulExists(dbServer,'CVE-2009-2446',mySQL,remoteExploit,privEscalation)","LEAF",1.0



شکل (پ-۱): گراف حمله تولیدشده برای شبکه نمونه شکل (۷)



شکل (پ-۲): گراف پیشگوی حمله برای شبکه نمونه شکل (۷)

جدول (پ-۲): حداقل و حداکثر احتمال رخدادن هر گره از گراف حمله در شبکه نمونه شکل (۷)

	$\underline{P}(n_i)$	$\overline{P}(n_i)$
$\hat{P}(n_1)$	۰/۲۰۰۰	۰/۵۰۷۰
$\hat{P}(n_2)$	۰/۲۰۰۰	۰/۵۰۷۰
$\hat{P}(n_3)$	۰/۰۰۰۰	۰/۹۶۰۰
$\hat{P}(n_4)$	۰/۳۰۰۰	۰/۶۰۷۰
$\hat{P}(n_5)$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_6)$	۰/۲۰۰۰	۰/۵۴۰۰
$\hat{P}(n_7)$	۰/۲۰۰۰	۰/۵۴۰۰
$\hat{P}(n_8)$	۰/۰۰۰۰	۰/۹۴۸۵
$\hat{P}(n_9)$	۰/۲۰۰۰	۰/۷۴۲۴
$\hat{P}(n_{10})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{11})$	۰/۴۰۰۰	۰/۸۷۵۱
$\hat{P}(n_{12})$	۰/۲۰۰۰	۰/۴۷۵۱

	$\underline{P}(n_i)$	$\overline{P}(n_i)$
$\hat{P}(n_{13})$	۰/۴۰۰۰	۰/۸۷۵۱
$\hat{P}(n_{14})$	۰/۴۰۰۰	۰/۸۷۵۱
$\hat{P}(n_{15})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{16})$	۰/۳۰۰۰	۰/۶۷۵۱
$\hat{P}(n_{17})$	۰/۳۰۰۰	۰/۶۷۵۱
$\hat{P}(n_{18})$	۰/۳۰۰۰	۰/۶۴۰۰
$\hat{P}(n_{19})$	۰/۰۰۰۰	۰/۹۶۰۰
$\hat{P}(n_{20})$	۰/۴۰۰۰	۰/۸۰۰۰
$\hat{P}(n_{21})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{22})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{23})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{24})$	۰/۲۰۰۰	۰/۶۰۷۰

	$\underline{P}(n_i)$	$\overline{P}(n_i)$
$\hat{P}(n_{25})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{26})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{27})$	۰/۳۰۰۰	۰/۷۴۰۰
$\hat{P}(n_{28})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{29})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{30})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{31})$	۰/۲۰۰۰	۰/۷۴۲۴
$\hat{P}(n_{32})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{33})$	۱/۰۰۰۰	۱/۰۰۰۰
$\hat{P}(n_{34})$	۱/۰۰۰۰	۱/۰۰۰۰

جدول (پ-۳): گوشه‌ای از تصمیمات انتخاب‌شده توسط سامانه‌های پاسخ آینده‌نگر و غیرآینده‌نگر در وضعیت‌های امنیتی مختلف شبکه نمونه شکل (۷)

تصمیم سامانه پاسخ آینده‌نگر	تصمیم سامانه پاسخ غیرآینده‌نگر	وضعیت امنیتی شبکه
R3-VL-workStation	R15-VL-dbServer	R1R7R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R7R10R13R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R7R8R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R7R8R10R13R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R8R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R8R10R13R14a1a2a3
-R1-NL-workStation	R9-VL-WebServer	R1R17a1a2a3
-R1-NL-workStation	R9-VL-WebServer	R1R16a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R7R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R7R10R13R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R7R8R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R7R8R10R13R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R8R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R8R10R13R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R10R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R10R13R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R10R11R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R10R11R13R14a1a2a3
-R1-NL-workStation	R9-VL-WebServer	R1R2R17a1a2a3
-R1-NL-workStation	R9-VL-WebServer	R1R2R16a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R11R13a1a2a3
R3-VL-workStation	R15-VL-dbServer	R1R2R11R13R14a1a2a3
R15-VL-dbServer	-R2-AL-workStation	R2R4R11R17a1a2a3
R3-VL-workStation	R15-VL-dbServer	R2R7R10R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R2R7R8R10R14a1a2a3
R3-VL-workStation	R15-VL-dbServer	R2R8R10R14a1a2a3
R15-VL-dbServer	R9-VL-WebServer	R2R17a1a2a3
-R2-AL-workStation	R9-VL-WebServer	R2R16a1a2a3
R15-VL-dbServer	-R13-NL-dbServer	R4R11R13a1a2a3
R15-VL-dbServer	-R13-NL-dbServer	R4R11R13R14a1a2a3
-R13-NL-dbServer	R3-VL-workStation	R7R13R16a1a2a3
-R13-NL-dbServer	R3-VL-workStation	R7R13R14R16a1a2a3
-R17-SL-dbServer	R3-VL-workStation	R7R16R17a1a2a3
-R13-NL-dbServer	R3-VL-workStation	R7R8R13R16a1a2a3
-R13-NL-dbServer	R3-VL-workStation	R7R8R13R14R16a1a2a3
-R17-SL-dbServer	R3-VL-workStation	R7R8R16R17a1a2a3
-R13-NL-dbServer	R3-VL-workStation	R8R13R16a1a2a3
-R13-NL-dbServer	R3-VL-workStation	R8R13R14R16a1a2a3
…	…	…

Journal of Electronical & Cyber Defence
Vol. 6, No. 3, 2018, Serial No. 23

A Foresight Framework for Intrusion Response Systems in Computer Networks

M. Ghasemi Gol

*University of Birjand

(Received: 12/03/2017, Accepted: 01/11/2017)

ABSTRACT

Today, the number of alerts issued by network security systems has increased significantly and network administrators encounter new problems in handling the issued alerts and responding to them. As managing and responding to such a large number of alerts is difficult, alert management and intrusion response system (IRS) are the main part of the security protection systems including intrusion detection systems. The main task of alert management is to reveal the attack details to IRS. Subsequently, the appropriate responses are applied to reduce the attack damage and recover the compromised computer networks back to their normal operational mode. In the literature, researchers have investigated alert management techniques and IRS solutions separately, despite the fact that alert management is one of the basic requirements of response process and its outcome directly affects the IRS performance. Alert management design should provide the necessary information about the attacks to the response system according to its type and requirements. This information along with information from network resources present the current state of the network to IRS. However, if decisions taken by the response system is only based on the current network status, the total cost of the network will increase over the time. Therefore with a futuristic concept and considering the present available information and all possible coming states, decision making process in the response system can be improved. In this paper, using a futuristic approach we seek to propose optimal solutions for confronting already-occurred and future-probable attacks. To achieve this goal, the proposed framework contains two subsystems: attacks and alerts modeling, and response modeling. In the first subsystem, we analyze the IDS alerts to find the similarity and causality relationships. We also present a comprehensive approach for network attack forecasting to obtain some useful predictions about the future states of the network. In the second subsystem, the response analyzer presents a multilevel response model to categorize intrusion responses. It also provides a foresight model to estimate the response cost by considering IDS alerts, network dependencies, attack damage, response impact, and the probability of potential attacks. Finally, models are proposed to make the best decision based on available information about the present and all possible coming states. Simulation results for different scenarios show that the response system, with a prospective vision, steers the network toward desired states with reduced cost of attack and response.

Keywords: Intrusion Response System, Foresight, Alert Management, Uncertainty-aware Attack Graph, Network Dependency Graph, Markov Decision Process

* Corresponding Author Email: ghasemigol@birjand.ac.ir