تشخیص نفوذ مبتنی بر مدل‌های مخفی مارکوف: روش‌ها، کاربردها و چالش‌ها

علی احمدیان رمکی [۱]، عباس رسول‌زادگان [۲،*] و عباس جوان جعفری [۳]

اطلاعات مقاله

دریافت مقاله: ۱۳۹۵/۰۴/۱۴

پذیرش مقاله: ۱۳۹۶/۰۴/۱۸

واژگان کلیدی:

امنیت سیستم،

امنیت شبکه،

سیستم تشخیص نفوذ،

تشخیص نفوذ،

مدل مخفی مارکوف.

چکیده

امروزه، با توجه به گسترش استفاده از شبکه اینترنت، امنیت سیستم‌های نرم‌افزاری به‌عنوان یکی از مهم‌ترین مؤلفه‌های ضروری در کیفیت خدمات فن‌آوری اطلاعات به‌حساب می‌آید. علاوه بر راهکارهای امنیتی سنتی نظیر رمزنگاری، دیواره آتش و مکانیزم‌های کنترل دسترسی در سیستم‌های نرم‌افزاری، استفاده از سیستم‌های تشخیص نفوذ، امری ضروری و انکارناپذیر است. تاکنون روش‌های زیادی برای تشخیص نفوذهای احتمالی در سیستم‌های نرم‌افزاری معرفی شده‌اند. این روش‌ها بر اساس معیارهایی به دسته‌های متفاوتی تقسیم می‌شوند. یکی از این دسته روش‌های مهم، روش‌های مبتنی بر یادگیری ماشین هستند. مزیت اصلی این روش‌ها، کاهش دخالت عامل انسانی در تشخیص نفوذها و فعالیت‌های ناهنجار است. یکی از مهم‌ترین روش‌های تشخیص نفوذ مبتنی بر یادگیری ماشین، استفاده از مدل‌های مخفی مارکوف می‌باشد. سه مزیت بارز این روش، دقت زیاد در تشخیص نفوذ، قابلیت تشخیص نفوذهای ناشناخته جدید و نیز بازنمایی دانش کسب شده به‌صورت بصری است تا عامل انسانی بتواند بر اساس اطلاعات مدل، تصمیم‌گیری‌های لازم مدیریتی را به‌عمل آورد. در این مقاله، با توجه به استفاده متعدد از مدل‌های مخفی مارکوف برای تشخیص نفوذ از یک سو و عدم وجود مروری جامع در این زمینه از سوی دیگر، قصد داریم که با استفاده از یک فرآیند تحقیق نظام‌مند، مروری بر پژوهش‌های انجام شده در این حوزه صورت داده و بر مبنای نقد و تحلیل مزایا، محدودیت‌ها و کاربردهای روش‌های موجود، به معرفی مستدل چالش‌ها و مسائل باز این حوزه بپردازیم.

۱-مقدمه

امروزه، با افزایش استفاده از خدمات شبکه اینترنت، امنیت اطلاعات و داده‌های موجود در سیستم‌های نرم‌افزاری به یک چالش اصلی برای پژوهش‌گران فعال در این حوزه تبدیل شده است [۱، ۴]. سیستم‌های نرم‌افزاری مختلف، نیازمند سطوح مختلفی از امنیت، به‌عنوان یک ویژگی کیفی در ارائه خدمات هستند. برای تحقق سطح مطلوب امنیت در سیستم‌های نرم‌افزاری، علاوه بر ابزارها و تکنیک‌هایی نظیر دیواره‌های آتش[۱]، لیست‌های کنترل دسترسی[۲]، مکانیزم‌های تصدیق هویت[۳]، سیستم‌های دیگری به نام سیستم‌های تشخیص نفوذ[۴] (IDSs) موردنیاز هستند تا بتوانند در صورتی که نفوذگر از دیواره‌ی آتش، ضدویروس و دیگر تجهیزات امنیتی نفوذ کرد و وارد سیستم شد، آن را تشخیص داده و چاره‌ای برای آن اتخاذ نماید [۱، ۳].

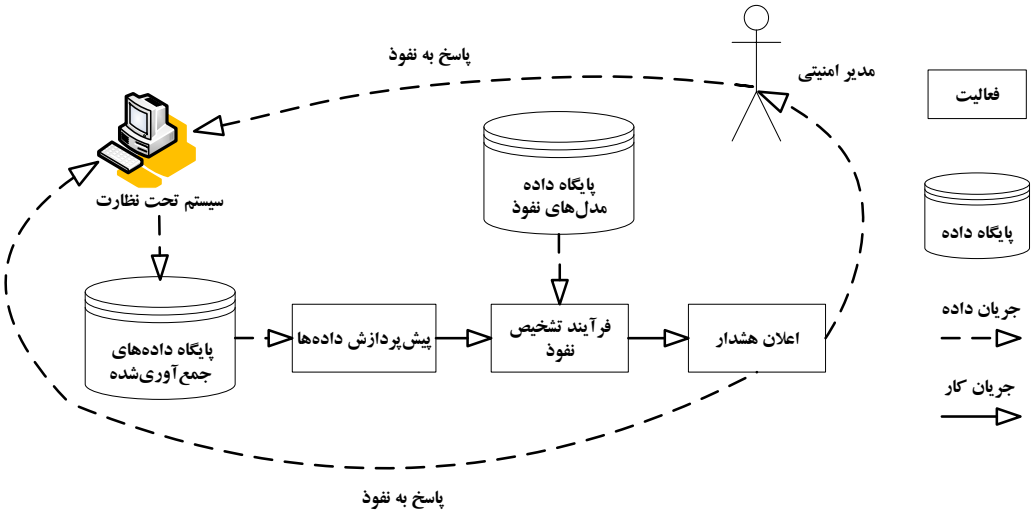
* پست الکترونیک نویسنده مسئول: rasoolzadegan@um.ac.ir

۱. دانشجوی دکتری تخصصی، گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد

۲. دانشیار و عضو هیأت علمی، گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد

۳. دانش‌آموخته کارشناسی ارشد، گروه مهندسی کامپیوتر، دانشگاه فردوسی مشهد، مشهد

1. Firewall
2. Access Control List
3. Authentication
4. Intrusion Detection System



شکل۱- سازمان اصلی یک سیستم تشخیص نفوذ

سه اصل پایه‌ای امنیت: محرمانگی[1]، جامعیت[2] و دسترس‌پذیری[3]، در مورد هنجار یا ناهنجار بودن آن‌ها تصمیم‌گیری می‌نمایند [۲]. سازمان اصلی یک سیستم تشخیص نفوذ در شکل (۱) نشان داده شده است که در آن پیکان‌های ممتد نشان‌دهنده جریان‌های داده و پیکان‌های خط‌چین نشان‌دهنده جریان‌های کاری می‌باشد.

سیستم‌های تشخیص نفوذ در مواجهه با نقص سیاست‌های امنیتی، هشداری را جهت اعلان وضعیت جاری امنیتی، برای مدیران سطح بالا تولید می‌نمایند. به منظور مقابله با نفوذگران به سیستم‌های نرم‌افزاری، روش‌های متعددی تحت عنوان روش‌های تشخیص نفوذ معرفی شده است که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم نرم‌افزاری را بر عهده دارند.

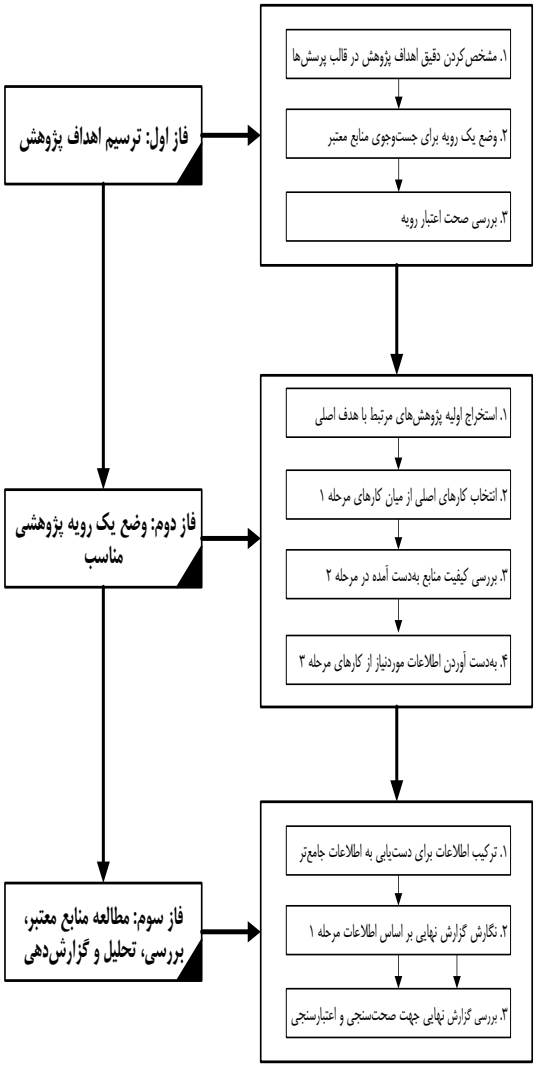
تلاش‌های محققان حوزه امنیت، منجر به ارائه روش‌ها و مدل‌های متنوعی برای تشخیص نفوذهای احتمالی مهاجمان به سیستم‌های نرم‌افزاری شده است [۲، ۳، ۴]. در پژوهش‌های اخیر سعی شده است تا با استفاده از روش‌های یادگیری ماشین[4]، با ایجاد مدل‌های هوشمند، الگوهای رفتاری پرخطر تشخیص داده شود [۴]. از جمله مهم‌ترین مزیت این روش‌ها، عدم دخالت عامل انسانی در تفسیر داده‌های مورد تحلیل می‌باشد [۳].

یکی از روش‌های بسیار قدرتمند مبتنی بر یادگیری ماشین، بهره‌گیری از مدل‌های مخفی مارکوف[5] (HMM) و توسعه گونه‌های متنوعی از این مدل‌ها، در جهت تشخیص نفوذهای احتمالی و نیز تمیز دادن فعالیت هنجار از یک فعالیت ناهنجار می‌باشد [۳، ۴، ۵]. این عمل با استفاده از مقایسه رفتار مشاهده شده با آن‌چه که به عنوان یک فعالیت هنجار سیستم نرم‌افزاری مدل شده است، صورت می‌گیرد. تلاش محققان در ارائه روش‌های مختلف تشخیص نفوذ مبتنی بر مدل مخفی مارکوف، منجر به معرفی گونه‌های متنوعی از مدل‌های مخفی مارکوف شده است. تاکنون تعداد محدودی پژوهش‌های مروری بر روی تشخیص نفوذ با استفاده از مدل مخفی مارکوف صورت گرفته است [۶، ۸، ۹] که همگی آن‌ها از جامعیت برخوردار نبوده و به تحلیل هر یک از روش‌های مبتنی بر مدل مخفی مارکوف نپرداخته‌اند . در این مقاله، با استفاده از یک روش تحقیق نظام‌مند ضمن بررسی کاربردهای مدل مخفی مارکوف در حیطه‌های مختلف تشخیص نفوذ، روش‌های مختلف تشخیص نفوذ مبتنی بر این مدل، چالش‌ها و مزایای هر روش مورد تحلیل و بررسی قرار گرفته است. در انتها نیز ضمن بررسی معیارهای کمّی کیفیت روش‌های ارائه شده مبتنی بر مدل مخفی مارکوف، به تشریح چالش‌ها و مسائل باز پژوهشی در این حوزه پرداخته شده است.

یکی از مزیت‌های اصلی پژوهش جاری استفاده از یک روش تحقیق نظام‌مند[6] [۱۰، ۱۱] در گردآوری کارهای پژوهشی، انتخاب، تحلیل و بررسی پژوهش‌های موجود بوده است.

1. Confidentiality
2. Integrity
3. Availability
4. Machine Learning
5. Hidden Markov Model
6. Systematic Literature Review

هدف از به‌کارگیری یک روش تحقیق نظام‌مند برای انجام یک پژوهش مروری، فراهم آوردن مروری جامع، کامل و عادلانه می‌باشد تا با استفاده از این فرآیند بتوان، ۱) تمامی پژوهش‌های موجود در یک حوزه را جمع‌آوری و مورد بررسی قرار داد، ۲) تمامی منابع موجود که شامل اطلاعاتی درباره مسئله مورد پژوهش هستند را مورد بررسی قرار داد و ۳) از عدم مطالعه یک کار پژوهشی، به‌طور عمدی و یا سهوی، جهت سوق دادن یافته‌های پژوهشی به سمت یک هدف خاص جلوگیری نمود.



شکل۲- گام‌های روش تحقیق نظام‌مند مورد استفاده در پژوهش جاری [۱۰]

تاکنون، چند روش تحقیق نظام‌مند معتبر معرفی شده است که بسیار مورد استفاده پژوهشگران حوزه‌های مختلف قرار گرفته‌اند [۱۰، ۱۱]. در شکل (۲)، نمایی از روش تحقیق نظام‌مند مورد استفاده در این پژوهش نشان داده شده است [۱۰]. با استفاده از این روش تحقیق نظام‌مند، پس از جمع‌آوری پژوهش‌های موجود سعی شده است تا پژوهش‌های معتبر، مورد بررسی قرار گرفته و یافته‌های پژوهش بر اساس تحلیل نتایج این مقالات و در فضایی عادلانه صورت گیرد.

در پژوهش جاری با کلمات کلیدی مانند: سیستم تشخیص نفوذ، مدل مخفی مارکوف، روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف و معیارهای ارزیابی سیستم‌های تشخیص نفوذ و در منابعی نظیر: « Springer Online Journal Collection»، «Scopus»، «IEEEXplore»، «Pad - پایگاه اشتراک داده دانشگاه فردوسی مشهد»، «ACM Digital Library»، «Google Scholar» و «Science Direct» به مرور نظام‌مند تحقیقات صورت پذیرفته در حوزه مربوطه پرداخته‌ایم و در فرآیند تحقیق، منابع به زبان انگلیسی و فارسی را مورد بررسی قرار داده‌ایم. البته بخش عمده‌ای از منابع مورد تحقیق را مقالات معتبر تشکیل داده‌اند. برای تعیین این که آیا مقالات به‌دست آمده حاوی اطلاعات مرتبط هستند، عنوان و چکیده‌ی آن‌ها را مورد مطالعه قرار داده‌ایم که در نهایت نتایج یافته‌های ما بر اساس پژوهش‌های موجود صورت گرفته در این حوزه در جدول ۱ نشان داده شده است. علاوه بر این، فایل مربوط به محتویات تحقیق نظام‌مند مورد استفاده برای مسئله مورد پژوهش در مرجع [۱۲] قابل دسترسی است.

از جمله مهم‌ترین نوآوری‌های موجود در پژوهش جاری می‌توان به موارد زیر اشاره نمود:

- ایجاد یک دسته‌بندی جدید و جامع بر اساس مرور نظام‌مند پژوهش‌های پیشین موجود در حوزه تشخیص نفوذ مبتنی مدل مخفی مارکوف
- بررسی روش‌های مختلف تشخیص نفوذ معرفی شده مبتنی بر مدل مخفی مارکوف
- ارزیابی کیفیت روش‌های مختلف تشخیص نفوذ معرفی شده مبتنی بر مدل مخفی مارکوف بر اساس معیارهای ارزیابی کمّی موجود

ادامه مقاله به‌صورت زیر سازمان‌دهی شده است. ابتدا در بخش دوم به تبیین جایگاه تشخیص نفوذ به کمک مدل مخفی مارکوف پرداخته شده است. در بخش سوم دسته‌بندی جامعی از به‌کارگیری این مدل‌ها برای کاربردهای تشخیص نفوذ ارائه شده است. در بخش چهارم، روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف معرفی شده و ضمن تشریح هر روش، مزایا، محدودیت‌ها و

چالش‌های هر یک از آن‌ها تبیین شده است. در بخش پنجم، معیارهای کمّی برای اندازه‌گیری کیفیت روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف بیان شده است و روش‌های مختلف مبتنی بر این مدل، از این منظر با یکدیگر مقایسه شده‌اند. در بخش ششم به مقایسه پژوهش جاری با دیگر پژوهش‌های مروری موجود پرداخته شده است. در بخش هفتم، با تحلیل‌های صورت گرفته در بخش‌های قبلی، چالش‌ها و مسائل باز پژوهشی موجود در این حیطه تشریح شده است و در انتها در بخش هشتم نیز نتیجه‌گیری از پژوهش آورده شده است.

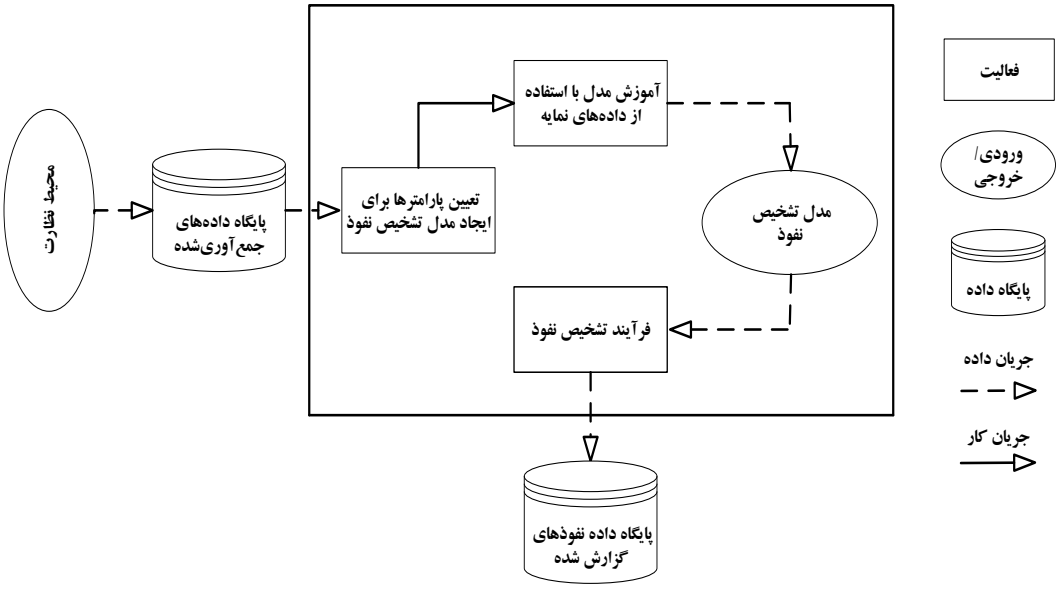
۲- جایگاه مدل مخفی مارکوف در تشخیص نفوذ

تاکنون روش‌های بسیاری برای تشخیص نفوذ در سیستم‌های نرم‌افزاری معرفی شده‌اند که هر کدام دارای ویژگی‌های مربوط به خود می‌باشند و مزایا و معایب خاص خود را دارند [۱۳، ۱۴، ۱۵]. غالب روش‌های تشخیص نفوذ دارای سه مرحله اصلی هستند که در شکل (۳) نشان داده شده است. این سه مرحله عبارتند از:

- انتخاب ویژگی[1] برای ایجاد مدل تشخیص نفوذ: ورودی این مرحله، داده‌های جمع‌آوری شده (نمایه) از سیستم هدف (محیط نظارت) است که هر یک بیانگر یک رخداد امنیتی بر روی سیستم هدف بوده و دارای تعداد زیادی ویژگی می‌باشند. در این مرحله با استفاده از روش‌های انتخاب ویژگی جهت کاهش ابعاد داده‌های ورودی، ویژگی‌های اصلی و مهم برای ساخت مدل تشخیص نفوذ استخراج می‌گردند.

جدول ۱- نتایج یافته‌های پژوهشی بر اساس روش تحقیق نظام‌مند

ردیف	نوع پژوهش	تعداد
۱	کنفرانس‌های ملی	۵
۲	کنفرانس‌های بین‌المللی	۱۷
۳	کارگاه‌های بین‌المللی	۸
٤	نشریات معتبر علمی- پژوهشی و ISI	۲۰
۵	پایان‌نامه‌های تحصیلات تکمیلی	۵
٦	کتب مرجع	٦
۷	پژوهشگران	۲۳



شکل۳- مراحل کلی یک روش تشخیص نفوذ جهت ایجاد مدل رفتاری از یک سیستم

- آموزش مدل[2] با استفاده از داده‌های نمایه: در این مرحله با استفاده از داده‌های موجود در نمایه و به کمک روش‌های مختلف آموزش، یک مدل تشخیص نفوذ از رفتار سیستم هدف به‌دست می‌آید تا در مراحل بعدی، جهت تمیز دادن فعالیت‌های هنجار و ناهنجار مورد استفاده قرار گیرد. فرآیند آموزش می‌تواند با

1. Feature Selection

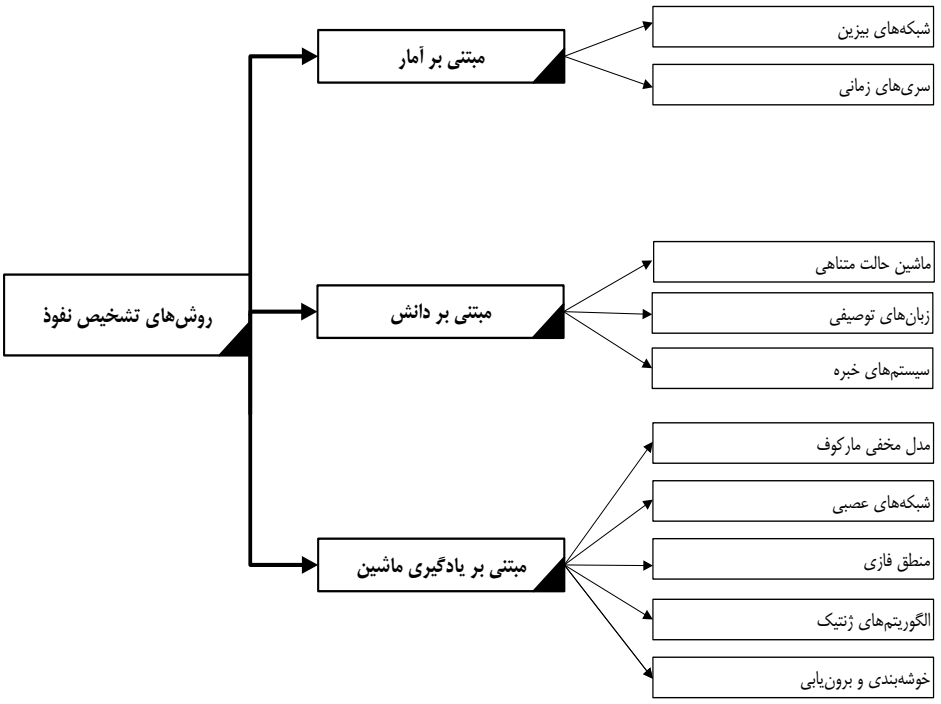
2. Model Training

استفاده از روش‌های مختلف به‌صورت خودکار و یا دستی صورت بگیرد.

- فرآیند تشخیص نفوذ: در این مرحله، با استفاده از مدل رفتاری به‌دست آمده در مرحله قبل، به ارزیابی مشاهدات دریافتی بر روی سیستم هدف پرداخته می‌شود. به‌عبارت دیگر، وقتی مدل رفتاری سیستم در دسترس باشد، می‌توان با استفاده از آن، رفتار مشاهده شده جاری را ارزیابی نمود و یک انحراف معیار بین مدل رفتاری نهایی سیستم و رفتار مشاهده شده جاری به‌دست آورد. اگر انحراف معیار به‌دست آمده از یک آستانه از پیش تعریف‌شده[1] بیشتر باشد، هشداری مبنی بر بروز یک ناهنجاری تولید و ثبت خواهد شد.

فرآیند ایجاد مدل تشخیص نفوذ (خروجی مرحله آموزش مدل با استفاده از داده‌های نمایه) بر اساس نوع پردازش‌های لازم می‌تواند به سه دسته اصلی مبتنی بر آمار، مبتنی بر دانش و مبتنی بر یادگیری ماشین تقسیم‌بندی گردد [۱۶، ۱۷، ۱۸، ۱۹، ۲۰]. روش‌های موجود در هر دسته در شکل (۴) نشان داده شده است. در ادامه، هر دسته به‌طور مختصر تشریح شده است.

- روش‌های مبتنی بر آمار[2]: در روش‌های تشخیص نفوذ مبتنی بر آمار، مشاهدات موردنظر (ترافیک شبکه در NIDS و دنباله فرامین در HIDS) ثبت شده و یک نمایه برای نمایش رفتارهای هنجار آن ایجاد می‌شود. این نمایه می‌تواند بر اساس معیارهایی نظیر نرخ ترافیک، تعداد بسته‌ها برای هر پروتکل، تعداد اتصالات، تعداد آدرس‌های IP مختلف برای سیستم‌های NIDS و از طرف دیگر تعداد فرامین مورد استفاده، نوع ترتیب فرامین مورد استفاده، میزان مصرف منابع سیستم برای سیستم‌های HIDS ایجاد گردد.
- روش‌های مبتنی بر دانش[3]: دسته دیگر از روش‌های تشخیص نفوذ، روش‌های مبتنی بر دانش هستند که با عنوان سیستم‌های خبره نیز یاد می‌شوند. این روش‌ها قصد دارند تا داده‌های ممیّزی[4] موجود در نمایه را بر اساس یک مجموعه‌ای از قوانین و با انجام سه گام زیر طبقه‌بندی نمایند: ۱) خصیصه‌ها و کلاس‌های مختلف از داده‌های آموزشی شناسایی می‌گردند، ۲) یک مجموعه‌ای از قوانین طبقه‌بندی بر اساس ویژگی‌ها یا خصیصه‌ها تعیین می‌گردند و ۳) داده‌های ممیزی بر اساس قوانین تعریف شده، طبقه‌بندی می‌گردند.



شکل۴- جایگاه مدل مخفی مارکوف در روش‌های دسته‌های سه‌گانه تشخیص نفوذ

1. Predefined Threshold
2. Statistical-based Methods
3. Knowledge-based Methods
4. Audit Data

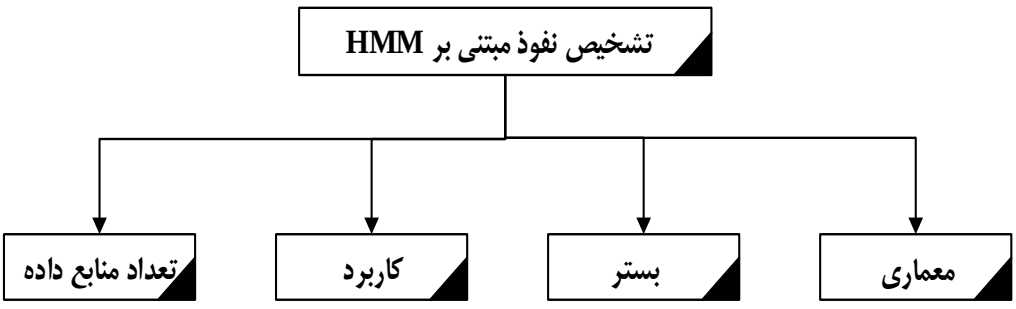
- روش‌های مبتنی بر یادگیری ماشین[1]: تکنیک‌های مبتنی بر یادگیری ماشین بر اساس ایجاد یک مدل صریح یا ضمنی از مشاهدات دریافتی عمل می‌نمایند که در ادامه قادر خواهند بود تا با استفاده از تحلیل الگوها، دنباله مشاهدات دریافتی جدید را طبقه‌بندی نمایند. یکی از ویژگی‌های منحصر به‌فرد این روش‌ها، نیاز آن‌ها به برچسب‌گذاری[2] داده‌هایی است که قرار است برای ایجاد مدل رفتاری آموزش داده شوند؛ نیازی که خود استفاده زیاد از منابع را به دنبال خواهد داشت.

در جدول ۲، مزایا و چالش‌های استفاده از سه دسته روش‌های بیان شده برای کاربردهای تشخیص نفوذ، با یکدیگر مقایسه شده‌اند. همان‌گونه که در جدول ۲ مشاهده می‌شود، با توجه به مزایای منحصر به فرد روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف یعنی، ۱) دقت زیاد این مدل در تشخیص نفوذهای احتمالی، ۲) قابلیت تشخیص نفوذهای ناشناخته جدید و ۳) بازنمایی دانش کسب شده در قالب یک نمایش گرافیکی تا عامل انسانی بتواند بر اساس اطلاعات مدل، تصمیم‌گیری‌های لازم مدیریتی را به‌عمل آورد، از یک سو و از سوی دیگر با توجه به تعدد استفاده از این روش برای ایجاد مدل‌های تشخیص نفوذ [۶، ۸، ۹]، در ادامه این مقاله سعی می‌کنیم با تمرکز بیشتر بر روی این مدل‌ها، مروری بر پژوهش‌های انجام شده در این حوزه صورت داده و بر مبنای نقد و تحلیل مزایا، محدودیت‌ها و کاربردهای روش‌های موجود، به معرفی مستدل چالش‌ها و مسائل باز این حوزه بپردازیم.

۳- تشخیص نفوذ مبتنی بر HMM

در این بخش قصد داریم تا پژوهش‌های صورت گرفته را از جنبه‌های مختلف، دسته‌بندی نماییم و در هر دسته مهم‌ترین کارهای پژوهشی صورت گرفته معتبر را به‌اختصار شرح دهیم. بعد از یک مرور ادبیاتی جامع، سعی کرده‌ایم تا یک طبقه‌بندی جامع و جدیدی برای مبحث تشخیص نفوذ به کمک مدل مخفی مارکوف ارائه نماییم. تاکنون تعداد محدودی پژوهش‌های مروری بر روی تشخیص نفوذ با استفاده از مدل مخفی مارکوف صورت گرفته است که از جمله آن‌ها می‌توان به پژوهش‌های [۶، ۸، ۹] اشاره کرد. این پژوهش‌ها، جامعیت لازم را در مرور کارهای پیشین ندارند و هر یک تنها از یک منظر به بیان کارهای موجود پرداخته‌اند. ضمن این که پژوهش‌های مروری موجود، فاقد دسته‌بندی خاصی از دیدگاه‌های مختلف بوده و تنها به شرح کارهای موجود پرداخته‌اند.

در این مقاله، ما یک طبقه‌بندی جامع و جدیدی را برای روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف ارائه می‌دهیم که در ابعاد اصلی آن در شکل (۵) نشان داده شده است. این طبقه‌بندی سعی می‌کند تا یک دید کلی را درباره مسئله تشخیص نفوذ به کمک مدل مخفی مارکوف ارائه دهد. در این طبقه‌بندی، علاوه بر تمرکز بر روی روش‌های مختلف مدل مخفی مارکوف برای کاربرد تشخیص نفوذ، جنبه‌های دیگری نظیر تعداد منابع داده مورد استفاده جهت آموزش مدل، بسترهای موجود برای به‌کارگیری روش‌های تشخیص نفوذ و کاربردهای مختلف آن در حوزه امنیت سیستم‌های نرم‌افزاری لحاظ می‌گردد. در پژوهش جاری، به‌دلیل اهمیت بیشتر معماری‌های متنوع مبتنی بر مدل مخفی مارکوف، بررسی این معماری‌ها به‌طور جداگانه در بخش ۴ صورت گرفته است. در ادامه این بخش، به تشریح سایر دسته‌های طبقه‌بندی پیشنهادی می‌پردازیم.



شکل۵- دسته‌بندی تکنیک‌های تشخیص نفوذ مبتنی بر HMM از منظرهای مختلف

1. Machine Learning-based Methods

2. Labeling

جدول۲- مقایسه مزایا و معایب دسته‌های سه‌گانه تشخیص نفوذ

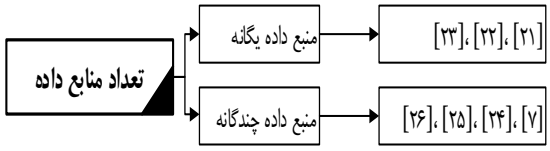
ردیف	نوع روش	مزایای روش	معایب روش
۱	روش‌های مبتنی بر آمار	- عدم وابستگی به دانش قبلی درباره فعالیت‌های هنجار سیستم - دقت بالا در تشخیص فعالیت‌های مخرّب	- امکان آموزش مدل توسط افراد مهاجم - دشواری تنظیم پارامترها و معیارها - ضعف در تشخیص حملات جدید ناشناخته
۲	روش‌های مبتنی بر دانش	- کارایی برای کاربردهای با حجم داده زیاد (کلان داده[1]) - انعطاف‌پذیری و گسترش‌پذیری زیاد - میزان پایین تعداد تشخیص‌های نادرست	- دشواری و زمان‌بر بودن فرآیند دست‌یابی به دانش/داده با کیفیت بالا برای آموزش مدل - وابستگی به دانش قبلی درباره فعالیت‌های هنجار سیستم
۳	روش‌های مبتنی بر یادگیری ماشین	- انعطاف‌پذیری و قابلیت تطابق‌پذیری بالا - دقت زیاد روش پس از ایجاد مدل تشخیص نفوذ - افزایش کارایی با توجه به یادگیری تطبیقی در مواجهه با دریافت اطلاعات جدید - قابلیت نمایش گرافیکی الگوهای نفوذ کشف شده - قدرت تشخیص حملات ناشناخته جدید	- زمان‌بر بودن فرآیند آموزش مدل - مصرف منابع بالا - امکان آموزش مدل توسط افراد مهاجم

۳-۱-روش‌های تشخیص نفوذ از دیدگاه تعداد منابع داده

یکی از معیارهایی که در این مقاله برای دسته‌بندی و مقایسه پژوهش‌های انجام شده در این حوزه مورد توجه قرار داده شده است، تعداد منابع داده‌ای مورد استفاده توسط روش‌های تشخیص نفوذ می‌باشد. با توجه به بررسی‌های انجام شده بر روی پژوهش‌های موجود، این منابع داده در شش دسته اصلی پایگاه داده فراخوانی‌های سیستمی[2]، پایگاه داده ممیزی[3]، پایگاه داده فرامین کاربران، پایگاه داده آسیب‌پذیری‌ها[4]، پایگاه داده موردی[5] و پایگاه داده بازنمایی دانش[6] تقسیم‌بندی می‌شوند. پژوهش‌های موجود بر اساس استفاده از این منابع داده‌ای به دو زیردسته اصلی تقسیم می‌شوند. در ادامه با معرفی هر یک از این دو زیردسته، با نمونه‌هایی از پژوهش‌های صورت گرفته در هر دسته آشنا خواهیم شد. ابعاد این دیدگاه به‌همراه پژوهش‌های نمونه در شکل (۶) نشان داده شده است.

۳-۱-۱-منبع داده یگانه

در این دسته از روش‌ها، از یکی از منابع داده‌ای شش‌گانه معرفی شده در بالا، برای تشخیص نفوذهای احتمالی استفاده می‌شود.



شکل۶- ابعاد دیدگاه تعداد منابع داده به‌همراه پژوهش‌های نمونه

غالب این روش‌ها از پایگاه داده فراخوانی‌های سیستمی یا پایگاه داده فرامین کاربران برای تحلیل نفوذهای احتمالی استفاده می‌کنند. گونه‌ای از روش‌ها نیز بر مبنای مفهوم سیستم‌های تشخیص نفوذ همکارانه[7] شکل گرفته‌اند که منابع اطلاعاتی مورد استفاده در آن‌ها نیز پایگاه داده فرامین می‌باشد. به‌عنوان نمونه‌ای از روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف که از یک منبع داده استفاده نموده است، می‌توان به پژوهش انجام شده در مرجع [۲۱] اشاره کرد که در آن با استفاده از یک مجموعه داده (نمایه) مربوط به تراکنش‌های معتبر کارت اعتباری به امر تشخیص تقلب در کارت‌های اعتباری پرداخته شده است. علاوه بر

1. Big Data
2. System Call
3. Audit Database
4. Vulnerability Database
5. Case Database
6. Knowledge Representation Database
7. Co-operative

این، در مرجع [۲۲] نیز با استفاده از مجموعه داده DARPA 2000 [۲۳] که حاوی هشدارهای نفوذی در یک شبکه کامپیوتری است، یک مدل مخفی مارکوف برای تشخیص رفتارهای ناهنجار ایجاد شده است.

۳-۱-۲-منبع داده چندگانه

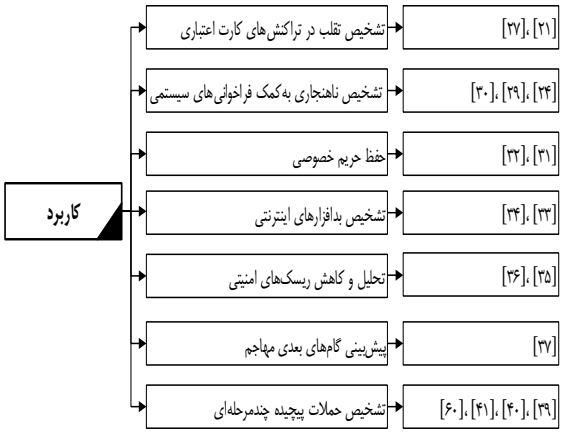
در این روش، از ترکیبی از منابع داده ذکر شده در بالا برای ایجاد مدل‌های تشخیص نفوذ استفاده می‌شود. متداول‌ترین نوع استفاده از چند منبع داده، به کارگیری ترکیبی از پایگاه داده‌های فراخوانی‌های سیستمی، فرامین و ممیزی است که نمونه‌هایی از این کار را می‌توان در مراجع [۷، ۲۴، ۲۵] یافت که در آن‌ها با استفاده از ترکیبی از منابع داده‌ای مذکور و به‌کمک رویدادنامه‌های هر یک از کاربران و نیز دنباله فراخوانی‌های سیستمی ثبت شده به‌هنگام اجرای دستورات توسط آن‌ها، مدل تشخیص نفوذ ایجاد می‌گردد. در برخی از کاربردهای تشخیص نفوذ نظیر مرجع [۲۶]، از سه منبع داده‌ای مختلف نظیر فایل‌های رویدادنامه سه ابزار IDS، دیواره آتش و تله‌عسل[1] برای ایجاد مدل مخفی مارکوف جهت حفاظت بلادرنگ[2] از منابع شبکه در برابر حملات شبکه‌ای استفاده شده است.

۳-۲-روش‌های تشخیص نفوذ از دیدگاه کاربرد

یکی دیگر از جنبه‌های مورد مطالعه در پژوهش جاری، دسته‌بندی روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف از دیدگاه کاربرد تشخیص نفوذ در امنیت سیستم‌های نرم‌افزاری است. به‌عبارت دیگر، بررسی این که پژوهش‌های مختلف برای برآورده کردن چه جنبه‌هایی از تشخیص نفوذ، سعی در ارائه راه‌کار نموده‌اند. پژوهش‌های صورت گرفته از این دیدگاه، به‌طور کلی در شش دسته تشخیص تقلب در تراکنش‌های کارت اعتباری[3]، تشخیص ناهنجاری[4] به کمک فراخوانی‌های سیستمی، حفظ حریم خصوصی[5]، تشخیص بدافزارهای[6] اینترنتی، تحلیل و کاهش ریسک‌های امنیتی، پیش‌بینی گام‌های بعدی مهاجم و تشخیص حملات پیچیده چند مرحله‌ای گنجانده می‌شوند که در شکل (۵) نشان داده شده است. در ادامه، ضمن تشریح هر یک از دامنه‌های کاربردی مختلف، به بیان مهم‌ترین پژوهش‌های انجام شده در هر یک از آن‌ها می‌پردازیم. ابعاد این دیدگاه به‌همراه پژوهش‌های نمونه در شکل (۷) نشان داده شده است.

۳-۲-۱-تشخیص تقلب در تراکنش های کارت اعتباری

یکی از کاربردهای مهم تشخیص نفوذ، تشخیص تقلب در تراکنش‌های کارت‌های اعتباری است. در این کاربرد، هدف اصلی، تشخیص رفتار ناهنجار انجام شده با استفاده از یک کارت اعتباری است که تحت عنوان تقلب خوانده می‌شود. در این‌گونه کاربردها، فرض بر این است که هر کارت اعتباری، دارای یک نمایه مخصوص به خود است که حاوی تراکنش‌های صورت گرفته توسط دارنده کارت و یا افراد مجاز استفاده کننده از کارت وجود دارد. در ادامه با استفاده از این نمایه هنجار، یک مدل HMM به کمک الگوریتم‌های آموزش معرفی شده برای این مدل نظیر الگوریتم بام-وِلش[7] ایجاد می‌شود. در این دسته از روش‌ها، هدف اصلی مدل ایجاد شده، تشخیص یک تراکنش ناهنجار است. این کار با استفاده از محاسبه میزان احتمال تولید یک دنباله معتبر به‌همراه تراکنش دریافتی جدید صورت می‌گیرد.



شکل۷- ابعاد دیدگاه کاربرد به‌همراه پژوهش‌های نمونه

به‌عنوان مثال اگر $T_1, T_2, \ldots, T_N$ یک دنباله از تراکنش‌های معتبر با احتمال p_1 از یک کارت اعتباری بوده و تراکنش دریافتی جدید معادل T_{N+1} باشد، آنگاه با محاسبه احتمال تولید دنباله تراکنش جدید $T_2, T_3, \ldots, T_N, T_{N+1}$ توسط مدل ایجاد شده می‌توان دریافت که تراکنش رسیده T_{N+1} هنجار است یا خیر. به‌عبارتی اگر این میزان احتمال برابر p_2 باشد، آن‌گاه در صورتی که اختلاف

1. Honeypot
2. Real Time
3. Credit Card Transactions
4. Anomaly Detection
5. Privacy
6. Malware Detection
7. Baum-Welch

$p_2 - p_1$ از یک حد آستانه δ بیشتر باشد، تراکنش T_{N+1} به‌عنوان یک تراکنش ناهنجار تشخیص داده شده و در غیر این‌صورت، تراکنش هنجار خواهد بود.

به‌عنوان نمونه پژوهش‌هایی دیگر در این حوزه می‌توان به کار ریواستاوا و همکاران [۲۱] اشاره کرد که در آن با استفاده از ایجاد یک مدل مخفی مارکوف به کمک تراکنش‌های هنجار دارنده یک کارت اعتباری، سیستمی را برای تشخیص تراکنش تقلبی معرفی نموده‌اند. وارتاک و همکاران [۲۷] نیز با استفاده از یک مدل مخفی مارکوف، نشان داده‌اند که می‌توان از این مدل برای کاربردهای بلادرنگ تشخیص تقلب در تراکنش‌های بانکی استفاده نمود. به‌عنوان پژوهشی دیگر می‌توان به کار هوک [۲۸] اشاره کرد که در آن با ایجاد یک مدل HMM، رفتارهای متقلبانه به‌صورت منفعل تشخیص داده شده و به مدیر سیستم گزارش داده می‌شوند.

۳-۲-۲-تشخیص ناهنجاری به کمک فراخوانی‌های سیستمی

از جمله مهم‌ترین روش‌های تشخیص نفوذ مبتنی بر ناهنجاری، ارزیابی رفتار برنامه‌های کاربردی موجود بر روی یک ماشین میزبان جهت تشخیص فعالیت‌های ناهنجار است. در این سطح با یک مسئله تشخیص ناهنجاری در مقیاس زیر سطح[1] مواجه هستیم که هدف اصلی آن، ایجاد مدل رفتاری یک کاربر بر اساس نمایه فراخوانی‌های سیستمی است. این نمایه بر مبنای فرامین مورد استفاده کاربر هنگام استفاده از یک برنامه کاربردی ایجاد می‌شود. در مقابل، اگر بخواهیم برای هر کاربر موجود بر روی یک ماشین میزبان چندکاربره، مدل‌های رفتاری هنجار را با استفاده از مدل مخفی مارکوف ایجاد نماییم، در این حالت با یک مسئله درشت‌سطح[2] روبرو خواهیم بود. در نوع درشت‌سطح، دنباله فرامین صادر شده از سوی کاربر برای ایجاد مدل مورد استفاده قرار می‌گیرد. این فرامین در مکان‌های مشخصی از سیستم رویدادنگاری می‌شوند. به‌طور کلی، گام‌های اصلی ایجاد یک سیستم تشخیص ناهنجاری به کمک فراخوانی‌های سیستمی شامل موارد زیر است:

- ایجاد یک پایگاه داده از رفتارهای هنجار کاربران برنامه کاربردی
- ساخت مدل HMM برای هر کاربر (یک مدل ساده شامل دو حالت مخفی هنجار و ناهنجار که در آن مشاهدات از نوع فراخوانی‌های سیستمی قابل تولید توسط یک برنامه کاربردی است).
- دریافت یک دنباله جدید از مشاهدات
- تخمین میزان احتمال تولید دنباله دریافتی توسط مدل HMM به‌دست آمده متناظر با کاربر موردنظر
- تصمیم‌گیری درباره اجرا و یا عدم اجرای فرامین صادر شده از سوی کاربر

از جمله کارهای انجام شده در این دسته می‌توان به پژوهش هانگ و همکاران [۲۴] اشاره کرد که در آن با استفاده از یک مدل مخفی مارکوف افزایشی، حملات منع خدمت بر روی مجموعه‌ای از کارگزاران[3] تشخیص داده می‌شوند. در این پژوهش، فراخوانی‌های سیستمی انجام شده بر روی کارگزاران ارزیابی شده و فعالیت‌های بدخواهانه تشخیص داده می‌شوند. روسی و همکاران [۲۹] با تحلیل و ارزیابی سیستم‌های تشخیص نفوذ مبتنی بر ناهنجاری و با استفاده از بررسی فراخوانی‌های سیستمی، روش تشخیص نفوذی را معرفی نموده‌اند که هدف اصلی آن‌ها حفاظت از اطلاعات یک ماشین میزبان در بستر یک شبکه است. از جمله دیگر پژوهش‌های این دسته می‌توان به مدل HMM معرفی شده توسط یولاکان و همکاران [۳۰] اشاره کرد که هدف اصلی آن، تشخیص ناهنجاری با استفاده از فراخوانی‌های سیستمی جهت تشخیص کاربران پرخطر بر روی یک ماشین میزبان می‌باشد.

۳-۲-۳-حفظ حریم خصوصی

هدف برخی دیگر از پژوهش‌های جدید، معرفی روش‌هایی با استفاده از مدل مخفی مارکوف است که در آن داده‌های دریافتی توسط مدل، از یک درجه حساسیت بالایی از محرمانگی برخوردار می‌باشند. به‌عبارت دیگر داده‌هایی که برای آموزش مدل مورد استفاده قرار می‌گیرند، متعلق به مجموعه‌ای از مشترکین داده هستند که در آن حفظ محرمانگی داده‌های هر یک از مشترکین، یک امر حیاتی و مهم محسوب می‌شود.

در این دسته کاربردها، به‌دنبال طبقه‌بندی احتمالاتی دنباله‌های دریافتی بدون اطلاع از اصل داده‌های مشترکین

1. Micro Level
2. Macro Level
3. Servers

هستیم. در واقع، در این کاربردها، از مدل مخفی مارکوف برای آموزش توزیع احتمال دنباله‌ها استفاده می‌شود تا با استفاده از آن دریافت که هر دنباله داده‌ای دریافتی به کدام کلاس داده‌ای تعلق دارد. به عنوان یک نمونه، فرض کنید بخواهیم دنباله داده‌های مربوط به یک مجموعه از افراد بیمار را در دسته بیماری‌های مختلف تقسیم‌بندی نماییم، به‌گونه‌ای که مدل مخفی مارکوف مورد استفاده، محرمانگی داده‌های بیماران را حفظ نماید.

پاتاک و همکاران [۳۱] مدل ارتباطی را بر اساس استفاده از مدل‌های مخفی مارکوف در یک محیط اشتراکی معرفی نموده‌اند که با استفاده از آن، هر یک از میزبان‌های کارخواه[1] می‌توانند با استفاده از مدل HMM خصوصی موجود در کارگزار، به‌صورت محرمانه با آن تعامل داشته و استنتاج‌های موردنیاز را انجام دهند. در یکی دیگر از پژوهش‌ها، جاو و همکاران [۳۲] مدل HMMای برای محیط‌های اشتراکی معرفی نموده‌اند که در آن هر یک از مشترکین، ضمن ارسال اطلاعات محرمانه خود به کارگزار، قادر به برقراری ارتباط محرمانه با آن هستند. مدل ایجاد شده قادر خواهد بود تا محرمانگی اطلاعات هر یک از مشترکین را در محیط اشتراکی ناامن برآورده نماید.

۳-۲-۴-تشخیص بدافزارهای اینترنتی

یکی دیگر از چالش‌های جدید در زمینه امنیت سیستم‌های نرم‌افزاری، حفاظت منابع و دارایی‌های شبکه در بستر ناامن اینترنت است. استفاده از اینترنت، در کنار به‌وجود آوردن یک فرصت برای انجام کارها در بستر شبکه، تهدیدی را ایجاد می‌کند و آن گسترش تهاجم به افراد، سازمان‌ها و دارایی‌های آن‌ها از طریق ایجاد برنامه‌ها و بدافزارهای مخرب نظیر شبکه‌های بات و انواع ویروس‌ها می‌باشد. انتشار در سطح وسیعِ این بدافزارها در سایت‌های قربانی، تأثیرات جبران‌ناپذیری را به‌دنبال خواهد داشت.

بدافزارهای مخرب برای انجام اعمال خصمانه خود، رفتارهای منحصر به‌فردی را انجام می‌دهند. این رفتارها با تحلیل بسته‌های شبکه و به‌طور کلی بررسی ترافیک شبکه قابل استخراج و مدل‌سازی خواهند بود. به‌عنوان مثال، یکی از گام‌های مهم در شکل‌گیری شبکه‌های بات، بحث ایجاد ارتباط هر یک از گره‌های بات با فرمانده شبکه بات[2] است.

با استفاده از مدل‌های احتمالاتی مبتنی بر استنتاج نظیر HMM، می‌توان رفتار فرمانده‌های بات و به‌طور کلی‌تر شبکه‌های بات را مدل‌سازی نمود و از شکل‌گیری آن‌ها در بستر شبکه‌های محلی جلوگیری نمود. ویروس‌های کامپیوتری، نمونه‌ای دیگر از بدافزارها هستند که با رفتار دِگَرریختی[3] و چندریختیِ[4] خود قادر به تغییر ساختار ظاهری خود می‌باشند، در صورتی که ماهیت رفتار آن‌ها ثابت می‌ماند. با استفاده از مدل مخفی مارکوف، می‌توان میزان تشابه دو رفتار به یکدیگر را به‌دست آورد که این امر در جهت تشخیص این دسته از ویروس‌ها بسیار حائز اهمیت است. از جمله مهم‌ترین پژوهش‌های صورت گرفته جهت تشخیص بدافزارهای اینترنتی می‌توان به مراجع [۳۳، ۳۴] اشاره کرد که هدف اصلی این پژوهش‌ها، ایجاد مدل مخفی مارکوف جهت تشخیص بدافزارهایی نظیر بات‌ها و ویروس‌های کامپیوتری است تا از فعالیت‌های مخرب آن‌ها در شبکه جلوگیری به‌عمل آید. مدل‌های HHM موجود در این کاربرد، بر اساس تحلیل آماری محتوای داده‌های موجود در بسته‌های تسخیر شده[5] از شبکه عمل می‌نمایند.

۳-۲-۵-تحلیل و کاهش ریسک‌های امنیتی

یکی دیگر از دسته کاربردهای مدل مخفی مارکوف، ارزیابی ریسک‌های امنیتی جهت تعیین تأثیر رویدادهای امنیتی مختلف بر دارایی‌ها و منابع شبکه‌های کامپیوتری است. بسیاری از روش‌های موجود محدود به ارزیابی ریسک بر اساس دانش خبره هستند که برای کاربردهای خودکار و بلادرنگ مناسب نیستند. دسته خاصی از روش‌ها که با استفاده از مدل HMM به تحلیل و ارزیابی ریسک‌های امنیتی می‌پردازند، از قدرت بسیار بالایی در جهت کاهش ریسک‌ها برخوردارند [۳۵]. در غالب روش‌های ارائه شده در این دسته، میزان ریسک شبکه بر اساس ترکیبی از میزان ریسک‌های هر یک از میزبان‌ها و به‌صورتی دقیق و ریزدانه مدل به‌دست می‌آید. علاوه بر این، در روش‌های ارزیابی ریسک امنیتی مبتنی بر مدل مخفی مارکوف می‌توان احتمال انتقالات بین حالت‌های امنیتی مختلف را به‌صورت یک گراف حمله بازنمایی نمود که این عامل برای مدیر امنیتی جهت استنتاج‌های آتی بسیار مفید واقع می‌شود.

از جمله پژوهش‌های این حوزه می‌توان به کار آرنِس و

1. Clients
2. Botnet Master
3. Metamorphism
4. Polymorphism
5. Captured Packets

همکاران [۳۵] اشاره کرد که در آن یک مدل ارزیابی با درنظر گرفتن موارد ریسک شبکه معرفی شده است. از جمله ویژگی‌های این روش می‌توان به توزیع احتمال بین حالت‌های امنیتی سیستم (به کمک مدل HMM) و گسترش‌پذیری فرآیند ارزیابی ریسک اشاره کرد. به‌عنوان نمونه‌ای دیگر از پژوهش‌های صورت گرفته می‌توان به کار هیتان و همکارن [۳۶] اشاره کرد که هدف از پژوهش آن‌ها معرفی یک روش مبتنی بر مدل مخفی مارکوف جهت ارزیابی و تحلیل ریسک‌های موجود بر روی یک شبکه است. گام‌های اصلی روش آن‌ها در موارد زیر خلاصه می‌شوند:

- ایجاد یک مدل مخفی مارکوف برای تشریح رفتار یک سیستم موجود بر روی یک شبکه
- ایجاد یک ماتریس گذار برای ارزیابی کمّی فاکتورهای ریسک
- به‌کارگیری متدولوژی ارزیابی ریسک بر روی بستر شبکه اینترنت جهت محاسبه مقدار ریسک امنیتی برای هر سیستم

۳-۲-۶-پیش‌بینی گام‌های بعدی مهاجم

یکی دیگر از کاربردهای تشخیص نفوذ در بستر شبکه، پیش‌بینی گام‌های آتی مهاجمان و فراهم نمودن مکانیزم‌هایی در جهت جلوگیری از گسترش فعالیت‌های مخرب آن‌ها است. اکثر روش‌های تشخیص نفوذ، تنها قادر به تشخیص نفوذها بعد از وقوع یک حمله در بستر شبکه هستند. در دسته‌ای از کاربردهای جدید، سعی شده است تا با استفاده از پیش‌گویی گام‌های آتی یک مهاجم موجود در بستر شبکه، از سایر اعمال خصمانه او جلوگیری به‌عمل آید. یکی از مهم‌ترین ابزارهای موجود در جهت تحقق این هدف، مدل‌های مخفی مارکوف است که در شرایطی با دقت بیش از ۹۵٪ عمل می‌نماید [۳۷].

۳-۲-۷-تشخیص حملات پیچیده چندمرحله‌ای

از دیگر کاربردهای بسیار مهم مدل مخفی مارکوف، استفاده از این مدل برای همبسته‌سازی هشدارهای[1] تولید شده توسط سیستم‌های تشخیص نفوذ در یک محیط تحت نظارت نظیر یک شبکه می‌باشد. هشدارهایی که سیستم‌های تشخیص نفوذ تولید می‌کنند، هشدارهای سطح پایینی هستند که چنانچه به‌صورت منفرد در نظر گرفته شوند، تهدیدات واقعی سیستم را به‌درستی نشان نمی‌دهند. معمولا مهاجم برای نیل به اهداف خود از حملات پیچیده چندمرحله‌ای استفاده می‌کند. حملاتی که در آن‌ها ابتدا مهاجم از یک یا چند آسیب‌پذیری شناخته شده موجود در سیستم استفاده کرده و حمله خود را یک گام به جلو می‌برد و سپس با بهره‌گیری از نتایج این گام که پیش‌نیاز گام بعدی حمله است، گام بعدی را اجرا می‌کند و به این ترتیب حمله خود را گام‌به‌گام به سمت هدف نهایی سوق می‌دهد. سیستم‌های تشخیص نفوذ، تنها قادر به تولید هشدارهای سطح پایین برای هر کدام از گام‌های حمله به‌صورت مجزا هستند که امکان تشخیص سناریوی حملات چندمرحله‌ای و ارتباط دادن هشدارهای یک حمله به یکدیگر را ندارند. بنابراین نیازمند ایجاد یک دید سطح بالاتر از وضعیت امنیتی سیستم هستیم. همبسته‌سازی هشدارها چنین دیدی را از سیستم و یا شبکه تحت حفاظت از طریق پردازش هشدارهای سیستم‌های تشخیص نفوذ تولید می‌کند. به‌طور کلی دو یا چند حس‌گر تشخیص نفوذ ممکن است برای اهداف زیر با یکدیگر همکاری کنند:

- تحلیل هشدارهای صادر شده یکدیگر
- تکمیل پوشش تقویت هشدارهای یکدیگر و کاهش نرخ مثبتِ غلط[2]
- تقویت هشدارهای یکدیگر و پایین آوردن نرخ مثبتِ غلط

همبسته‌سازی هشدارها فرآیندی است که طی آن هشدارهای تولید شده توسط یک یا چند حس‌گر موجود در شبکه، تحلیل می شود تا یک دیدگاه مختصر و سطح بالایی از تلاش‌های نفوذ احتمالی فراهم گردد [۳۸]. همبسته‌ساز با بررسی هشدارهای تولید شده و کشف ارتباطات منطقی آن‌ها به‌جای تولید صدها هشدار سطح پایین و گسسته، یک هشدار سطح بالا را به مدیر سیستم ارائه می‌کند. بنابراین تعیین رخدادهای بسیار مهم از میان حجم زیادی از وقایع ثبت شده، هدف نهایی فرآیند همبسته‌سازی است تا بر کیفیت هشدارها افزوده و از تعداد آن‌ها کاسته شود. در ادامه برخی از پژوهش‌هایی که از مدل مخفی مارکوف برای برآورده نمودن این جنبه از مسئله تشخیص نفوذ، استفاده کرده‌اند به اختصار شرح داده می‌شوند.

از جمله پژوهش‌های صورت گرفته در حوزه توسعه سیستم‌های همبسته‌سازی هشدار مبتنی بر مدل مخفی

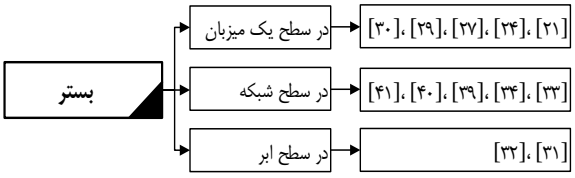
1. Alert Correlation

2. False-Positive

مارکوف می‌توان به پژوهش فرهادی و همکاران [۳۹] اشاره کرد که در آن با استفاده از یک مدل HMM به تشخیص طرح حمله[1] مهاجم به کمک استخراج الگوی حملات پرداخته شده است. از جمله دیگر پژوهش‌های صورت گرفته در این حوزه می‌توان به مراجع [۴۰، ۴۱، ۵۹] اشاره نمود که هدف اصلی آن‌ها استخراج سناریوی حملات چندمرحله‌ای با تحلیل همبستگی بین هشدارهای تولید شده توسط سیستم‌های تشخیص نفوذ است.

۳-۳-روش‌های تشخیص نفوذ از دیدگاه بستر

در این بخش، به دسته‌بندی پژوهش‌های صورت گرفته در این حوزه بر اساس بستر مورد نظارت یک IDS خواهیم پرداخت که این سیستم‌ها از این منظر به سه دسته اصلی در سطح میزبان، در سطح شبکه و در سطح ابر تقسیم می‌شوند که در ادامه ضمن تشریح هر یک از این دسته‌ها، مهم‌ترین پژوهش‌های صورت گرفته در هر دسته را نیز بیان خواهیم نمود. ابعاد این دیدگاه به‌همراه پژوهش‌های نمونه در شکل (۸) نشان داده شده است.



شکل۸- ابعاد دیدگاه بستر به‌همراه پژوهش‌های نمونه

۳-۳-۱-در سطح میزبان

تکنیک‌های معرفی شده در این سطح، تشخیص فعالیت‌های ناهنجار بر روی یک ماشین میزبان منحصربه‌فرد را بر عهده دارند. یک IDS مبتنی بر میزبان می‌تواند حملات و تهدیداتی نظیر دسترسی به فایل‌ها و اسب‌های تراوا را بر روی سیستم‌های بحرانی تشخیص دهد. سیستم تشخیص نفوذ توسعه داده شده در این سطح، فقط از میزبان‌هایی که بر روی آن‌ها مستقر است، محافظت می‌نماید. این سیستم‌ها با استقرار بر روی میزبانی که باید نظارت شود، از همه اطلاعات محلی و ملاحظات امنیتی مربوط به پیاده‌سازی (شامل فراخوانی‌های سیستمی، تغییرات فایل‌های سیستمی و داده‌های ممیزی مربوط به فرامین کاربران) مطلع می‌باشند که از این اطلاعات برای ساخت مدل‌ها استفاده می‌شود.

از جمله مهم‌ترین پژوهش‌های صورت گرفته در این دسته می‌توان به پژوهش هو [۷، ۴۲] اشاره کرد که در آن با استفاده از فراخوانی‌های سیستمی مربوط به یک برنامه کاربردی، مدلی برای تشخیص ناهنجاری در یک ماشین میزبان معرفی شده است. این مدل بر پایه یک HMM دو سطحی کار می‌کند که در آن، از یک سو دستورات مجاز مورد استفاده برای هر کاربر و از سوی دیگر، دنباله فراخوانی‌های سیستمی مجاز برای هر برنامه کاربردی جهت ایجاد مدل نهایی از رفتار سیستم مورد استفاده قرار می‌گیرد. از جمله دیگر پژوهش‌ها می‌توان به کار وانگ و همکاران [۴۳] اشاره کرد که در آن یک سیستم تشخیص نفوذ مبتنی بر HMM و بر اساس فراخوانی‌های سیستمی مربوط به کارگزار ایمیل Sendmail معرفی شده است. از جمله ویژگی‌های این مدل، پویایی نرخ آستانه است تا در شرایط متفاوت، میزان این آستانه جهت افزایش قابلیت تشخیص قابل تغییر باشد.

۳-۳-۲-در سطح شبکه

در این سطح، یک IDS از منظر محلی که قرار گرفته است، بر تمام شبکه تحت پوشش خود نظارت می‌نماید. شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیستم‌های بحرانی[2]، به عهده IDS مبتنی بر شبکه است. سیستم‌های موجود در این سطح اغلب از دو بخش ناظر و عامل[3] استفاده می‌کنند. نقش ناظر جمع‌آوری داده‌های مبادله شده در اتصالات مختلف شبکه است در حالی‌که عامل با تحلیل این بسته‌ها، اقدام به تشخیص فعالیت‌های ناهنجار می‌نماید. این دو بخش اغلب در پشت دیواره آتش نصب می‌شوند تا عملیات خود را انجام دهند. در این ساختارها، عامل‌های شبکه می‌توانند بر اساس مدل مخفی مارکوف توسعه داده شوند تا ضمن بررسی محتوای بسته‌های موجود در شبکه، از بروز حملات علیه شبکه تحت پوشش جلوگیری نمایند.

از جمله پژوهش‌های موجود در این دسته می‌توان به پژوهش شین و همکاران [۴۴] اشاره کرد که در آن یک روش احتمالاتی کارای مبتنی بر HMM برای پیش‌بینی و تشخیص نفوذهای موجود در شبکه معرفی شده است. این سیستم NIDS از یک زنجیره مارکوف برای تخمین احتمالات رفتارهای هنجار و ناهنجار استفاده می‌کند. برای تعیین وضعیت‌های مختلف شبکه و نیز محاسبه انتقال بین حالت‌ها از روش خوشه‌بندی[4] K-Means استفاده می‌شود.

1. Attack Plan Recognition
2. Critical Systems
3. Agent
4. Clustering

از جمله پژوهش‌های دیگر موجود در این دسته، می‌توان به مراجع [۲۶، ۴۵] اشاره کرد که در آن‌ها مدل‌های رفتاری HMM، بر اساس محموله[1] بسته‌های پروتکل TCP/IP مبادله شده در شبکه ایجاد شده و بر اساس آن‌ها رفتارهای مخرب شناسایی می‌شوند.

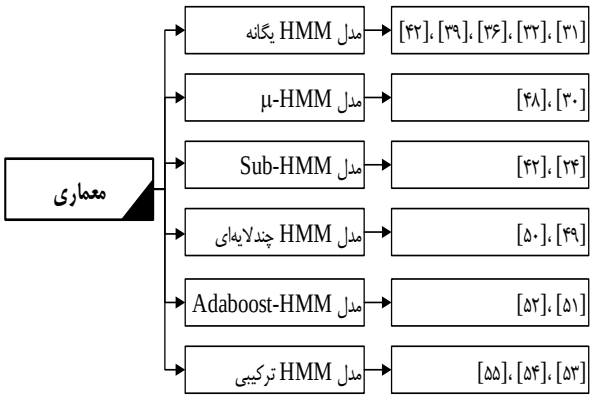
۳-۳-۳-در سطح ابر

یکی از روش‌های مقابله با تهدیدهای احتمالی، توسعه روش‌هایی برای حفظ تمامیت داده‌های کاربران برون‌سپاری شده در ابر است. به دلیل ذات توزیع‌شده بسترهای ابر، اغلب از تکنیک‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف جهت برآورده کردن نیاز صحت داده‌ها استفاده می‌شود. در واقع با استفاده از قدرت انعطاف‌پذیری و گسترش‌پذیری روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف، به‌کارگیری این روش‌ها در بستر ابر نتایج مفیدی را به‌دنبال خواهد داشت. از جمله پژوهش‌های موجود در این دسته می‌توان به کارهای موجود در مراجع [۴۶، ۴۷] اشاره کرد که در آن‌ها تکنیک‌های تشخیص نفوذ جهت شناسایی نفوذهای احتمالی مبتنی بر مدل مخفی مارکوف می‌باشد.

با توجه به مطالب گفته شده در بخش ۳، می‌توان به این نتیجه مهم رسید که با گذشت زمان زیادی از معرفی مدل‌های مخفی مارکوف برای کاربردهای تشخیص نفوذ، استفاده از این مدل‌ها برای کاربردهای جدید نظیر تشخیص سناریوی حملات پیچیده چندمرحله‌ای و یا پیش‌بینی گام‌های آتی مهاجم در حملات شبکه‌ای نیز رایج شده است. از سوی دیگر، با توجه به گسترش ارائه خدمات گوناگون در محیط‌های توزیع‌شده نظیر ابر و پیشرفت این فن‌آوری، مدل‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف در این بستر نیز مورد استفاده قرار گرفته است که این امر زمینه‌ساز انجام پژوهش‌های آتی در این حوزه خواهد بود.

۴- روش‌های تشخیص نفوذ مبتنی بر HMM از دیدگاه معماری

جنبه دیگر برای مطالعه و دسته‌بندی روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف، معماری‌های مورد استفاده در توسعه روش‌های مبتنی بر این مدل می‌باشند. از آن‌جا که مدل‌های معرفی شده مبتنی بر مدل مخفی مارکوف برای کاربردهای تشخیص نفوذ، پس از آموزش اولیه، در تشخیص رفتارهای ناهنجار (نفوذها و حملات) از دقت بسیار بالایی برخوردار هستند و به‌عبارت دقیق‌تر یک طبقه‌بند قوی به‌حساب می‌آیند [۸]، لذا کارهای بسیاری برای مرتفع ساختن مدت زمان موردنیاز برای آموزش اولیه مدل صورت گرفته است که همگی سعی می‌کنند کارایی نهایی مدل را بهبود بخشند. تاکنون معماری‌های مختلفی معرفی شده‌اند که مهم‌ترین آن‌ها در شکل (۹) آورده شده است. در ادامه، پس از معرفی حالت کلی مدل HMM یگانه، مهم‌ترین تلاش‌های انجام شده جهت بهبود مدل HMM یگانه را بیان نموده و به تشریح هر یک از آن‌ها می‌پردازیم. ابعاد این دیدگاه به‌همراه پژوهش‌های نمونه در شکل (۹) نشان داده شده است.



شکل۹- ابعاد دیدگاه معماری به‌همراه پژوهش‌های نمونه

۴-۱-۱-مدل HMM یگانه

همان‌گونه که پیش از این نیز گفته شد، ساده‌ترین راه برای ایجاد یک مدل رفتاری از سیستم جهت کاربردهای تشخیص نفوذ، استفاده از یک نمایه حاوی فعالیت‌های هنجار سیستم می‌باشد. این فرآیند در شکل (۱۰) نشان داده شده است. نمایه می‌تواند مجموعه داده‌ای از فراخوانی‌های سیستمی یا اطلاعات موجود در بسته‌های جریان‌های مختلف در یک شبکه باشد. در ادامه می‌توان با دریافت مشاهدات موجود در نمایه، پیش‌پردازش آن‌ها و سپس به‌کارگیری الگوریتم‌های آموزش مورد استفاده در مدل HMM نظیر الگوریتم بام-وِلش، یک مدل رفتاری نهایی از نمایه ایجاد نمود. این فرآیند در شکل (۱۰-الف) نشان داده شده است. برای انجام عمل آزمون و ارزیابی یک دنباله جدید دریافتی نیز می‌توان، با استفاده از الگوریتم‌های پیش‌رو[2] یا پس‌رو[3]، میزان احتمال تولید دنباله توسط مدل

1. Payload
2. Forward
3. Backward

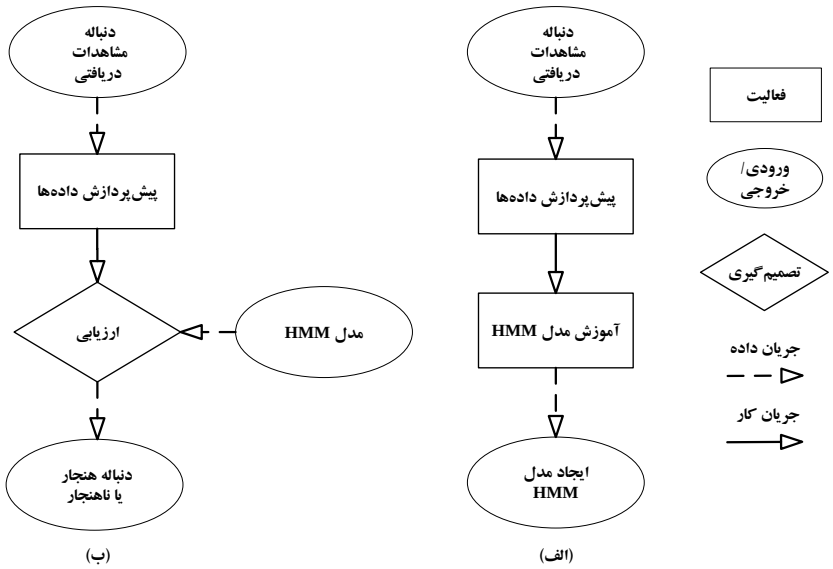
ایجاد شده در مرحله (الف) را محاسبه و درباره هنجار یا ناهنجار بودن دنباله مشاهدات دریافتی تصمیم‌گیری نمود. این فرآیند در شکل (۱۰-ب) نشان داده شده است.

یکی از معایب اصلی این روش، افزایش زمان یادگیری و در نتیجه آن کاهش کارایی سیستم است. به‌همین دلیل استفاده از این مدل برای کاربردهای بلادرنگ که هدف اصلی آن‌ها پردازش برخط[1] دنباله مشاهدات دریافتی است، توصیه نمی‌شود. برای بهبود سرعت فرآیند یادگیری و افزایش قابلیت تشخیص مدل HMM و نیز کاهش نرخ هشدارهای نادرست، مدل‌های متنوع دیگری معرفی شده‌اند که در ادامه، ضمن تشریح دسته‌های مختلف، هر یک را به اختصار تشریح خواهیم نمود و به بیان اهداف معرفیِ هر معماری خواهیم پرداخت.

۴-۱-۲-مدل μ-HMM

همان‌گونه که پیش از این نیز گفته شد، الگوریتم معروف برای آموزش مدل HMM، معمولا الگوریتم بام-وِلش است. در این دسته از معماری‌ها، قبل از فرآیند آموزش مدل، ابتدا باید تعداد حالت‌های مخفی سیستم را معین نمود. از آن‌جا که تعداد حالت‌ها یک پارامتر ضروری برای کارایی مدل HMM نهایی محسوب می‌شود، از این رو پارامتر تعداد حالت‌ها با انتخاب مقدار منحصر به‌فردی که بهترین کارایی را بر روی داده‌های آموزشی فراهم می‌آورد، به‌صورت اکتشافی[2] (با استفاده از الگوریتم‌های خوشه‌بندی) و یا تجربی (با استفاده از دانش فرد خبره) انتخاب می‌شود. به دلیل عدم وجود یک رویه معین برای تعیین تعداد حالت‌های مدل، بهترین مدل HMM به‌دست آمده از این روش نیز، سطح بالایی از کارایی را برای همه فضای تشخیص فراهم نمی‌آورد.

جهت افزایش کارایی هنگام ایجاد مدل‌های مخفی مارکوف، روش‌هایی تحت عنوان μ-HMM ارائه شده است که در آن، هر مدل HMM با استفاده از تعداد مختلفی از حالت‌های مخفی آموزش داده می‌شود و مدل‌های HMM حاصل با استفاده از تکنیک MRROC و در فضای ROC [۳۰] با یکدیگر ترکیب شده و مدل نهایی به‌دست می‌آید. این فرآیند در شکل (۱۱) نشان داده شده است. مدل نهایی به‌دست آمده در این حالت با توجه به ترکیب مدل‌های مختلف HMM که هر یک دارای تعداد حالات مخفی مختلف بوده و با استفاده از پارامترهای مختلفی آموزش دیده شده‌اند، ایجاد می‌گردد. معماری μ-HMM به‌دلیل ترکیب دانش‌های مستخرج از مدل‌های مختلف از کارایی بالاتری نسبت به مدل‌های HMM یگانه برخوردار است. به عنوان یکی از ضعف‌های اصلی این دسته از معماری‌ها می‌توان به افزایش نسبی زمان یادگیری اشاره کرد که این امر به دلیل آموزش همزمان چند مدل HMM صورت می‌گیرد. از جمله مدل‌های توسعه داده شده موجود در این



شکل ۱۰- الف) فرآیند یادگیری در مدل HMM یگانه و ب) فرآیند آزمون در مدل HMM یگانه

1. Online

2. Heuristic

دسته می‌توان به پژوهش‌های [۳۰، ۴۸] اشاره کرد.

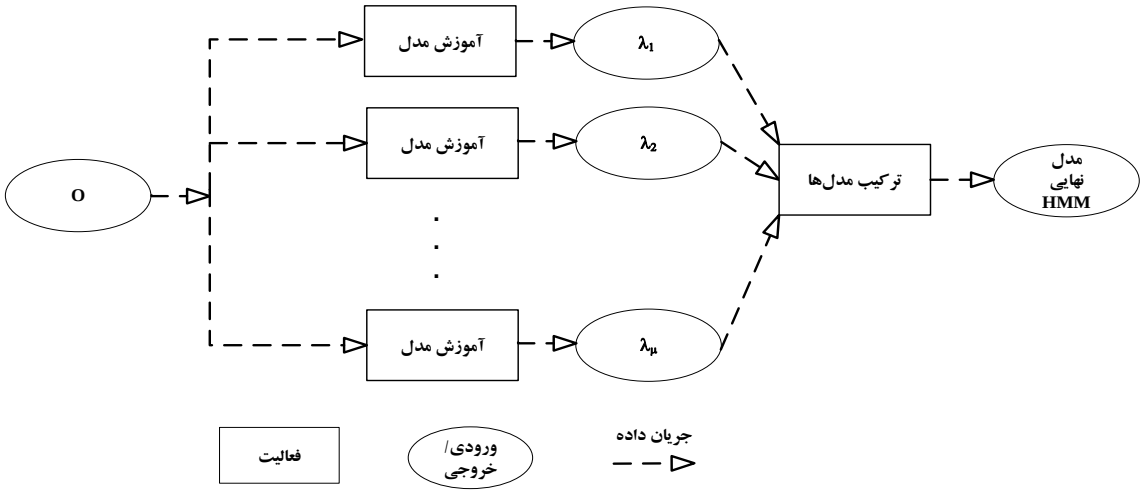
۴-۱-۳-مدل sub-HMM

به‌دلیل زمان‌بر بودن فرآیند آموزش مدل HMM، این فرآیند به‌صورت برون‌خط[1] انجام می‌شود. برای تسریع فرآیند یادگیری در مدل‌های HMM، می‌توان از دسته دیگری از روش‌های معرفی شده استفاده کرد که به روش‌های ایجاد مدل sub-HMM معروفند. در این روش‌ها اغلب مجموعه داده آموزشی به تعدادی زیربخش (زیردنباله) تقسیم می‌شود که هر یک از زیربخش‌های مجموعه داده اصلی، برای آموزش یک مدل sub-HMM به‌اندازه کافی بزرگ می‌باشند. در این نوع معماری‌ها، مهم‌ترین عامل در بخش‌بندی نمایه به زیربخش‌ها این است که هر زیربخش باید شامل اطلاعات متنوعی از رفتار کاربر یا سیستم باشد. در ادامه هر زیردنباله برای آموزش زیرمدل‌ها مورد استفاده قرار می‌گیرد و زیرمدل‌های آموزش دیده شده به‌صورت افزایشی برای ایجاد مدل نهایی با استفاده از یک الگوریتم میانگین وزنی[2] ادغام می‌شوند.

فرآیند ایجاد مدل HMM نهایی با استفاده از این روش در شکل (۱۲) نشان داده شده است. همان‌گونه که از شکل پیداست، عمل بخش‌بندی مجموعه داده بزرگ O به r زیربخش بر اساس یک مقدار آستانه مشابهت شکل می‌گیرد. اگر دو زیر بخش مقدار مشابهتشان بیش از مقدار آستانه باشد با یکدیگر ادغام می‌شوند. نقطه قوت استفاده از آستانه مشابهت این است که با تجمیع زیربخش‌های مشترک، تعداد sub-HMM ها و به دنبال آن زمان آموزش مدل‌ها کاهش می‌یابد. بنابراین هدف اصلی این روش‌ها کاهش زمان آموزش است که البته عیب بسیار بزرگ آن‌ها، بالا بودن نرخ خطای مثبتِ غلط می‌باشد. چون ممکن است در مرحله ادغام دو زیربخش مشابه، اطلاعات مربوط به دنباله‌های ناهنجار نادیده گرفته شود. از جمله مدل‌های توسعه داده شده موجود در این دسته می‌توان به پژوهش‌های [۲۴، ۴۲] اشاره کرد.

۴-۱-۴-مدل HMM چندلایه‌ای

برای کاهش نرخ هشدارهای نادرست مثبتِ غلط و نیز افزایش قابلیت تشخیص تکنیک‌های تشخیص نفوذ مبتنی بر HMM، معماری‌هایی با نام معماری HMM چندلایه معرفی شده‌اند که بیشتر برای کاربردهای تشخیص نفوذ در سطح میزبان مورد استفاده قرار می‌گیرند. عملکرد این مدل در شکل (۱۳) نشان داده شده است.



شکل۱۱- فرآیند ایجاد مدل تشخیص نفوذ μ-HMM

در این مدل تمرکز اصلی بر روی نحوه آزمون یک دنباله مشاهدات دریافتی جدید است. به‌عبارتی با داشتن مدل HMM نهایی سعی می‌شود فرآیند تصمیم‌گیری درباره یک دنباله مشاهدات دریافتی جدید تسریع یابد. فرآیند آزمون در این مدل به دو بخش اصلی تقسیم می‌شود:

۱. دنباله مشاهدات دریافتی با دنباله‌های موجود در یک

1. Offline

2. Weighted Average

پایگاه داده هنجار مقایسه می‌شود تا بررسی شود که آیا یک عدم تطابق رخ داده است یا خیر؛ به‌عبارت دیگر آیا یک دنباله نادر با فرکانس رخداد پایین دریافت شده است یا خیر؟

۲. اگر دنباله مشاهدات دریافتی نادر بوده و یا عدم تطابقی صورت گرفت، در این حالت دنباله مشاهدات دریافتی به مدل HMM داده شده تا احتمال تولید آن توسط مدل محاسبه گردد. در ادامه با مقایسه مقدار محاسبه شده توسط مدل با یک مقدار آستانه از پیش‌تعریف شده درباره دنباله مشاهدات دریافتی تصمیم‌گیری می‌شود.

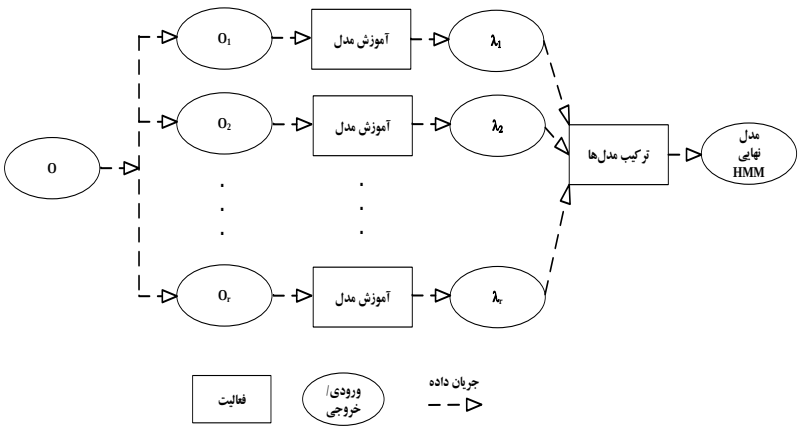
این عامل سبب افزایش قدرت تشخیص نفوذهای احتمالی و نیز کاهش نرخ هشدارهای مثبتِ غلط می‌گردد. از جمله مدل‌های توسعه داده شده موجود در این دسته می‌توان به پژوهش‌های [۴۹، ۵۰] اشاره کرد.

۴-۱-۵-مدل Adaboost-HMM

از جمله دیگر روش‌های توسعه داده شده مبتنی بر HMM برای تشخیص فعالیت‌های ناهنجار، استفاده از مدل Adaboost-HMM می‌باشد. در این مدل سعی می‌شود تا عیب روش‌های مبتنی بر مدل sub-HMM رفع شود و آن نیز کاهش نسبی نرخ خطای مثبتِ غلط می‌باشد که این عمل به کمک ایجاد یک مجموعه‌ای از طبقه‌بندهای ضعیف و در نهایت، ترکیب نتایج این طبقه‌بندها جهت دست‌یابی به یک دقت تشخیص بالاتر صورت می‌گیرد. دلیل این افزایش دقت در نرخ تشخیص، استفاده مدل Adaboost-HMM از الگوریتم Adaboost است. الگوریتم Adaboost [۵۱] یک الگوریتم یادگیری ماشین نظارتی[1] است که نرخ اطمینان هر طبقه‌بند ضعیف را محاسبه نموده و سعی در تنظیم وزن‌های هر نمونه دارد. با تکرار این الگوریتم در دفعات مختلف، بر میزان یادگیری روش افزوده می‌شود و دلیل آن نیز تمرکز الگوریتم بر روی نمونه‌های ضعیف‌تر است تا در نهایت آن‌ها را بهبود بخشد.

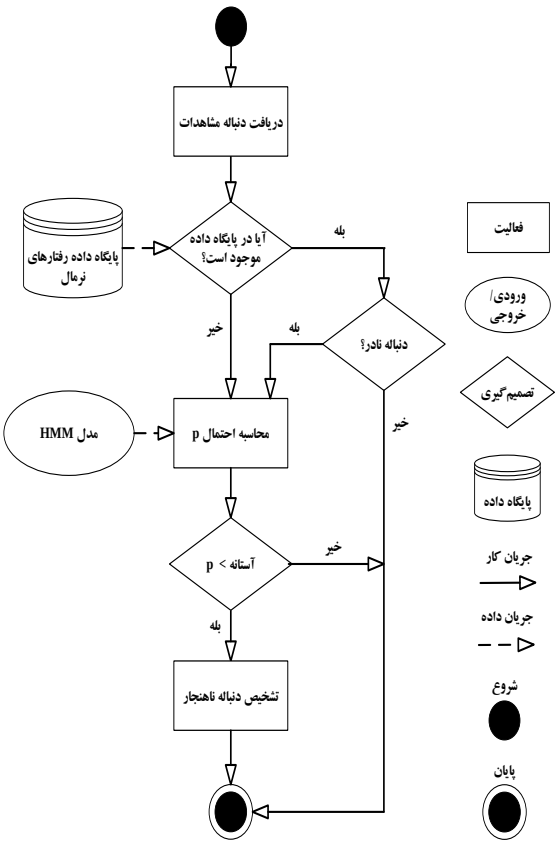
در مدل‌های مبتنی بر Adaboost-HMM، هر طبقه‌بند ضعیف یک مدل HMM است که تنها بر روی کلاس خاصی از حملات آموزش داده می‌شود. جهت ایجاد یک مدل Adaboost-HMM از یک نمایه هنجار استفاده می‌شود. فرآیند ترکیب الگوریتم‌های HMM و Adaboost برای آموزش نمایه هنجار در شکل (۱۴) نشان داده شده است. در این شکل α_iها بیانگر نرخ اطمینان هر طبقه‌بند ضعیف و $h_n(x_n)$ ها بیانگر میزان احتمال یک نمونه از یک طبقه‌بند ضعیف است. در نهایت با استفاده از رابطه (۱)، مقدار نهایی مدل (H) به ازای یک دنباله مشاهدات دریافتی به‌دست می‌آید. به‌عنوان دو عیب عمده این روش می‌توان به حساسیت بالای مدل به داده‌های نویزی و نیز افزایش زمان یادگیری کل به دلیل نوع آموزش دسته‌ای طبقه‌بندهای ضعیف اشاره کرد. از جمله مدل‌های توسعه داده شده موجود در این دسته می‌توان به پژوهش‌های [۵۱، ۵۲] اشاره کرد.

$$H=\sum_{i=1}^{K} \alpha_k h_k(x_n) \qquad (۱)$$



شکل۱۲- فرآیند ایجاد مدل تشخیص نفوذ sub-HMM

1. Supervised



شکل۱۳- روندنما مدل تشخیص نفوذ HMM چندلایه‌ای

۴-۱-۶-مدل‌های HMM ترکیبی

یکی دیگر از روش‌های متداول در ساخت مدل‌های تشخیص نفوذ مبتنی بر HMM، ترکیب مدل HMM با سایر روش‌های یادگیری ماشین است که هدف اصلی این روش نیز بهبود عملکرد آموزش مدل نهایی است. برخی روش‌های تشخیص نفوذ مبتنی بر مدل مارکوف، نیازمند منابع رایانشی و زمان پردازش زیاد برای فرآیند یادگیری هستند. برای رفع این مشکل می‌توان از روش‌های ترکیبی استفاده نمود. جهت کاهش زمان یادگیری در مدل‌های ترکیبی، از روش‌های کاهش حجم داده استفاده می‌شود تا داده‌های نامربوط موجود در مجموعه داده آموزش، قبل از فرآیند یادگیری حذف گردد. نمونه‌ای از این روش‌ها جهت حذف داده‌های نویزی موجود در مجموعه داده در مرجع [۵۳] معرفی شده است. در ادامه، فرآیند آموزش با استفاده از حجم داده‌های کمتری صورت می‌گیرد. در برخی روش‌های دیگر با ترکیب مدل HMM و الگوریتم‌هایی نظیر شبکه‌های عصبی مصنوعی[1]، سعی می‌شود تا قدرت یادگیری سیستم افزایش یابد که در این حالت، ابتدا دنباله‌ی مشاهدات دریافتی برای به‌دست آوردن دنباله گذار حالت (با استفاده از الگوریتم ویتربی[2]) به مدل HMM داده شده و در ادامه برای انجام فرآیند تشخیص نفوذ از شبکه عصبی مصنوعی استفاده می‌شود. از جمله مدل‌های توسعه داده شده موجود در این دسته می‌توان به مراجع [۵۳، ۵۴، ۵۵] اشاره کرد. در ادامه، هر یک از معماری‌های مبتنی بر HMM در جدول ۳ از جنبه‌های مختلف با یکدیگر مقایسه شده‌اند.

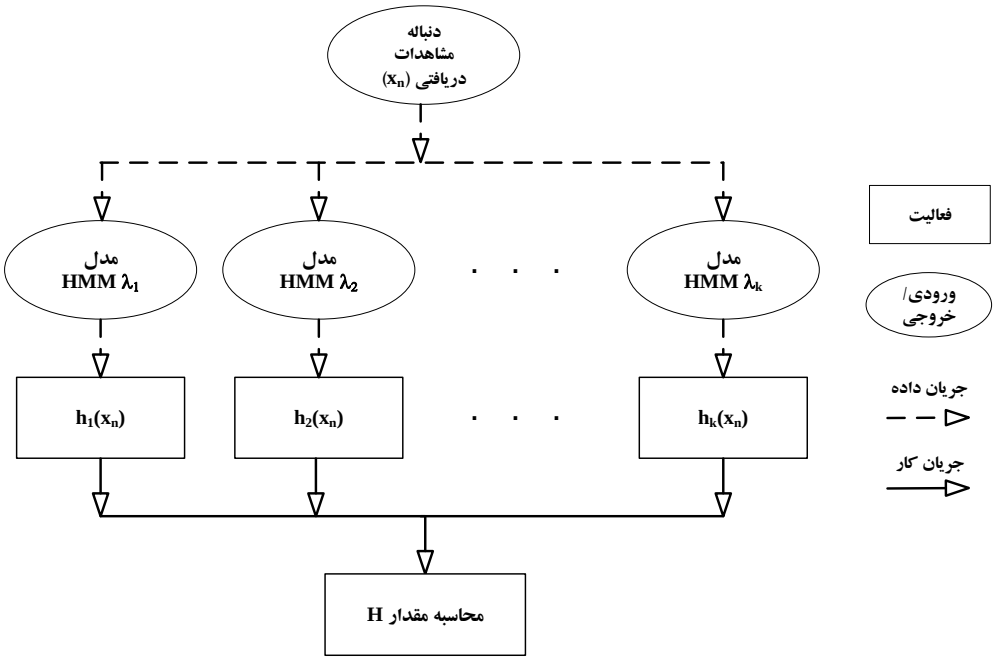
۵-معیارهای ارزیابی کمّی کیفیت روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف

برای ارزیابی جنبه‌های کیفی سیستم‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف، معیارهای کمّی وجود دارد تا کیفیت تکنیک‌های مختلف بر اساس این معیارها مورد مقایسه قرار گیرد [۵۶، ۵۷، ۵۸، ۵۹، ۶۰، ۶۱، ۶۲، ۶۳، ۶۴، ۶۵]. در ادامه برخی از مهم‌ترین این تکنیک‌ها که در پژوهش‌های موجود برای ارزیابی روش‌های مختلف مورد استفاده قرار گرفته‌اند، معرفی شده و سپس مدل‌های مختلف تشخیص نفوذ مبتنی بر HMM، از منظر این معیارها با یکدیگر مقایسه خواهند شد.

مهم‌ترین معیارهای ارزیابی کمّی موجود در حوزه تشخیص نفوذ مبتنی بر HMM عبارتند از:

- خطای مثبتِ غلط (FP) و منفیِ غلط[3] (FN): در بحث تشخیص نفوذ، یک داده مثبت، یک داده ناهنجار (نفوذ یا حمله) درنظر گرفته می‌شود در حالی که یک داده منفی، یک داده هنجار است. علاوه بر این، وقتی که یک IDS سعی می‌کند تا داده‌ها را طبقه‌بندی نماید، تصمیم او می‌تواند درست یا نادرست باشد. معمولا در سیستم‌های عملیاتی، نرخ داده‌های طبقه‌بندی شده صحیح، به‌مراتب بیشتر از نرخ داده‌های طبقه‌بندی شده اشتباه می‌باشد.

1. Artificial Neural Network
2. Viterbi
3. False Negative



شکل۱۴- نحوه ایجاد و ترکیب طبقه‌بندها در مدل Adaboost-HMM

مهم‌ترین معیارهای مورد استفاده برای ارزیابی کمّی دقت طبقه‌بندی داده‌ها، معیارهای مثبتِ غلط و منفیِ غلط هستند. یک خطای مثبتِ غلط هنگامی رخ می‌دهد که یک IDS، یک فعالیت مشروع را به اشتباه به‌عنوان فعالیت ناهنجار دسته‌بندی نماید. در مقابل، یک خطای منفیِ‌غلط وقتی رخ می‌دهد که یک IDS، یک فعالیت نامشروع را به اشتباه به‌عنوان فعالیت هنجار طبقه‌بندی کند.

- دقت: دقت عبارتست از میزان صحت عملکرد یک IDS که از طریق درصد تشخیص درست و نادرست فعالیت‌های ناهنجار ارزیابی می‌شود. به‌عنوان مثال، یک سیستمی که دارای دقت ۸۵٪ است، سیستمی است که ۸۵ نمونه از ۱۰۰ نمونه وقایع را به‌درستی در کلاس‌های صحیح دسته‌بندی می‌نماید. در یک دسته‌بندی ساده تعداد کلاس‌ها می‌تواند به دو دسته رفتار هنجار و ناهنجار (نفوذ یا حمله) تقسیم‌بندی شود.

جدول۳- مقایسه جنبه‌های کارایی تکنیک‌های مختلف تشخیص نفوذ مبتنی بر HMM

ردیف	نوع معماری	قابلیت تشخیص	زمان یادگیری	پیچیدگی محاسباتی	پیچیدگی فضایی	قابلیت گسترش‌پذیری	مهم‌ترین کارهای پژوهشی موجود
۱	HMM یگانه	کاهش	افزایش	کاهش	افزایش	کم	[۲۷]، [۳۱]، [۳۲]
۲	μ-HMM	افزایش	افزایش	افزایش	افزایش	زیاد	[۳۰]، [۴۸]
۳	sub-HMM	کاهش	کاهش	کاهش	کاهش	زیاد	[۲۴]، [۴۲]
۴	HMM چندلایه‌ای	افزایش	کاهش	افزایش	افزایش	زیاد	[۴۹]، [۵۰]
۵	Adaboost HMM	افزایش	افزایش	افزایش	کاهش	زیاد	[۵۱]، [۵۲]
۶	HMM ترکیبی	افزایش	کاهش	افزایش	کاهش	کم	[۵۳]، [۵۴]، [۵۵]

معیار دقت در رابطه (۲) نشان داده شده است.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad , Accuacy \in [0,1] \qquad (۲)$$

- صحت، فراخوانی و معیار F: همان‌گونه که پیش از این گفته شد، در شرایط هنجار، یک تفاوت بزرگ بین نرخ داده‌های هنجار و نرخ داده‌های نفوذ وجود دارد. این سه معیار از داده‌های صحیح طبقه‌بندی شده چشم‌پوشی نموده و تنها بر روی داده‌های نفوذ (TP+FN) و هشدارهای مثبتِ غلط (FP) تولید شده توسط یک IDS تمرکز می‌کنند.
صحت معیاری است که نشان می‌دهد در نمونه‌های مختلف، به چه میزان پیش‌بینی‌های یک IDS مبنی بر انجام یک نفوذ، واقعا درست بوده است. رابطه دقت در رابطه (۳) نشان داده شده است.

$$Precision = \frac{TP}{TP+FP} \quad , Precision \in [0,1] \qquad (۳)$$

معیار فراخوانی، بخش از دست رفته توسط معیار دقت را اندازه‌گیری کمّی می‌کند. به‌عبارت دیگر، درصد نفوذهای واقعی پوشش‌داده شده توسط طبقه‌بند را مشخص می‌کند. هر چه این میزان بیشتر باشد، تکنیک تشخیص نفوذ کارایی بالاتری خواهد داشت. نحوه محاسبه این معیار در رابطه (۴) نشان داده شده است.

$$Recall = \frac{TP}{TP+FN} \quad , Recall \in [0,1] \qquad (۴)$$

معیار F نیز، دیدگاه دیگری از دقت را با ترکیب دو معیار دقت و فراخوانی فراهم می‌آورد که دید جامع‌تری از دقت را ارائه می‌دهد. نحوه محاسبه این معیار در رابطه (۵) نشان داده شده است. هر چه میزان معیارهای دقت و فراخوانی بیشتر باشد، مقدار نهایی معیار F نیز بیشتر می‌شود.

$$F\_measure = \frac{2}{1/precision+1/recall}, F\_measure \in [0,1] \qquad (۵)$$

- کارایی: این معیار نیز بیانگر اعتبار و میزان درستی تصمیمات یک طبقه‌بند تشخیص نفوذ را نشان می‌دهد. نحوه محاسبه این معیار نیز در رابطه (۶) نشان داده شده است.

$$Soundness = \frac{\#\ of\ Correctly\ Detected\ Intrusions}{\#\ of\ Detected\ Intrusions} \qquad (۶)$$

- پاسخ به‌موقع (R_s): در واقع این یک معیارِ زمانی است که نشان می‌دهد تا چه میزان یک IDS بلافاصله بعد از تشخیص یک رفتار ناهنجار، هشدار موردنظر را ثبت نموده و مؤلفه پاسخ‌دهی به نفوذ را جهت انجام عمل متقابل راه‌اندازی می‌نماید. هر چه این میزان کمتر باشد، عملکرد IDS بهتر خواهد بود.

- کامل بودن (R_c): این معیار نمایانگر فضای حالتِ آسیب‌پذیری‌ها و حملاتی است که توسط یک IDS پوشش داده می‌شود. هر چه روش موردنظر بتواند حملات شناخته شده و ناشناخته بیشتری را پوشش دهد، میزان این معیار بیشتر خواهد بود. در ادامه، در جدول(۴)، مدل‌های مختلف تشخیص نفوذ مبتنی بر HMM، از منظر پارامترهای ارزیابی با یکدیگر مقایسه شده‌اند.

۶-مقایسه پژوهش جاری با پژوهش‌های موجود

با استفاده از روش تحقیق نظام‌مند مورد استفاده در این پژوهش و با بررسی پژوهش‌های انجام شده از سال ۲۰۰۰ میلادی به بعد، تعداد سه پژوهش مروری صورت گرفته در زمینه تشخیص نفوذ به کمک مدل‌های مخفی مارکوف یافت شده است [۶، ۸، ۹، ۵۸] که هیچ یک از پژوهش‌های مذکور به‌صورت نظام‌مند صورت نپذیرفته است. علاوه بر این در هیچ یک از پژوهش‌های مذکور، دسته‌بندی جامعی برای تبیین اهمیت و جایگاه مدل‌های مخفی مارکوف در کاربردهای تشخیص نفوذ ارائه نشده است.
به‌طور مثال در پژوهش صورت گرفته توسط وانگ و همکاران [۵۸] سعی شده است تا معماری‌های متنوع مدل مخفی مارکوف برای کاربردهای تشخیص نفوذ تبیین گردد که عدم تبیین بصری مدل‌ها، فهم معماری‌های معرفی شده را دشوار می‌سازد. به‌عنوان نمونه‌ای دیگر در پژوهش شیمپی و پیتال [۸] سعی شده است تا مهم‌ترین کاربردها در حوزه تشخیص نفوذ مبتنی بر مدل مخفی مارکوف بیان گردد که این امر به‌طور ناقص و بدون اشاره به پژوهش‌های مهم انجام شده در هر کاربرد صورت پذیرفته است. یکی دیگر از برتری‌های پژوهش جاری، بررسی پژوهش‌های موجود مبتنی بر مدل مخفی مارکوف در هر دو شاخه مبتنی بر امضاء و مبتنی بر ناهنجاری بوده است که به‌طور مثال، پژوهش [۵۸] تنها به بررسی گونه خاصی از روش‌های تشخیص نفوذ مبتنی بر ناهنجاری پرداخته است. از جمله دیگر مزیت‌های مهم پژوهش جاری می‌توان به بررسی معیارهای اندازه‌گیری کمّی کیفیت روش‌های تشخیص نفوذ مبتنی بر مدل مخفی مارکوف و ارزیابی معماری‌های مختلف معرفی شده مبتنی بر این مدل اشاره کرد که در

پژوهش‌های پیشین تلاشی در جهت تحقق این امر نیز صورت نپذیرفته است. در ادامه، نتایج مقایسه پژوهش جاری با پژوهش‌های پیشین انجام شده در این حوزه، در جدول (۵) ارائه شده است.

۷-چالش‌ها و مسائل باز

با استفاده از مطالب گفته شده در بخش‌های پیشین، از جمله مهم‌ترین مسائل و نقاط پژوهشی باز موجود در این حوزه می‌توان به موارد زیر اشاره کرد:

- ایجاد مدل‌های تشخیص نفوذ مبتنی بر منابع داده‌ای چندگانه در محیط‌های توزیع‌شده
- لزوم معرفی مدل‌های مبتنی بر HMM کاراتر جهت غلبه هر چه بیشتر بر زمان یادگیری مدل و افزایش دقت تشخیص
- استفاده از مدل‌های تشخیص نفوذ برای سه کاربرد نسبتا جدید یعنی استفاده از آن‌ها در محیط‌های ابر، پیش‌بینی اهداف بعدی مهاجم در حملات شبکه‌ای و تشخیص سناریوی حملات چندمرحله‌ای پیچیده
- ترکیب مدل‌های HMM با دیگر روش‌های یادگیری ماشین نظیر تکنیک‌های خوشه‌بندی جهت دقیق‌تر نمون هر چه بیشتر تعداد حالت‌های مخفی و نیز مقادیر احتمالات گذار بین حالت‌ها

جدول۴- مقایسه مدل‌های تشخیص نفوذ مختلف بر اساس معیارهای ارزیابی

ردیف	نوع معماری	خطای مثبتِ غلط	دقت	صحت	معیار F	کامل بودن	پاسخ به نفوذ
۱	HMM یگانه	زیاد	زیاد	کم	زیاد	دارد	سریع
۲	μ-HMM	کم	زیاد	زیاد	زیاد	دارد	کند
۳	sub-HMM	زیاد	کم	کم	کم	دارد	کند
۴	HMM چندلایه‌ای	زیاد	کم	کم	کم	دارد	سریع
۵	Adaboost HMM	کم	زیاد	زیاد	زیاد	دارد	کند
۶	HMM ترکیبی	کم	زیاد	زیاد	زیاد	دارد	سریع

جدول۵- مقایسه ی پژوهش مروری جاری با دیگر مرورهای موجود در حوزه تشخیص نفوذ مبتنی بر مدل مخفی مارکوف

معیار / پژوهش	نوع مرور	تعداد مقالات پایه	ارائه دسته‌بندی	بررسی و تحلیل بصری معماری‌ها	ارزیابی کارایی انواع معماری‌ها	پوشش انواع کاربرد	مقایسه‌ی پژوهش‌های انجام شده
پژوهش جاری، ۲۰۱۵	نظام‌مند	۳۸	*	*	*	*	*
[۶]، ۲۰۱۴	غیر نظام‌مند	۱۶	*				
[۸]، ۲۰۱۳	غیر نظام‌مند	۱۴				*	
[۵۸]، ۲۰۱۰	غیر نظام‌مند	۲۰			*		
[۹]، ۲۰۰۱	غیر نظام‌مند	۱۹		*			*

۸-نتیجه گیری

سیستم تشخیص نفوذ به‌عنوان یکی از مهم‌ترین ابزارهای مورد استفاده در سیستم‌های نرم‌افزاری، نقش بسیار مهمی در تحقق امنیت به‌عنوان یک جنبه کیفی مهم در این سیستم‌ها ایفا می‌کند. استفاده از سیستم‌های تشخیص نفوذ علاوه بر سایر تجهیزات امنیتی سخت، سبب کاهش میزان احتمال نفوذهای ناخواسته به سیستم‌های نرم‌افزاری می‌گردد. روش‌های متنوعی برای فرآیند تشخیص نفوذ معرفی شده‌اند که یکی از پرکاربردترین آن‌ها که دارای قابلیت گسترش‌پذیری زیادی است، مدل‌های مخفی مارکوف می‌باشد. هرچند به‌کارگیری این مدل‌ها در ابتدای راه، ممکن است به دلیل هزینه‌های مربوط به آموزش اولیه مدل، کمّی دارای سربار رایانشی باشد، اما پس از ایجاد مدل، دقت تشخیص رخدادهای ناهنجار و نیز قابلیت انعطاف‌پذیری آن‌ها در جهت به‌روزرسانی دانش دریافتی از مشاهدات از میزان بسیار مطلوبی برخوردار است. در این مقاله، ضمن بررسی همه‌جانبه پژوهش‌های موجود در این زمینه، به بیان چالش‌ها و مسائل باز موجود در این حیطه پرداخته شده است.

مراجع

[1] R. Mitchell, and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems", ACM Computing Surveys, Vol. *46*, NO. *4*, April 2014, pp. 55.

[2] S. Axelsson, "Intrusion detection systems: A survey and taxonomy", Vol. *90*, March 2000, Technical report.

[3] H. Debar, M. Dacier, and A. Wespi, "A revised taxonomy for intrusion-detection systems", In Annales des télécommunications, Vol. *55*, NO. *7-8*, July 2000, pp. 361 – 378.

[4] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey", ACM computing surveys (CSUR), Vol. *41*, NO. *3*, July 2009, pp. 15.

[5] A. Lazarevic, L. Ertöz, V. Kumar, A. Ozgur and J. Srivastava "A comparative study of anomaly detection schemes in network intrusion detection", In Proceedings of the SIAM International Conference on Data Mining, San Francisco, USA, May 2003, pp. 25-36.

[6] H. Sukhwani, V. Sharma, and S. Sharma, "A Survey of anomaly detection techniques and hidden Markov model", International Journal of Computer Applications, Vol. *93*, NO. *18*, January 2014, pp. 26 – 31.

[7] J. Hu, "Host-based anomaly intrusion detection", In Handbook of information and communication security, Springer, Berlin, Heidelberg, 2010, pp. 235 – 255.

[8] S. Shimpi, and V. Patil, "Hidden Markov model as classifier: a survey", In 2013 International Conference on Computer Science and Engineering, March 2013, pp. 13530-13533.

[9] S. Jha, K. Tan, and R. A. Maxion, "Markov chains, classifiers, and intrusion detection", In Computer Security Foundations Workshop, June 2011, pp. 0206.

[10] B. Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, "Systematic literature reviews in software engineering–a systematic literature review", Information and software technology, Vol. *51*, NO. *1*, January 2009, pp. 7 – 15.

[11] P. Brereton, B. A. Kitchenham, D. Budgen, M. Turner, and M. Khalil, "Lessons from applying the systematic literature review process within the software engineering domain", Journal of systems and software, Vol. *80*, NO. *4*, April 2007, pp. 571 – 583.

[12] The Results of the SLR of this Paper, (Available Online: http://sqlab.um.ac.ir/images/219/files/SQLab-RequestFarsi.pdf)..

[13] A. S. Abdel-Aziz, A. E. Hassanien, A. T. Azar, and S. E. O. Hanafi, "Machine learning techniques for anomalies detection and classification", In Advances in security of information and communication networks, Springer, Berlin, Heidelberg, 2013, pp. 219 – 229.

[14] T. Verwoerd, and R. Hunt, "Intrusion detection techniques and approaches", Computer Communications, Vol. *25*, NO. *15*, September 2002, pp. 1356 – 1365.

[15] C. F. Tsai, Y. F. Hsu, C. Y. Lin, and W. Y. Lin, "Intrusion detection by machine learning: A review", Expert Systems with Applications, Vol. *36*, NO. *10*, December 2009, pp. 11994 – 12000.

[16] P. Blunsom, "Hidden markov models", Lecture notes, Vol. *15*, NO. *18-19*, August 2004, pp. 48.

[17] L. R. Rabiner, and B. H. Juang, "An introduction to hidden Markov models", IEEE ASSP magazine, Vol. *3*, NO. *1*, January 1986, pp. 4 – 16.

[18] T. F. Lunt, "A survey of intrusion detection techniques", Computers & Security, Vol. *12*, 1993, pp. 405 – 418.

[19] W. Lee, and S. J. Stolfo, "Data mining approaches for intrusion detection", In USENIX Security Symposium, January 1998, pp. 79 – 93.

[20] Y. Zhang, and W. Lee, "Intrusion detection in wireless ad-hoc networks", In Proceedings of the 6th annual international conference on Mobile computing and networking, Boston, Massachusetts, USA, August 2000, pp. 275-283.

[21] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden Markov model", IEEE Transactions on dependable and secure computing, Vol. *5*, NO. *1*, January 2008, pp. 37 – 48.

[22] N. Luktarhan, X. Jia, L. Hu, and N. Xie, "Multi-stage attack detection algorithm based on hidden Markov model", In Web Information Systems and Mining, Springer Berlin Heidelberg, 2012, pp. 275 – 282.

[23] DARPA Intrusion Detection Datasets, (Available Online: https://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/data/2000data.html).

[24] X. A. Hoang, and J. Hu, "An efficient hidden Markov model training scheme for anomaly intrusion detection of server applications based on system calls", In Networks, 2004.(ICON 2004). Proceedings. 12th IEEE International Conference on, Singapore, Vol. *2*, November 2004, pp. 470-474.

[25] S. B. Cho, and H. J. Park, "Efficient anomaly detection by modeling privilege flows using hidden Markov model", Computers & Security, Vol. *22*, NO. *1*, January 2003, pp. 45 – 55.

[26] W. Li, and Z. Guo, "Hidden Markov model based real time network security quantification method", In Networks Security, Wireless Communications and Trusted Computing, NSWCTC'09. International Conference on, Wuhan, Hubei, China, Vol. *2*, April 2009, pp. 338-343.

[27] A. Vartak, C. D. Patil, and C. K. Patil, "Hidden Markov model for credit card fraud detection", International Journal of Computer Science and Information Technologies, Vol. *5*, NO. *6*, 2014, pp. 7446 – 7451.

[28] S. S. Dhok, and G. R. Bamnote, "Credit card fraud detection using hidden Markov model", International Journal of Soft Computing and Engineering (IJSCE), Vol. *2*, NO. *1*, May 2012, pp. 231 – 237.

[29] A. Frossi, F. Maggi, G. L. Rizzo, and S. Zanero, "Selecting and improving system call models for anomaly detection", In Detection of Intrusions and Malware, and Vulnerability Assessment, Springer Berlin Heidelberg, 2009, pp. 206-223.

[30] E. N. Yolacan, J. G. Yolacan, and D. R. Kaeli, "System Call anomaly detection using multi-HMMs", In Software Security and Reliability-Companion (SERE-C), IEEE Eighth International Conference on, San Francisco, CA, USA, June 2014, pp. 25-30.

[31] M. A. Pathak, S. Rane, W. Sun, and B. Raj, "Privacy preserving probabilistic inference with hidden Markov models", In Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on, May 2011, pp. 5868 – 5871.

[32] S. Guo, S. Zhong, and A. Zhang, "A privacy preserving Markov model for sequence classification", In Proceedings of the International Conference on Bioinformatics, Computational Biology and Biomedical Informatics, Wshington DC, USA, September 2013, pp. 561.

[33] W, Gobel, “Detecting botnets using hidden Markov models on network traces", white paper, 2013.

[34] T. H. Austin, E. Filiol, S. Josse, and M. Stamp, "Exploring hidden Markov models for virus analysis: a semantic approach", In System Sciences (HICSS), 46th Hawaii International Conference on, Wailea, Maui, HI, USA, January 2013, pp. 5039-5048.

[35] A. Årnes, F. Valeur, G. Vigna, and R. A. Kemmerer, "Using hidden Markov models to evaluate the risks of intrusions", In Recent Advances in Intrusion Detection, Springer Berlin Heidelberg, 2006.

[36] H. Li, Y. Liu, and D. He, "Research on technology for IT system security assessment based on Markov chain", In Signal Processing, 8th International Conference on, Beijing, China, Vol. *4*, November 2006.

[37] C. Lai-Cheng, "A high-efficiency intrusion prediction technology based on Markov chain", In Computational Intelligence and Security Workshops, CISW, International Conference on, Heilongjiang, China, December 2007, pp. 518-521.

[38] F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer, "Comprehensive approach to intrusion detection alert correlation", IEEE Transactions on dependable and secure computing, Vol. *1*, NO. *3*, July 2004, pp. 146 – 169.

[39] H. Farhadi, M. AmirHaeri, and M. Khansari, "Alert correlation and prediction using data mining and HMM", The ISC International Journal of Information Security, Vol. *3*, NO. *2*, October 2011, pp. 77 – 102.

[40] X. Zan, F. Gao, J. Han, and Y. Sun, "A hidden Markov model based framework for tracking and predicting of attack intention", In Multimedia Information Networking and Security, MINES'09. International Conference on, Hubei, China, Vol. *2*, November 2009, pp. 498-501.

[41] S. Zhicai, and X. Yongxiang, "A novel hidden Markov model for detecting complicate network attacks", In Wireless Communications, Networking and Information Security (WCNIS), IEEE International Conference on, Beijing, China, June 2010, pp. 312-315.

[42] J. Hu, X. Yu, D. Qiu, and H. H. Chen, "A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection", IEEE network, Vol. *23*, NO. *1*, January 2009, pp. 42 – 47.

[43] W. Wang, X. H. Guan, and X. L. Zhang, "Modeling program behaviors by hidden Markova models for intrusion detection", In Machine Learning and Cybernetics, Proceedings of 2004 International Conference on, Shanghai, China, China, Vol. *5*, August 2004, pp. 2830-2835.

[44] S. Shin, S. Lee, H. Kim, and S. Kim, "Advanced probabilistic approach for network intrusion forecasting and detection", Expert systems with applications, Vol. *40*, NO. *1*, January 2013, pp. 315 – 322.

[45] R. Salazar-Hernández, and J. E. Díaz-Verdejo, "Hybrid detection of application layer attacks using Markov models for normality and attacks", In Information and Communications Security, Springer Berlin Heidelberg, 2010.

[46] P. Kumar, N. Nitin, V. Sehgal, K. Shah, S. S. P. Shukla, and D. S. Chauhan, "A novel approach for security in Cloud Computing using Hidden Markov Model and clustering", In Information and Communication Technologies (WICT), World Congress on, Mumbai, India, December 2011, pp. 810-815.

[47] H. Banafar, and S. Sharma, "Intrusion detection and prevention system for cloud simulation environment using hidden Markov model and MD5", IEEE Transactions on Energy Conversion, Vol. *90*, NO. *19*, January 2014, pp. 6 – 11.

[48] G. Author1, K. Author2, and A. Author3, "Combining hidden Markova models for improved anomaly detection", In Communications, ICC'09. IEEE International Conference on, Dresden, Germany, August 2009, pp. 1-6.

[49] X. Zhou, Q. Peng, and J. Wang, "Intrusion detection method based on two-layer HMM", Application Research of Computers, Vol. *25*, NO. *3*, March 2004.

[50] X. D. Hoang, J. Hu, and P. Bertok, "A multi-layer model for anomaly intrusion detection using program sequences of system calls", In Proc. 11th IEEE Int’l. Conf, 2003, pp. 531-536.

[51] J. Zhang, Y. Liu, and X. Liu, "Anomalous detection based on Adaboost-HMM", In Intelligent Control and Automation, WCICA 2006. The Sixth World Congress, Dalian, China, Vol. *1*, June 2006, pp. 4360-4363.

[52] Y. S. Chen, and Y. M. Chen, "Combining incremental Hidden Markov Model and Adaboost algorithm for anomaly intrusion detection", In Proceedings of the ACM SIGKDD Workshop on Cybersecurity and intelligence informatics, Paris, France, June 2009, pp. 3-9.

[53] F. Zeng, K. Yin, M. Chen, and W. Wang, "New anomaly detection method based on rough set reduction and HMM", In Computer and Information Science, ICIS 2009. Eighth IEEE/ACIS International Conference on IEEE, Shanghai, China, June 2009, pp. 285-289.

[54] Y. Jiang, Y. Xu, and Y. Xu, "A novel intrusions detection method based on HMM embedded neural network", In Advances in Natural Computation, Springer Berlin Heidelberg, 2005, pp. 139-148.

[55] X. D. Hoang, J. Hu, and P. Bertok, "A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference", Journal of Network and Computer Applications, Vol. *32* NO. *6*, November 2009, pp. 1219 – 1228.

[56] A. S. Coronado, "Computer Security: Principles and Practice", Journal of information privacy and security", Vol. *9*, NO. *2*, July 2014, pp. 62 – 65.

[57] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges", Computers & Security, Vol. *28*, NO. *1-2*, February 2009, pp. 18 – 28.

[58] P. Wang, L. Shi, B. Wang, Y. Wu, and Y. Liu, "Survey on HMM based anomaly intrusion detection using system calls", In 5th International Conference on Computer Science & Education, Hefei, China, August 2010, pp. 102-105.

[59] A. S. Sendi, M. Dagenais, M. Jabbarifar, and M. Couture, "Real time intrusion prediction based on optimized alerts with hidden Markov model", Journal of Networks, Vol. *7*, NO. *2*, February 2012, pp. 311 – 321.

[60] S. Xiang, Y. Lv, C. Xia, Y. Li and Z. Wang, "A method of network security situation assessment based on hidden Markov model", In International Symposium on Intelligence Computation and Applications, Springer Singapore, 2015, pp. 631-639.

[61] S. C. Liu, and Y. Liu, "Network security risk assessment method based on HMM and attack graph model", In Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 17th IEEE/ACIS International Conference, Shanghai, China, May 2016, pp. 517-522.

[62] H. K. Pao, Y. J. Lee, and C. Y. Huang, "Statistical learning methods for information security: fundamentals and case studies", Applied Stochastic Models in Business and Industry, Vol. *31*, NO. *2*, March 2015, pp. 97 – 113.

[63] D. Iyar, A. Mohanpurkar, S. Janardhan, D. Rathod, and A. Sardeshmukh, "Credit card fraud detection using hidden Markov model", In 2011 World Congress on Information and Communication Technologies, Mumbai, India, 2011, pp. 1062-1066.

[64] A. L. Buczak, and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection", IEEE Communications Surveys & Tutorials, Vol. *18*, NO. *2*, October 2016, pp. 1156 – 1176.

[65] M. M. Bharati, and S. Lomte, "A survey on hidden Markov model (HMM) based intention prediction techniques", International Journal of Engineering Research and Applications, Vol. *6*, NO. *2*, January 2016, pp. 167 – 172.