

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



دانشگاه شاهرود

دانشکده ریاضی و رایانه
بخش علوم رایانه

پایان نامه تحصیلی برای دریافت درجه کارشناسی ارشد رشته علوم رایانه گرایش
سیستم‌های هوشمند

ارائه روشی جدید به منظور تشخیص نفوذ به شبکه با داده کاوی

مؤلف:

زهرا اصغری ورزنده

استاد راهنما:

دکتر مرجان کوچکی رفسنجانی

استاد مشاور:

دکتر محمد مسعود جاویدی

شهریور ۹۲



این پایان نامه به عنوان یکی از شرایط احراز کارشناسی ارشد به

بخش کامپیوتر - دانشکده ریاضی و رایانه
دانشگاه شهید باهنر کرمان

تسلیم شده است و هیچگونه مدرکی به عنوان فراغت از تحصیل دوره مزبور شناخته نمی شود.

دانشجو: زهرا اصغری ورزنده

استاد راهنما: دکتر مرجان کوچکی رفسنجانی

استاد مشاور: دکتر محمد مسعود جاویدی

دوره ۱:

دوره ۲:

نماینده تحصیلات تکمیلی دانشکده:

معاون آموزشی و پژوهشی دانشکده:

حق چاپ محفوظ و مخصوص به دانشگاه شهید باهنر کرمان است.

تقدیم به پدر و مادرم

آنانکه وجودم برایشان همه رنج است

و وجودشان برایم همه مهر

و تقدیم به خواهر و برادران عزیزم که همواره موجب شادی و دلگرمی من بوده اند.

باساس از سه وجود مقدس:

آنانکه ناتوان شدند تا ما به توانایی برسیم...

موباشان سپید شد تا ما رو سفید شویم...

و عاشقانه سوختند تا کرم بخش وجود ما و رو سگند را بهمان باشند...

پدرانمان

مادرانمان

و استادانمان

بطور خاص از استید کراتقدر سرکار خانم دکتر کوچکی و جناب آقای دکتر جاویدی که با تشویق ها و راهنمایی های خود راه را برایم
هموار نمودند شکر می نمایم.

چکیده

امروزه با گسترش روزافزون شبکه‌های کامپیوتری، امنیت شبکه از اولویت زیادی برخوردار می‌شود. سیستم‌های تشخیص نفوذ، سخت‌افزار و یا نرم‌افزاری است که کار نظارت بر شبکه کامپیوتری را در مورد فعالیت‌های مخرب و یا نقض سیاست‌های مدیریتی و امنیتی انجام می‌دهد و گزارش‌های حاصل را به بخش مدیریت شبکه ارائه می‌دهد. رویکردهای تشخیص نفوذ به دو دسته کلی تشخیص موارد سوءاستفاده و تشخیص موارد غیرمتعارف تقسیم می‌شوند. سیستم‌های تشخیص موارد سوءاستفاده تلاش می‌کنند حمله‌ها را با استفاده از کشف الگوهای نفوذ که توسط خبرگان تشخیص داده شده و گزارش می‌شوند شناسایی کنند. رویکرد تشخیص موارد غیر متعارف در واقع توسعه رویکرد قبلی است با این توضیح که در این رویکرد، الگوهایی از رفتارهای نرمال در شبکه از قبل، تشخیص داده شده است و نفوذ می‌تواند مبتنی بر مقداری انحراف از رفتارهای نرمال در شبکه تعریف شود. در سیستم‌های تشخیص نفوذ از روش‌های مختلفی استفاده می‌شود که یکی از این روش‌ها داده‌کاوی است. داده‌کاوی از تکنیک‌های مختلفی مانند تکنیک‌های آماری و یادگیری ماشین بهره می‌برد. در این پایان نامه تکنیک‌های یادگیری ماشین بررسی شده و برای پیاده‌سازی سیستم تشخیص نفوذ از روش دسته‌بندی مبتنی بر قانون فازی استفاده شده است و این طرح برای یافتن وزن‌های بهینه قوانین از الگوریتم ژنتیک بهره می‌برد. روش پیشنهادی بر روی پایگاه داده KDD99 و با استفاده از نرم‌افزار متلب پیاده‌سازی شده است که در مقایسه با سایر روش‌ها (الگوریتم‌های ماشین بردار پشتیبان (SVM)¹، K-Nearest Neighbor (KNN)²، Naïve Bayes³، مدل پنهان مارکوف (HMM)³، C4.5، K-mean، Y-mean و برخی از روش‌های ترکیبی) نتایج بهتری حاصل شده است.

کلید واژه: تشخیص نفوذ⁴، داده‌کاوی⁵، سیستم دسته‌بندی مبتنی بر قانون فازی⁶، الگوریتم ژنتیک⁷

¹ Support Vector Machine (SVM)

² K-Nearest Neighbor (KNN)

³ Hidden Markov models (HMM)

⁴ Intrusion Detection (ID)

⁵ Data mining

⁶ Fuzzy Rule Base Classification System (FRBCS)

⁷ Genetic Algorithm (GA)

فهرست مطالب

| صفحه | عنوان |
|---------|--|
| | فصل اول: کلیات |
| ۲-۱-۱ | مقدمه |
| ۲-۱-۲ | بیان مسئله و پیشینه تحقیق |
| ۲-۱-۳ | چالش‌ها و اهداف تحقیق |
| ۲-۱-۴ | مروری بر فصول پایان نامه |
| | فصل دوم: مفاهیم کلی درباره سیستم‌های تشخیص نفوذ |
| ۲-۱-۱ | مقدمه |
| ۲-۲-۱ | انواع حملات شبکه |
| ۲-۲-۱-۱ | انواع حملات شبکه ای با توجه به طریقه حمله |
| ۲-۲-۱-۲ | انواع حملات شبکه ای با توجه به حمله کننده |
| ۲-۲-۳ | تشخیص نفوذ |
| ۲-۳-۱ | اجزای سامانه‌های تشخیص نفوذ |
| ۲-۳-۲ | ساختار و همبندی اجزای سیستم تشخیص نفوذ |
| ۲-۴-۱ | انواع روش‌های تشخیص نفوذ |
| ۲-۴-۱-۱ | روش‌های تشخیص سوء استفاده |
| ۲-۴-۱-۲ | سیستم‌های خبره |
| ۲-۴-۱-۳ | استفاده از روش‌های بازیابی اطلاعات |
| ۲-۴-۱-۴ | روش‌های تشخیص ناهنجاری |
| ۲-۴-۲ | مدل اولیه Denning |
| ۲-۴-۲-۱ | معیارهای آماری |
| ۲-۴-۲-۲ | سایر معیارها |
| ۲-۵-۱ | انواع سیستم‌های تشخیص نفوذ |
| ۲-۵-۱-۱ | سیستم‌های تشخیص نفوذ مبتنی بر میزبان |
| ۲-۵-۱-۲ | سیستم‌های تشخیص نفوذ مبتنی بر شبکه |

- ۲-۵-۲-۱- اجزای تشکیل دهنده سیستم‌های تشخیص نفوذ مبتنی بر شبکه ۲۲
- ۲-۵-۳- سیستم‌های توزیع شده ۲۲
- ۲-۶-۱- انواع معماری در سیستم‌های تشخیص نفوذ ۲۳

فصل سوم: داده کاوی و تکنیک‌های آن

- ۳-۱-۱- مقدمه ۲۵
- ۳-۲-۱- اهداف و وظایف داده کاوی ۲۵
- ۳-۳-۱- ریشه‌های داده کاوی ۲۷
- ۳-۴-۱- فرآیند داده کاوی ۲۷
- ۳-۴-۲- بیان مسئله و فرموله کردن فرضیه‌ها ۲۸
- ۳-۴-۳- جمع‌آوری داده‌ها ۲۸
- ۳-۴-۴- پیش‌پردازش داده‌ها ۲۹
- ۳-۴-۵- برآورد مدل ۳۰
- ۳-۴-۶- تفسیر مدل و نتیجه‌گیری ۳۰
- ۳-۵-۱- آماده‌سازی داده ۳۱
- ۳-۵-۲- نمایش داده‌های خام ۳۱
- ۳-۵-۳- مشخصه‌های داده‌های خام ۳۲
- ۳-۵-۴- تبدیل داده‌های خام ۳۲
- ۳-۶-۱- تقلیل داده‌ها ۳۴
- ۳-۶-۲- ابعاد مجموعه‌های داده بزرگ ۳۴
- ۳-۶-۳- کاهش ویژگی‌ها ۳۵
- ۳-۶-۴- کاهش مقادیر ۳۶
- ۳-۷-۱- یادگیری از داده ۳۶
- ۳-۷-۲- انواع روش‌های یادگیری ۳۷
- ۳-۸-۱- ورودی‌ها و خروجی‌ها ۳۹
- ۳-۹-۱- تکنیک‌های داده کاوی ۴۲
- ۳-۹-۲- روش‌های آماری ۴۲

| | |
|----|---|
| ۴۲ |۳-۹-۱-۱- استنباط آماری |
| ۴۲ |۳-۹-۱-۲- ارزیابی تفاوت‌ها در مجموعه‌های داده |
| ۴۳ |۳-۹-۱-۳- استنباط بیزی |
| ۴۳ |۳-۹-۱-۴- رگرسیون پیش‌بینی |
| ۴۴ |۳-۹-۱-۵- تحلیل واریانس |
| ۴۴ |۳-۹-۱-۶- رگرسیون لوژستیک |
| ۴۴ |۳-۹-۲- تحلیل خوشه‌ای |
| ۴۴ |۳-۹-۲-۱- مفاهیم خوشه‌بندی |
| ۴۵ |۳-۹-۲-۲- خوشه‌بندی سلسله‌مراتبی تراکمی |
| ۴۶ |۳-۹-۲-۳- خوشه‌بندی افزایی |
| ۴۷ |۳-۹-۲-۴- خوشه‌بندی افزایشی |
| ۴۸ |۳-۹-۳- درختان تصمیم و قوانین تصمیم‌گیری |
| ۴۹ |۳-۹-۳-۱- درخت‌های تصمیم‌گیری |
| ۵۲ |۳-۹-۴- قواعد انجمنی |
| ۵۲ |۳-۹-۵- شبکه‌های عصبی مصنوعی |
| ۵۴ |۳-۹-۶- الگوریتم‌های ژنتیک |
| ۵۶ |۳-۹-۶-۱- نمای کلی الگوریتم ژنتیک |
| ۵۹ |۳-۹-۷- مجموعه‌های فازی |
| ۶۰ |۳-۱۰-۱- معرفی چند الگوریتم داده‌کاوی |
| ۶۰ |۳-۱۰-۱- C4.5 |
| ۶۱ |۳-۱۰-۲- Naïve Bayes |
| ۶۲ |۳-۱۰-۳- ماشین‌های بردار پشتیبان (SVM) |
| ۶۳ |۳-۱۰-۴- K- نزدیکترین همسایه (KNN) |
| ۶۴ |۳-۱۰-۵- Apriori |
| ۶۵ |۳-۱۰-۶- K-means |
| ۶۶ |۳-۱۰-۷- C-means |

۶۷..... Y-means -۸-۱۰-۳

فصل چهارم: پیشینه داده کاوی در تشخیص نفوذ

۶۹..... ۱-۴- مقدمه

۶۹..... ۲-۴- فرآیند داده کاوی در تشخیص نفوذ

۷۰..... ۱-۲-۴- ایجاد بستر مناسب

۷۱..... ۲-۲-۴- پیش پردازش داده

۷۲..... ۳-۲-۴- انتخاب خصیصه

۷۲..... ۴-۲-۴- معماری سیستم‌های تشخیص نفوذ توسط حسگرهای شبکه

۷۳..... ۳-۴- استفاده از تکنیک‌های داده کاوی در تشخیص نفوذ

۷۳..... ۱-۳-۴- تکنیک‌های آماری در تشخیص نفوذ

۷۴..... ۱-۱-۳-۴- مدل‌های مخفی مارکوف (HMM)

۷۴..... ۲-۳-۴- تکنیک‌های یادگیری ماشین در تشخیص نفوذ

۷۴..... ۱-۲-۳-۴- تکنیک‌های دسته‌بندی

۸۰..... ۲-۲-۳-۴- تکنیک‌های خوشه‌بندی

۸۲..... ۴-۴- چگونگی مقایسه کارایی الگوریتم‌ها

۸۲..... ۱-۴-۴- انتخاب مجموعه داده

۸۳..... ۲-۴-۴- دسته‌بندی مجموعه داده KDD99

۸۴..... ۳-۴-۴- ویژگی‌های اشتقاقی

۸۶..... ۵-۴- نتایج بدست آمده از کارهای انجام شده

فصل پنجم: ارائه روش پیشنهادی

۸۹..... ۱-۵- مقدمه

۸۹..... ۲-۵- سیستم‌های دسته‌بندی مبتنی بر قانون فازی

۹۰..... ۱-۲-۵- ساختار پایگاه قانون فازی اولیه

۹۲..... ۳-۵- استفاده از الگوریتم ژنتیک در روش پیشنهادی

۹۵..... ۴-۵- ارائه روش پیشنهادی برای تعیین وزن قوانین

فصل ششم: پیاده‌سازی و ارزیابی کارایی

- ۹۸-۱-۶- مقدمه
- ۹۸-۲-۶- آماده‌سازی و پیش پردازش داده
- ۱۰۱-۳-۶- نحوه پیاده‌سازی روش پیشنهادی
- ۱۰۳-۴-۶- معیار ارزیابی کارایی برای سیستم‌های تشخیص نفوذ
- ۱۰۵-۵-۶- مقایسه کارایی روش پیشنهادی با سایر روش‌ها

فصل هفتم: نتیجه‌گیری و پیشنهادات

- ۱۱۱-۱-۷- نتیجه‌گیری
- ۱۱۲-۲-۷- پیشنهادات برای کارهای آتی
- ۱۱۳- مراجع
- ۱۲۱- چکیده انگلیسی

فهرست شکل‌ها

| صفحه | عنوان |
|----------|---|
| ۳۱..... | شکل ۱-۳: فرآیند داده‌کاوی |
| ۳۲..... | شکل ۲-۳: نمایش مجموعه داده |
| ۳۷..... | شکل ۳-۳: انواع استنباط |
| ۳۹..... | شکل ۴-۳: دونوع یادگیری (الف) یادگیری بدون راهنما (ب) یادگیری باراهنما |
| ۴۶..... | شکل ۵-۳: نمایش الگوریتم‌های تراکمی (الف) روش پیوند-کامل (ب) روش تک-پیوندی |
| ۴۹..... | شکل ۶-۳: دسته‌بندی نمونه‌ها در فضای دو بعدی |
| ۵۰..... | شکل ۷-۳: درخت تصمیم‌گیری ساده، با آزمایش بر روی ویژگی‌های X و Y |
| ۵۸..... | شکل ۸-۳: نمای کلی الگوریتم ژنتیک |
| ۶۵..... | شکل ۹-۳: الگوریتم Apriori |
| ۶۷..... | شکل ۱۰-۳: مراحل اجرای الگوریتم Y-means |
| ۷۳..... | شکل ۱-۴: معماری سیستم‌های تشخیص نفوذ توسط حسگرهای شبکه |
| ۹۰..... | شکل ۱-۵: توابع عضویت برای مجموعه‌های فازی |
| ۹۶..... | شکل ۲-۵: دیاگرام نحوه انجام کار سیستم تشخیص نفوذ پیشنهادی |
| ۱۰۱..... | شکل ۱-۶: روند کلی سیستم تشخیص نفوذ پیشنهادی |
| ۱۰۴..... | شکل ۲-۶: ماتریس پراکندگی |

فهرست جداول

| صفحه | عنوان |
|----------|--|
| ۸۴..... | جدول ۴-۱: دسته‌بندی انواع حملات |
| ۸۵..... | جدول ۴-۲: ویژگی‌های اصلی اتصالات TCP |
| ۸۵..... | جدول ۴-۳: ویژگی‌های اتصال در یک اتصال پیشنهاد شده بوسیله Domain Knowledge |
| ۸۶..... | جدول ۴-۴: ویژگی‌های ترافیک در ۲ ثانیه محاسبه شده است |
| ۸۷..... | جدول ۴-۵: کارهای انجام شده در زمینه تشخیص نفوذ با داده‌کاوی |
| ۹۹..... | جدول ۶-۱: حملات موجود در پایگاه داده و دسته‌بندی‌های مرتبط به آن |
| ۱۰۰..... | جدول ۶-۲: توزیع کلاس‌ها در ۱۰٪ از مجموعه داده |
| ۱۰۰..... | جدول ۶-۳: توزیع کلاس‌های مختلف در داده آموزشی و آزمایشی |
| ۱۰۲..... | جدول ۶-۴: مقداردهی پارامترهای اولیه در الگوریتم ژنتیک |
| ۱۰۵..... | جدول ۶-۵: نتایج مقایسه الگوریتم‌های داده‌کاوی با مدل پیشنهادی |
| ۱۰۸..... | جدول ۶-۶: فراخوانی، دقت و F-measure بدست آمده از الگوریتم‌های دسته‌کننده مختلف |

فهرست نمودارها

| صفحه | عنوان |
|----------|--|
| ۱۰۶..... | نمودار ۱-۶: مقایسه نرخ تشخیص نفوذ..... |
| ۱۰۷..... | نمودار ۲-۶: مقایسه نرخ هشدار نادرست..... |
| ۱۰۸..... | نمودار ۳-۶: مقدار فراخوانی، دقت و F-measure برای داده‌های نرمال در الگوریتم‌های دسته‌بندی..... |
| ۱۰۹..... | نمودار ۴-۶: مقدار فراخوانی، دقت و F-measure برای داده‌های حمله در الگوریتم‌های دسته‌بندی..... |

فصل اول:

کلیات

۱-۱- مقدمه

با رشد شبکه‌های کامپیوتری، امنیت شبکه‌های کامپیوتری از اهمیت بالایی برخوردار می‌شود. نفوذ، مجموعه اقدامات غیرقانونی است که صحت، محرمانگی و دسترسی به منبع را به خطر می‌اندازد [۱]. نفوذگران را می‌توان به دو دسته نفوذگران داخلی و خارجی دسته‌بندی کرد. نفوذگران داخلی کسانی هستند که برای دستیابی به سیستم اختیارات محدودی دارند، اما سعی دارند به منابعی که اجازه دسترسی به آن را ندارند دست پیدا کنند و نفوذگران خارجی کسانی هستند که اجازه استفاده از سیستم را ندارند، ولی سعی دارند سیستم را مورد دسترسی قرار دهند [۲].

از آنجایی که از نظر تکنیکی ایجاد سیستم‌های کامپیوتری بدون نقاط ضعف و شکست امنیتی عملاً غیرممکن است؛ تشخیص نفوذ در تحقیقات سیستم‌های کامپیوتری با اهمیت خاصی دنبال می‌شود. سیستم‌های تشخیص نفوذ، می‌توانند انواع نفوذ روی شبکه‌ها را که می‌تواند شامل جمع‌آوری اطلاعات، پویش پورت‌ها، بدست آوردن کنترل کامپیوترها و هک کردن آن‌ها باشد را شناسایی کنند.

۱-۲- بیان مسئله و پیشینه تحقیق

سیستم تشخیص نفوذ یک سیستم محافظتی است که خرابکاری‌های در حال وقوع روی شبکه را شناسایی می‌کند. عموماً سیستم‌های تشخیص نفوذ در کنار دیوارهای آتش^۱ و به صورت مکمل امنیتی برای آن‌ها مورد استفاده قرار می‌گیرند [۳]. این سیستم‌ها سعی دارند نفوذهای غیر مجاز به شبکه را با توجه به الگوریتم‌های خاص تشخیص دهند، که می‌توان آن‌ها را به دو دسته کلی تشخیص سوء-استفاده^۲ و تشخیص رفتار غیرمتعارف^۴ تقسیم کرد. سیستم‌های تشخیص موارد سوءاستفاده تلاش می‌کنند حمله‌ها را با استفاده از کشف الگوهای نفوذ که توسط خبرگان تشخیص داده شده و گزارش می‌شوند شناسایی کنند. رویکرد تشخیص موارد غیر متعارف در واقع توسعه رویکرد قبلی است با این توضیح که در این رویکرد، الگوهایی از رفتارهای نرمال در شبکه از قبل، تشخیص داده شده است و نفوذ می‌تواند مبتنی بر مقداری انحراف از رفتارهای نرمال در شبکه تعریف شود.

بدلیل اهمیت امنیت در شبکه‌های کامپیوتری از روش‌های زیادی برای تشخیص نفوذ استفاده شده

¹ Intrusion Detection System (IDS)

² Firewall

³ Misuse Detection

⁴ Anomaly Detection

است، از جمله این روش‌ها استفاده از الگوریتم‌های داده‌کاوی می‌باشد. در سیستم‌های تشخیص نفوذ نرم افزارهای مبتنی بر الگو، حسگرهای ترافیک شبکه را بررسی می‌کنند و الگوهایی را هم ذخیره می‌کنند و سپس هشدارها^۱ را فعال می‌سازند و در صورتی که رخدادی در سیستم اتفاق بیفتد، مأمور امنیتی را آگاه می‌سازند. وقتی یک شبکه بسیار بزرگ و پیچیده باشد، تعداد هشدارها زیاد می‌شود و بنابراین حملات هم بیشتر می‌شوند و حسگرها نیز ممکن است الگوها را درست تشخیص ندهند. این می‌تواند دلیلی برای بکارگیری داده‌کاوی باشد [۵۴]. داده‌کاوی فرآیند^۲ کشف مدل‌های مختلف، خلاصه‌ها و مقادیر کسب شده از مجموعه داده می‌باشد. داده‌کاوی یکی از تکنولوژی‌های کاربردی برای تشخیص نفوذ است که به ابداع یک الگوی جدید از داده‌های شبکه‌های عظیم می‌پردازد. در حال حاضر بسیاری از محققان بر روی سیستم‌های تشخیص نفوذ براساس تکنیک‌های داده‌کاوی متمرکز شده‌اند. داده‌کاوی از تکنیک‌های مختلفی مانند تکنیک‌های آماری و یادگیری ماشین استفاده می‌کند.

وجود مسائل پیچیده علمی منجر می‌شود تا به سراغ روش‌های بهینه‌سازی رفته و مسئله مورد نظر را به وسیله آن‌ها حل کرد. با توجه به زمانبر بودن و پیچیدگی روش‌های دقیق از رویکرد بهینه‌سازی هوشمند استفاده می‌شود. بهینه‌سازی، تغییر دادن ورودی‌ها و خصوصیات یک دستگاه، فرآیند ریاضی و یا آزمایش تجربی است به طوری که بهترین نتیجه حاصل شود. در تحقیقاتی که در سال‌های اخیر در زمینه تشخیص نفوذ انجام گرفته، سعی شده تا با سرعت و دقت بیشتر نفوذهای انجام شده به شبکه شناسایی شود. از اینرو محققان از مجموعه داده استاندارد KDD [۶]، برای انجام آزمایشات استفاده کرده‌اند. استفاده از الگوریتم‌های ترکیبی، تکنیک‌های فازی، شبکه‌های عصبی، الگوریتم‌های ژنتیک و غیره از جمله کارهایی است که به منظور تشخیص نفوذ به شبکه انجام شده است.

Wang و همکارانش [۷] از شبکه‌های عصبی مصنوعی^۳ و خوشه‌بندی فازی برای تشخیص نفوذ استفاده کردند. در این روش ابتدا از تکنیک‌های خوشه‌بندی فازی برای تولید زیرمجموعه‌های آموزشی مختلف استفاده می‌شود. براساس زیرمجموعه‌های آموزشی مختلف مدل‌های شبکه عصبی برای فرموله کردن مدل‌های مختلف پایه آموزش می‌بینند. در نهایت رویه تجمیع فازی، برای تجمیع این نتایج بکار برده می‌شود.

¹ Alarm

² Process

³ Artificial Neural Networks (ANN)

Muniyandi و همکاران [۸] از ترکیب الگوریتم خوشه‌بندی K-mean و الگوریتم دسته‌بندی C4.5 برای تشخیص رفتار غیرعادی استفاده کردند. در این روش ابتدا از K-mean برای بخش‌بندی نمونه‌های آزمایش استفاده شده است و سپس درخت تصمیم در هر خوشه مرزهای تصمیم‌گیری را تصحیح می‌کند.

Fores و همکاران [۹]، از رویکرد داده‌کاوی برای استخراج الگوهایی که رفتار نرمال را برای تشخیص نفوذ نشان می‌دهد، استفاده کردند. آن‌ها مجموعه‌ای از قوانین پیوندی فازی را بکار بردند که از داده‌بازبینی شبکه به‌عنوان مدل‌های رفتار نرمال استخراج می‌شوند. همچنین برای کشف رفتارهای غیر نرمال قوانین پیوندی را با هم ترکیب کردند و شباهت آن را با مجموعه‌های استخراج شده از داده نرمال محاسبه کردند.

Jian-hua و همکارش [۱۰] از الگوریتم ژنتیک برای بهبود وزن‌ها و حد‌آستانه شبکه‌های عصبی استفاده کردند. آن‌ها از شبکه‌های عصبی چندلایه BP برای دسته‌بندی داده‌های نرمال و حمله در زمینه تشخیص نفوذ استفاده کردند. وزن‌های اولیه و حد‌آستانه در این شبکه‌ها بصورت تصادفی انتخاب می‌شوند. آن‌ها برای انتخاب بهترین آستانه و وزن برای بهبود نتایج از الگوریتم ژنتیک استفاده کردند. این روش مدل شبکه عصبی BP را سرعت می‌بخشد و نرخ کشف نفوذ را بالا می‌برد.

۱-۳- چالش‌ها و اهداف تحقیق

با توجه به اینکه در سیستم‌های تشخیص نفوذ دو معیار دقت در تشخیص نفوذ به شبکه‌های کامپیوتری و همچنین کاهش تعداد هشدارهای نادرست از اهمیت زیادی برخوردار است، در این تحقیق سعی شده است تا با ارائه روش جدید مبتنی بر دسته‌بندی و الگوریتم‌های تکاملی نرخ تشخیص نفوذ را افزایش دهیم و کمترین میزان هشدارهای نادرست را داشته باشیم.

هدف از این تحقیق آشنایی با روش‌های تشخیص نفوذ، بررسی سیستم‌های تشخیص نفوذ موجود، بررسی روش‌های مختلف داده‌کاوی در تشخیص نفوذ و در نهایت هدف کلی ارائه روشی به منظور تشخیص نفوذ به شبکه با استفاده از تکنیک‌های داده‌کاوی جهت افزایش دقت و صحت تشخیص می‌باشد. در طرح پیشنهادی برای پیاده‌سازی سیستم تشخیص نفوذ از روش دسته‌بندی مبتنی بر قانون فازی استفاده شده است. علاوه بر آن، این طرح برای یافتن وزن‌های بهینه قوانین از الگوریتم ژنتیک بهره می‌برد.

۴-۱- مروری بر فصول پایان نامه

این پایان نامه مشتمل بر شش فصل می‌باشد. در فصل دوم سیستم‌های تشخیص نفوذ توضیح داده شده و روش‌های استفاده شده برای تشخیص نفوذ ذکر شده است. همچنین برخی از سیستم‌های تشخیص نفوذ موجود معرفی شده است.

در فصل سوم مفاهیم داده کاوی و تکنیک‌ها و الگوریتم‌های مختلف آن بررسی شده است. در این فصل سعی شده است تمامی موارد مربوط به داده کاوی به‌طور خلاصه پوشش داده شود.

در فصل چهارم ارتباط داده کاوی و سیستم‌های تشخیص نفوذ بررسی شده است و سعی شده است گام‌های انجام یک فرآیند داده کاوی به منظور تشخیص نفوذ توضیح داده شود. در ادامه این فصل مجموعه داده استاندارد استفاده شده به همراه ویژگی‌های آن معرفی شده است. همچنین تکنیک‌های داده کاوی مورد استفاده در تشخیص نفوذ بررسی شده و کارهای انجام گرفته در این زمینه معرفی شده است.

در فصل پنجم ابتدا مدل دسته‌بندی مبتنی بر قانون فازی توضیح داده شده و در ادامه روش پیشنهادی به‌منظور بهبود کارایی قوانین ارائه شده است.

در فصل ششم گام‌های پیاده‌سازی روش پیشنهادی تشریح شده و در ادامه نتایج بدست آمده با کارهای قبلی مقایسه شده است.

در فصل هفتم نتیجه‌گیری و پیشنهادات برای کارهای آینده ارائه شده است.

فصل دوم:

مفاهیم کلی درباره سیستم‌های تشخیص نفوذ