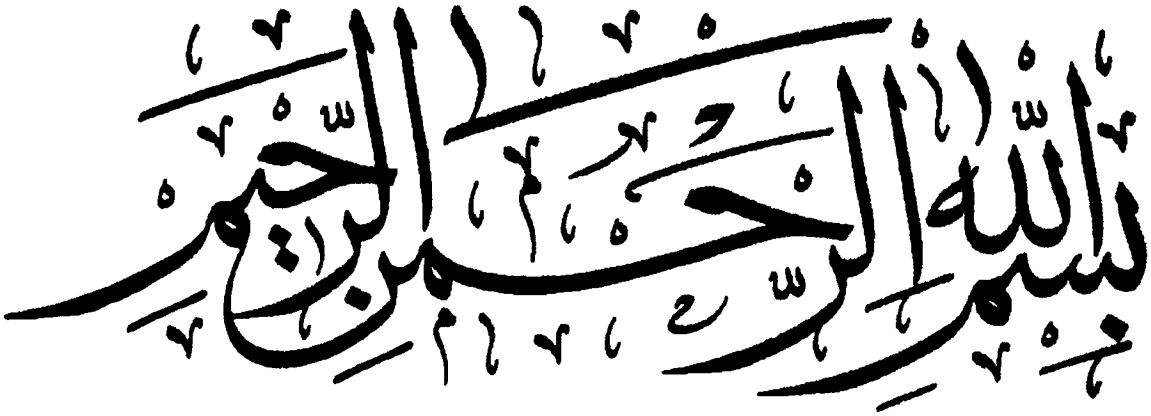

١٤٤٣هـ

دانشگاه شهید بهشتی
دانشکده مهندسی برق و کامپیوتر

عنوان پایان نامه

شناسایی نفوذگر بر مبنای رفتار غیر متعارف با استفاده از روشهای داده‌کاوی و روشهای ترکیبی یادگیری ماشین

پایان نامه کارشناسی ارشد مهندسی کامپیوتر
گرایش هوش مصنوعی

استاد راهنما:
جناب آقای دکتر مقصود عباسپور

توسط:
فرزانه گرامی‌راز

تابستان ۱۳۸۹

پایان نامه کارشناسی ارشد مهندسی کامپیوتر- گرایش هوش‌مصنوعی

تحت عنوان:

شناسایی نفوذگر بر مبنای رفتار غیر متعارف با استفاده از روشهای داده‌کاوی و روشهای ترکیبی یادگیری ماشین

در تاریخ ۱۳۸۹/۶/۲۴ پایان نامه دانشجو، فرزانه گرامی‌راز، توسط کمیته تخصصی داوران مورد بررسی و تصویب نهائی قرار گرفت.

۱- استاد راهنما اول:	جناب آقای دکتر مقصود عباسپور	امضاء
۲-استاد داور (داخلی)	جناب آقای دکتر فرشاد صفایی	امضاء
۵- استاد داور (خارجی)	جناب آقای دکتر احمد خونساری	امضاء
۶- نماینده تحصیلات تکمیلی	جناب آقای دکتر اسلام ناظمی	امضاء

تشکر و قدردانی

ستایش و سپاس خداوند را، آنکه پیوند دهنده‌ی ستایش است به نعمتها و پیوند دهنده‌ی نعمتهاست به سپاس. اکنون که به یاری ایزد یکتا توفیق تکمیل این رساله تحقیقاتی را یافته‌ام، بر خود لازم می‌دانم از زحمات و راهنمائیهای جناب آقای دکتر مقصود عباسپور-استاد راهنمای پروژه- که در تمام مدت انجام پروژه صبورانه و دلسوزانه در کنارم بودند کمال تقدیر و تشکر را به عمل آورم.

نام ونام خانوادگی: فرزانه گرامی‌راز

عنوان پایان نامه: شناسایی نفوذگر بر مبنای رفتار غیر متعارف با استفاده از روشهای داده‌کاوی و روشهای ترکیبی یادگیری ماشین

استاد/اساتید راهنما: جناب آقای دکتر مقصود عباسپور

نام ونام خانوادگی دانشجو: **فرزانه گرامی‌راز**

امضاء وتاریخ:

تقدیم به آنان که می‌بینند، می‌شنوند و در راه اهداف و اندیشه‌هایِ نیکشان تا پایِ نتیجه پای‌بندند.

تقدیم به پدر و مادر عزیزم.

فهرست مطالب:

فهرست جداول

فهرست شکلها:

واژه‌نامه

نمایه نرمال	Normal Profile
سیستمهای شناسایی نفوذ	Intrusion Detection System
نفوذ/حمله	Intrusion
الگوی حملات شناخته شده	Known Attack Patterns
اداره استخبارات فدرال ایالات متحده امر یکا	FBI
ناهنجاری/رفتار غیر متعارف	Anomay
شناسایی نفوذگر بر مبنای تشخیص ناهنجاری	Anomay-Based Intrusion Detection
وفقی	adaptive
محرمانگی	Confidentiality
در دسترس بودن	Availability
جامعیت	Integrity
مبتنی بر الگو	Signature-Based
شخصی کردن	Customize
رخنه‌های نفوذی	Vulnerable
مدل سازی بر اساس قوانین فازی	Fuzzy Rule-Based Modeling
FCM	Fuzzy C-Mean Clustering
درصد اعتماد به پیش بینی	Prediction Confidence Ratio
میزان کردن	Tune
میزان کننده مدل	Model Tuner
استلفو	Stolfo
لی	Lee
میزبان یکسان	Same Host
قطعات	Fragments
فوری	Urget
داغ	Hot
مصالحه	Compromised
پوسته ریشه	Root Shell
ریشه	Root
اعلان پوسته	Shell Prompt
تولایی	Tavallaee
تشخیص درست	SuccessfulPrediction
آندرسن	Anderson
دنینگ	Denning
اکسلسون	Axelsson
جمع آوری اطلاعات بازرسی	Audit data Collection
نگهدارنده اطلاعات بازرسی	Audit data storage
سوء استفاده	Misuse Detection
مثبت کاذب	False Positive
منفی کاذب	False Negative
منفی درست	True Negative
مثبت درست	True Positie
براساس شبکه	Network Based

پیگیری	Ttrace
مبتنی بر تک دستگاه	Host Based
ایستا	Static
بازخورد	FeedBack
معیار میزان شدت فعالیت	Activity Intensity Measure
معیار توزیع رکوردهای بازرسی	Audit record distribution measure
وصفی	Ordinal
غیر برخط/آفلاین	Offline
بلادرنگ	Real-Time
موسسه تحقیقاتی استنفورد	Stanford Research Institute(SRI)
سیستم موتور آماری تشخیص ناهنجاری در بسته-ها	Statistical Packet Anomaly Detection Engine(SPADE)
امتیاز ناهنجاری	Anomaly Score
پویش دروازه	Port Scan
فورست	Forrest
جدول مراجعه ای	Lookup Table
هافمیر	Hofmeyr
اسکین	Eskin
والدز	Valdes
شبکه بیزین ساده	Naïve Bayesian Netwok
	Principle Component Analysis(PCA)
شیو	Shyu
ماهالانبیس	Mahalanobis
یه	Ye
حداکثرکردن امید	Expectation Maximization(EM)
یونگ	Yeung
دستورهای پوسته‌ای	Shell Command
تولید قوانین استقرایی	Rule Generation Techniques Inductive
بدون سرپرست	Unsupervised
دیکرسون	Dickerson
FIRE	Fuzzy Intrusion Recognition Engine
راماداس	Ramadas
ANDSOM	Anomalous Network-Traffic Detection with Self Organizing Maps
SOM	Self-Organizing Map
SVM	Support Vector Machine
عنصر خارجی	Outlier Detection
MINDS	Minnesota Intrusion Detection System
یادگیری قوانین انجمنی	Association rule discovery
اقلام	Items
باربارا	Barbara´
ADAM	Audit Data Analysis and Mining

سیستم شناساگر نفوذ با قابلیت به روز رسانی اتوماتیک	An Adaptive Automatically Tuning Intrusion Detection System
یو	Yu
اسلیپر	SLIPPER
ممانعت از سرویس	DOS
چهارچوبی برای شناساگر نفوذ وفقی بر اساس بردارهای پشتیبانیِ توصیف داده	A Framework for Adaptive Anomaly Detection Based on Support Vector Data Description
یانگ	Yang
ابرکره	Hypersphere
شناساگر نفوذی وفقی بر اساس خوشه بندی و بر مبنای روش هسته	An Adaptive Intrusion Detection Algorithm Based on Clustering and Kernel-Method
عددی	Numeric
نمادین	Symbolic
نرخ یادگیری	Learning Rate
بردار مفهوم	Concept Vector
استفاده از تشدید تطبیقی فازی در شناسایی ناهنجاری وفقیِ شبکه	Investigation of Fuzzy Adaptive Resonance Theory in Network Anomaly Intrusion Detection
چارچوبی برای تشخیص ناهنجاری وفقی با استفاده از داده‌کاوی فازی	Detection System A Framework for an Adaptive Anomaly with Fuzzy Data Mining
ژیانگ	Xiang
یادگیری سیستم شناساگر نفوذ با استفاده از الگوریتم بیزینِ وفقی	Learning Intrusion Detection Based on Adaptive Bayesian Algorithm
شناساگر بلادرنگ نفوذی با استفاده از روش داده-کاوی	Real time data mining-based intrusion detection
چارچوبی برای تشخیص نفوذ با استفاده از شبکه بیزین	A Framework for an Adaptive Intrusion Detection System using Bayesian Network
جمیلی	Jemili
ذقدود	Zaghdoud
بن‌احمد	Ben Ahmed
مدل ترکیبی افزایشی با استفاده‌ی گروهی از کلاس-بندهای ضعیف	Incremental Hybrid Intrusion Detection Using Ensemble of Weak Classifiers
یادگیرهای ضعیف	Weak Learner
سیستم شناساگر نفوذ وفقی با استفاده از تکامل اتصالات سیستمی	Adaptive anomaly detection with evolving connectionist systems
لی‌هوآ	Liao
بر خط	Online
بردارهای وزن داری	Weighted Vector
سامانه تطبیقی یادگیری امضاء با استفاده از الگوریتم ژنتیک در تشخیص نفوذ	An adaptive genetic-based signature learning system for intrusion detection
شفیی	Shafi
ویژگی عملیاتی دریافت کننده	Receiver Operating Characteristic
اکسلسون	Axelsson
مولدِ مدلِ تشخیص	Detection Model Generator
خوشه‌بندی کاهشی	Subtractive Clustering

سبک	Style
میشیگان	Michigan
پیتزبرگ	Pittsburgh
کوچکترین ماکزیمم	Smallest Of Maximom
مرتبه زمانی	Order

چکیده:

به نظر می‌رسد استفاده از روشهای سابق از جمله استفاده از دیوارهای آتش و سیستم‌های تشخیص نفوذ مبتنی بر امضا به تنهایی قادر به تأمین امنیت شبکه نیستند، در نتیجه صرف هزینه‌های بیشتر برای تأمین امنیت غیر قابل انکار است. یکی از این هزینه‌ها می‌تواند تشخیص نفوذ بر اساس تشخیص رفتار غیرمتعارف(ناهنجاری) باشد. در این روشها ابتدا نمایه نرمال [1]سیستم مدل شده و از این مدل جهت شناسایی هر گونه رفتار مشکوک استفاده می‌گردد. روشهای مبتنی بر تشخیص ناهنجاری بر خلاف روش‌های سنتی می‌توانند حملات جدید را نیز تشخیص دهند اما تعداد زیاد هشدارهای کاذب مهمترین ضعف آن است، علاوه بر این، ساخت نمایه نرمال و به‌روز نگه داشتن آن از دیگر چالشهای این روش است.

در معماری ارائه شده از مدل سازی مبتنی بر قوانین فازی جهت مدل کردن رفتار سیستم استفاده شده است. مدل‌سازی مبتنی بر قوانین فازی تلاش می‌کند خروجی سیستم بر اساس ورودیهای آن را با استفاده از قوانین فازی مدل کند. چگونگی به‌دست‌آوردن قوانین و مجموعه‌های فازیِ متغیرهای ورودی از مشکلات اصلی این نوع روش مدل-سازی است. الگوریتم ژنتیک برای پیدا کردن قوانین مدل و FCM[2] برای پیدا کردن مجموعه‌های فازی متغیرهای ورودی استفاده شده است. برای هر یک از قوانین فازی آموزش دیده، درجه اعتماد به پیش بینی در نظر گرفته شده که در حقیقت میزان اطمینان سیستم به آن قانون محسوب می‌شود. این پارامتر نسبت نمونه‌های درست تشخیص داده شده به کل نمونه‌های آموزشی است.

با توجه به تغییر در رفتار نرمال شبکه و وقوع حملات جدید، استفاده از مدلهای غیرانطباقی مناسب نیست و تلاش برای به‌روزرسانی مدل غیر قابل انکار است. در روش ارائه شده، درجه اعتماد هر یک از قوانین با توجه به عملکردشان در طول فاز تست و با استفاده از یک کنترل‌کننده فازی به‌روز رسانده می‌شوند. با استفاده از مدل غیرانطباقی، دقت حدود ۵۵ درصد عاید ما شد، در حالی که استفاده از روش انطباقی این دقت را تا ۷۵ درصد افزایش داد.

نگاه ساده به مسئله به‌روز رسانی مدل تشخیص، به‌روز رسانی مدل با استفاده از پارامترهای کم اما مؤثر، تفاوت محسوس در دقت در مقایسه با روش‌های غیرانطباقی و به روز رسانی تقریباً آنلاین از مهم‌ترین مزایای سیستم انطباقی پیشنهادی هستند.

کلمات کلیدی: *تشخیص تطبیقیِ نفوذ بر مبنای تشخیص ناهنجاری، مدل‌سازی مبتنی بر قوانین فازی، کنترل کننده فازی*

[1] Normal Profile
[2] Fuzzy C-Mean Clustering

فصل اول:

معرفی پروژه