دانشگاه تربیت مدرس
دانشکده‌ی مهندسی برق و کامپیوتر

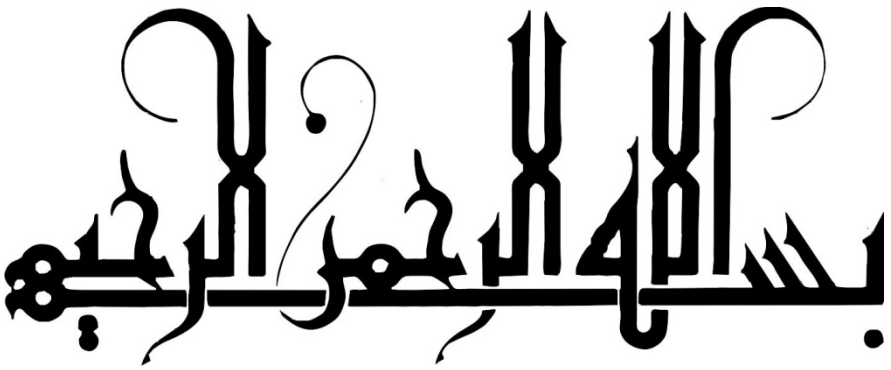
پایان‌نامه‌ی دوره‌ی کارشناسی ارشد مهندسی کامپیوتر- نرم افزار

تشخیص ناهنجاری پویا در شبکه‌های اقتضایی متحرک

میثم علیخانی

استاد راهنما:
دکتر مهدی آبادی

اسفند ۱۳۸۹



بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از پایان نامه کارشناسی ارشد

آقای میثم **علیخانی** پایان نامه ۹ واحدی خود را با عنوان **تشخیص ناهنجاری پویا در شبکه های اقتضایی متحرك** در تاریخ ۱۳۸۹/۱۲/۲۱ ارائه کردند.

اعضای هیات داوران نسخه نهایی این پایان نامه را از نظر فرم و محتوا تایید کرده، پذیرش آنرا برای اخذ درجه کارشناسی ارشد مهندسی کامپیوتر-نرم افزار پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر مهدی آبادی	**استادیار**	
استاد مشاور	دکتر سعید جلیلی	**دانشیار**	
استاد ناظر	دکتر بهزاد اکبری	**استادیار**	
استاد ناظر	دکتر رسول جلیلی	**دانشیار**	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر بهزاد اکبری	**استادیار**	

آیین‌نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

نظر به اینکه چاپ و انتشار پایان‌نامه (رساله)های تحصیلی دانشجویان دانشگاه تربیت مدرس، مبین بخشی از فعالیت‌های علمی - پژوهشی دانشگاه است بنابراین، به منظور آگاهی و رعایت حقوق دانشگاه، دانش‌آموختگان این دانشگاه نسبت به رعایت موارد ذیل متعهد می‌شوند:

ماده ۱: در صورت اقدام به چاپ پایان‌نامه (رساله)ی خود، مراتب را قبلاً به طور کتبی به «دفتر نشر آثار علمی» دانشگاه اطلاع دهد.

ماده ۲: در صفحه سوم کتاب (پس از برگ شناسنامه) عبارت ذیل را چاپ کند:

«کتاب حاضر، حاصل پایان‌نامه کارشناسی ارشد/ رساله دکتری نگارنده در رشته مهندسی کامپیوتر - نرم‌افزار است که در سال ۱۳۸۹ در دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر مهدی آبادی، مشاوره جناب آقای دکتر سعید جلیلی از آن دفاع شده است.»

ماده ۳: به منظور جبران بخشی از هزینه‌های انتشارات دانشگاه، تعداد یک درصد شمارگان کتاب (در هر نوبت چاپ) را به «دفتر نشر آثار علمی» دانشگاه اهدا کند. دانشگاه می‌تواند مازاد نیاز خود را به نفع مرکز نشر در معرض فروش قرار دهد.

ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می‌کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می‌تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند، به علاوه به دانشگاه حق می‌دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتاب‌های عرضه شده نگارنده برای فروش، تامین نماید.

ماده ۶: اینجانب میثم علیخانی دانشجوی رشته مهندسی کامپیوتر - نرم‌افزار مقطع کارشناسی ارشد تعهد فوق و ضمانت اجرایی آن را قبول کرده، به آن ملتزم می‌شوم.

نام و نام خانوادگی:

تاریخ و امضا:

آیین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش‌های علمی دانشگاه تربیت مدرس

مقدمه: با عنایت به سیاست‌های پژوهشی و فناوری دانشگاه در راستای تحقق عدالت و کرامت انسان‌ها که لازمه شکوفایی علمی و فنی است و رعایت حقوق مادی و معنوی دانشگاه و پژوهشگران، لازم است اعضای هیأت علمی، دانشجویان، دانش‌آموختگان و دیگر همکاران طرح، در مورد نتایج پژوهش‌های علمی که تحت عناوین پایان‌نامه، رساله و طرح‌های تحقیقاتی با هماهنگی دانشگاه انجام شده است، موارد زیر را رعایت نمایند:

ماده ۱- حق نشر و تکثیر پایان‌نامه/ رساله و درآمدهای حاصل از آن‌ها متعلق به دانشگاه می‌باشد ولی حقوق معنوی پدید آورندگان محفوظ خواهد بود.

ماده ۲- انتشار مقاله یا مقالات مستخرج از پایان‌نامه/ رساله به صورت چاپ در نشریات علمی و یا ارائه در مجامع علمی باید به نام دانشگاه بوده و با تایید استاد راهنمای اصلی، یکی از اساتید راهنما، مشاور و یا دانشجو مسئول مکاتبات مقاله باشد. ولی مسئولیت علمی مقاله مستخرج از پایان‌نامه و رساله به عهده اساتید راهنما و دانشجو می‌باشد.

تبصره: در مقالاتی که پس از دانش‌آموختگی بصورت ترکیبی از اطلاعات جدید و نتایج حاصل از پایان‌نامه/ رساله نیز منتشر می‌شود نیز باید نام دانشگاه درج شود.

ماده ۳- انتشار کتاب، نرم افزار و یا آثار ویژه (اثری هنری مانند فیلم، عکس، نقاشی و نمایشنامه) حاصل از نتایج پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی کلیه واحدهای دانشگاه اعم از دانشکده‌ها، مراکز تحقیقاتی، پژوهشکده‌ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس آئین نامه‌های مصوب انجام شود.

ماده ۴- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته‌ها در جشنواره‌های ملی، منطقه‌ای و بین‌المللی که حاصل نتایج مستخرج از پایان‌نامه/ رساله و تمامی طرح‌های تحقیقاتی دانشگاه باید با هماهنگی استاد راهنما یا مجری طرح از طریق معاونت پژوهشی دانشگاه انجام گیرد.

ماده ۵- این آیین‌نامه در ۵ ماده و یک تبصره در تاریخ۸۷/۴/۱ در شورای پژوهشی و در تاریخ ۸۷/۴/۲۳ در هیأت رئیسه دانشگاه به تایید رسید و در جلسه مورخ ۸۷/۷/۱۵ شورای دانشگاه به تصویب رسیده و از تاریخ تصویب در شورای دانشگاه لازم‌الاجرا است.

«اینجانب میثم علیخانی دانشجوی رشته مهندسی کامپیوتر - نرم‌افزار ورودی سال تحصیلی ۱۳۸۷ مقطع کارشناسی ارشد دانشکده مهندسی برق و کامپیوتر. متعهد می‌شوم کلیه نکات مندرج در آئین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش‌های علمی دانشگاه تربیت مدرس را در انتشار یافته‌های علمی مستخرج از پایان‌نامه/ رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد آئین‌نامه فوق‌الاشعار به دانشگاه وکالت و نمایندگی می‌دهم که از طرف اینجانب نسبت به لغو امتیاز اختراع بنام بنده و یا هر گونه امتیاز دیگر و تغییر آن به نام دانشگاه اقدام نماید. ضمناً نسبت به جبران فوری ضرر و زیان حاصله بر اساس برآورد دانشگاه اقدام خواهم نمود و بدینوسیله حق هر گونه اعتراض را از خود سلب نمودم»

نام و نام خانوادگی:

تاریخ و امضا

دانشگاه تربیت مدرس

دانشگاه تربیت مدرس

دانشکده‌ی مهندسی برق و کامپیوتر

پایان‌نامه‌ی دوره‌ی کارشناسی ارشد مهندسی کامپیوتر- نرم افزار

تشخیص ناهنجاری پویا در شبکه‌های اقتضایی متحرک

میثم علیخانی

استاد راهنما:

دکتر مهدی آبادی

استاد مشاور:

دکتر سعید جلیلی

اسفند ۱۳۸۹

چکیده

امروزه، رشد روزافزون فناوری بی‌سیم در دنیای اطلاعات و ارتباطات باعث به وجود آمدن زمینه‌های مختلفی در عرصه شبکه‌های ارتباطی شده است. یکی از این زمینه‌ها، شبکه‌های اقتضایی متحرک (MANETs) است. هر شبکه اقتضایی متحرک مجموعه‌ای از گره‌های خودمختار بی‌سیم است که در آن هیچ گونه زیرساخت ثابتی وجود ندارد. در شبکه‌های اقتضایی متحرک، تحرک شدید گره‌ها باعث تغییر مداوم همبندی شبکه می‌شود. این ویژگی‌های ذاتی باعث افزایش آسیب‌پذیری شبکه‌های اقتضایی متحرک در مقایسه با سایر شبکه‌ها می‌شوند. امروزه، سیستم‌های تشخیص نفوذ به عنوان یک ابزار دفاعی، از شبکه‌ها و سیستم‌ها در برابر حملات و نفوذها حفاظت می‌کنند. از آن‌جایی که همبندی شبکه در شبکه‌های اقتضایی متحرک همواره در حال تغییر است، در نتیجه رفتار شبکه به صورت پویا تغییر می‌کند. به این دلیل، استفاده از یک نمای عادی از پیش تعریف شده نمی‌تواند حالت جاری شبکه را به خوبی توصیف کند. در این پژوهش، دو روش متفاوت به نام‌های DCAD و IPCAAD برای تشخیص ناهنجاری پویا در شبکه‌های اقتضایی متحرک ارائه شده است. روش‌های پیشنهادی شامل دو مرحله آموزش و تشخیص می‌باشند. در روش DCAD، در مرحله آموزش برای ایجاد و به‌روزرسانی نمای عادی از الگوریتم خوشه‌بندی وزن‌دار WFWC استفاده می‌شود. در مرحله تشخیص، نمای عادی با استفاده از ضرایب وزنی و رابطه فراموشی به صورت متناوب و با توجه با تغییرات همبندی شبکه به‌روزرسانی می‌شود. در روش IPCAAD و نسخه تقریبی آن به نام IAPCAAD، در مرحله آموزش، نمای عادی با استفاده از تحلیل مولفه‌های اصلی ایجاد می‌شود. در مرحله تشخیص، نمای عادی با استفاده از تحلیل مولفه‌های اصلی افزایشی، ضرایب وزنی و رابطه فراموشی به‌روزرسانی می‌شود. برای شبیه‌سازی شبکه‌های اقتضایی متحرک و حملات مسیریابی از ابزار شبیه‌ساز NS2 استفاده شده است. همچنین، کارآیی روش‌های فوق برای تشخیص حملات سیاه‌چاله، سریع، همسایه و ارسال سیل‌آسای بسته‌های RREQ مورد ارزیابی قرار گرفت. هر حمله به صورت مجزا شبیه‌سازی شده و مورد ارزیابی قرار گرفته است. آزمایش‌های انجام شده نشان می‌دهند که به‌روزرسانی نمای عادی باعث افزایش نرخ تشخیص و کاهش نرخ هشدار نادرست روش‌های پیشنهادی می‌شود.

کلمات کلیدی: شبکه اقتضایی متحرک، حملات مسیریابی، تشخیص ناهنجاری، خوشه‌بندی پویا، پروتکل مسیریابی AODV، رابطه فراموشی، به‌روزرسانی نمای عادی، تحلیل مولفه‌های اصلی افزایشی

فهرست مطالب

فصل چهارم: تشخیص ناهنجاری پویا

فهرست جداول

فهرست شکل‌ها

اختصارات

AODV	Ad hoc On demand Distance Vector
CBR	Constant Bite Rate
CTS	Clear To Send
DoS	Denial of Service
DR	Detection Rate
DSDV	Destination-Sequence Distance-Vector
DSR	Dynamic Source Routing
FAR	False Alarm Rate
FDMA	Frequency Division Multiple Access
FSA	Finite State Automaton
FSR	Fisheye State Routing
FTP	File Transfer Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MANET	Mobile Ad hoc NETwork
MPR	Message retransmission List
OLSR	Optimized Link State Routing
PCA	Principal Component Analysis
PDR	Packet Delivery Ratio
QoS	Quality of Service
RERR	Route REPly
RREP	Route REQuest
RREQ	Route ERRor
RTS	Request To Send
RWP	Random WayPoint
SVD	Singular Value Decomposition
SYN	Synchronies
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UDP	User Datagram Protocol
WAN	Wide Area Network

فصل اول

کلیات

۱-۱ مقدمه

امروزه، رشد روزافزون فناوری بی‌سیم در دنیای اطلاعات و ارتباطات باعث به وجود آمدن زمینه‌های مختلفی در عرصه شبکه‌های ارتباطی شده است. یکی از این زمینه‌ها، شبکه‌های اقتضایی متحرک (MANETs[1]) می‌باشد. هر شبکه اقتضایی متحرک مجموعه‌ای از گره‌های خودمختار بی‌سیم است که در آن گره‌ها بدون هیچ زیرساخت ثابتی با یکدیگر به صورت همتا-به-همتا[2] در ارتباط هستند. این شبکه‌ها محیطی را فراهم می‌کنند تا کاربران بتوانند در حین حرکت با یکدیگر ارتباط برقرار کنند. در شبکه‌های اقتضایی متحرک، تحرک گره‌ها باعث تغییر مداوم همبندی شبکه می‌شود. هر گره علاوه بر انجام سرویس‌های مشتری، مسیریابی، هدایت بسته‌ها و عملیات تنظیم شبکه را نیز بر عهده دارد. بنابراین، در این شبکه‌ها مسیریاب مجزایی وجود ندارد و فعالیت‌های هر گره در مقایسه با سایر شبکه‌های بی‌سیم بیشتر است.

امنیت یک چالش مهم در دنیای فناوری اطلاعات و ارتباطات محسوب می‌شود. شبکه‌های اقتضایی متحرک نیز دور از این چالش نیستند و مانند هر شبکه اطلاعاتی، نیازمند فضایی اَمن برای ایجاد ارتباطات و تبادل اطلاعات می‌باشند. امنیت، ترکیبی از فرآیندها، رویه‌ها و سیستم‌ها برای تضمین ویژگی‌های زیر می‌باشد [۱]:

۱. محرمانگی[3]:

محرمانگی تضمین می‌کند که اطلاعات تنها در میان افراد و سیستم‌های مجاز به اشتراک گذاشته می‌شود و از افشای اطلاعات در برابر کاربران غیرمجاز جلوگیری به عمل می‌آید.

[1] Mobile Ad Hoc NETworks
[2] Peer-to-peer
[3] Confidentiality

۲. احراز هویت[1]:
با این روش می‌توان هر گره‌ای (کاربری) را شناسایی کرده و از جعل هویت جلوگیری به عمل آورد. در شبکه‌های سیمی و شبکه‌های بی‌سیمی که دارای زیر ساختار هستند، احراز هویت می‌تواند در مراکزی مانند مسیریاب‌ها، ایستگاه‌های پایه یا نقاط دسترسی انجام گیرد. اما در شبکه‌های اقتضایی متحرک این نقاط متمرکز وجود ندارند و احراز هویت می‌تواند مشکل باشد.

۳. صحت[2]:
صحت تضمین می‌کند که پیام دریافتی با پیام ارسالی کاملاً یکسان بوده و در طی ارسال تغییر داده نشده است.

۴. غیرقابل انکار بودن پیام[3]:
اگر یک موجودیت یک پیام را ارسال کند، نمی‌تواند ارسال آن را انکار کند، چرا که امضای آن موجودیت به آن پیام اضافه شده است.

۵. دسترس‌پذیری[4]:
دسترس‌پذیری اطمینان می‌دهد منابع و سرویس‌های شبکه برای کاربران مجاز در دسترس است.

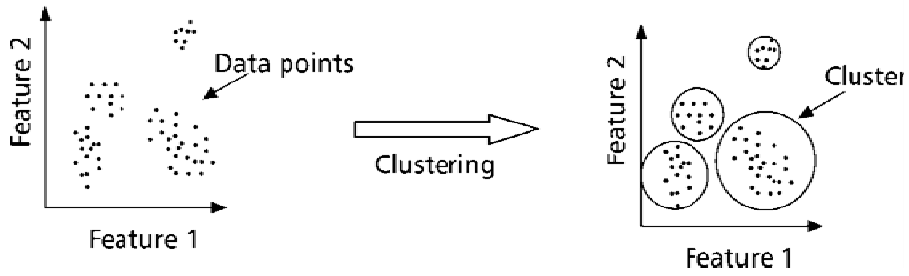
۶. کنترل دسترسی[5]:
کنترل دسترسی تضمین می‌کند که کاربران غیرمجاز از سرویس‌ها و منابع شبکه استفاده نخواهند کرد.

یک سیستم تشخیص نفوذ (IDS[6]) به عنوان یک ابزار امنیتی می‌تواند از ورود و استفاده کاربران غیرمجاز باخبر شده و با ایجاد هشدارهای مناسب مانع از به خطر افتادن سیستم شود. این سیستم‌ها فعالیت‌های خود را به دو روش تشخیص مبتنی بر امضاء[7] و تشخیص ناهنجاری[8] انجام می‌دهند. در روش‌های تشخیص مبتنی بر امضاء، یک سیستم تشخیص نفوذ رفتار جاری شبکه را با الگوهای نفوذهای شناخته شده مقایسه کرده و در صورت انطباق بین آن‌ها نفوذ تشخیص داده می‌شود. در روش‌های تشخیص ناهنجاری، ابتدا یک نما[9] از رفتار عادی شبکه ایجاد می‌شود. سپس، هر رفتاری که از نمای ایجاد شده انحراف داشته باشد به عنوان نفوذ تشخیص داده می‌شود. مزیت اصلی این روش‌ها تشخیص نفوذهای جدید و عیب عمده آن‌ها نرخ هشدار نادرست بالا است.

[1] Authentication
[2] Integrity
[3] Non-repudiation
[4] Availability
[5] Access control
[6] Intrusion Detection System (IDS)
[7] Signature-based detection
[8] Anomaly detection
[9] Profile

روش‌های تشخیص ناهنجاری به دو دسته شبه‌نظارتی[1] و بدون‌نظارت[2] تقسیم می‌شوند [۲]. روش‌های تشخیص ناهنجاری شبه‌نظارتی در مرحله آموزش، نیازمند مجموعه‌ای از داده‌های عادی برای ایجاد نما هستند. در حالی که روش‌های تشخیص ناهنجاری بدون‌نظارت در مرحله آموزش نیازی به داده‌های عادی ندارند. روش‌های بدون‌نظارت برای داده‌ها دو فرض را درنظر می‌گیرند: فرض اول این است که فراوانی داده‌های عادی از داده‌های ناهنجار خیلی بیشتر است و فرض دوم این است که داده‌های عادی از لحاظ آماری متمایز از داده‌های ناهنجار هستند.

خوشه‌بندی در بسیاری از مسائلی که هدف آن‌ها پیدا کردن یک ساختار و مدل از مجموعه‌ی داده‌های بدون برچسب است و در مسائل یادگیری بدون‌نظارت مطرح می‌شود. خوشه‌بندی فرآیندی برای سازماندهی اشیاء در یک گروه است به طوری که اعضای آن گروه بسیار مشابه یکدیگر هستند (شکل ۱-۱). بنابراین، یک خوشه مجموعه‌ای از اشیایی مشابه است به طوری که اعضای آن خوشه با اعضای سایر خوشه‌ها شباهت کمی دارند. تشخیص ناهنجاری یک نمونه از مسائل تشخیص داده‌های پَرت[3] است. داده‌های غیرعادی مانند داده‌های پَرت و دورافتاده از داده‌های عادی مجزا بوده و با استفاده از روش‌های خوشه‌بندی قابل تشخیص هستند.



شکل ۱-۱: فرآیند خوشه‌بندی داده‌ها [۳۷]

تحلیل مولفه‌های اصلی (PCA[4]) به وسیله پرسون در سال ۱۹۰۱ میلادی مطرح شد که هدف اصلی آن استخراج متغیرهای جدید بود به طوری‌که ترکیب خطی از متغیرهای اولیه باشند [۴۰]. تحلیل مولفه‌های اصلی یک روش شناخته شده برای توصیف پراکندگی و تحلیل الگوها در داده‌ها است. با استفاده از تحلیل مولفه‌های اصلی، اولین مولفه اصلی که نشان‌دهنده توزیع تقریبی داده‌ها است محاسبه می‌شود. برای ایجاد نما از داده‌های عادی و تشخیص ناهنجاری می‌توان از اولین مولفه اصلی استفاده کرد.

[1] Semi-supervised
[2] Unsupervised
[3] Outlier detection
[4] Principal Component Analysis

۱-۲ موضوع و اهداف پژوهش

با توجه به ویژگی‌های خاص شبکه‌های اقتضایی متحرک، از قبیل تغییر مداوم همبندی شبکه، تشخیص ناهنجاری در این شبکه‌ها مشکل است. روش‌های تشخیص ناهنجاری را می‌توان به دو دسته ایستا و پویا تقسیم کرد. روش‌های ایستا، در مرحله آموزش یک نما از رفتار عادی شبکه ایجاد کرده و همواره از آن نما بدون هیچ گونه تغییری برای تشخیص ناهنجاری استفاده می‌کنند. این نمای عادی از پیش ایجاد شده ثابت بوده و مبتنی بر تغییرات رفتاری شبکه و در هنگام تشخیص ناهنجاری به‌روزرسانی نمی‌شود. از طرفی، رفتار گره‌ها در شبکه‌های اقتضایی متحرک پویا بوده و این باعث تغییر رفتار شبکه با گذشت زمان می‌شود. به این دلیل، استفاده از یک روش ایستا برای تشخیص ناهنجاری در شبکه‌های اقتضایی متحرک نمی‌تواند خیلی موثر باشد.

در این پژوهش، هدف ارائه روشی پویا برای تشخیص ناهنجاری در شبکه‌های اقتضایی متحرک مبتنی بر پروتکل مسیریابی AODV است، به گونه‌ای که با تغییرات سریع در همبندی و رفتار شبکه سازگار بوده و در عین حال نرخ تشخیص بالا و نرخ هشدار نادرست پایین داشته باشد.

۱-۳ جنبه‌های نوآوری

از آن‌جایی که همبندی در شبکه‌های اقتضایی متحرک همواره در حال تغییر است، در نتیجه رفتار شبکه به صورت پویا تغییر می‌کند. در این پژوهش، دو روش متفاوت به نام‌های DCAD[۱] و IPCAAD[۲] برای تشخیص ناهنجاری در شبکه‌های اقتضایی متحرک ارائه شده است که می‌توانند با تغییرات همبندی و رفتار شبکه به صورت پویا منطبق شوند. روش DCAD یک روش تشخیص ناهنجاری بدون‌نظارت است که در آن از الگوریتم خوشه‌بندی وزن‌دار به نام WFWC[۳] برای ایجاد و به‌روزرسانی نمای عادی استفاده می‌شود. بردارهای داده که متناسب با رفتار و حالت شبکه می‌باشند ضرایبی را به عنوان وزن به خود اختصاص می‌دهند. از این ضرایب و یک رابطه فراموشی هنگام به‌روزرسانی نمای عادی استفاده می‌شود. روش IPCAAD و نسخه تقریبی آن به نام IAPCAAD یک روش تشخیص ناهنجاری شبه‌نظارتی است که در آن از تحلیل مولفه‌های اصلی افزایشی برای ایجاد و به‌روزرسانی نمای عادی استفاده می‌شود.

با توجه به نتایج آزمایش‌های انجام شده مشخص می‌شود که به‌روزرسانی نمای عادی تاثیر قابل ملاحظه‌ای در افزایش نرخ تشخیص و کاهش نرخ هشدار نادرست روش‌های پیشنهادی دارد. این نتایج ناشی از این واقعیت است که نمای عادی با تغییرات رفتاری شبکه -که ناشی از تغییرات همبندی

[1] Dynamic Clustering-based Anomaly Detection
[2] Incremental PCA Anomaly Detection
[3] Weighted Fixed-Width Clustering

است- منطبق شده و توانسته است رفتار فعلی شبکه را خیلی بهتر توصیف کند.

۱-۴ مروری بر فصل‌های آتی

در ادامه در فصل دوم شبکه‌های اقتضایی متحرک معرفی شده و ویژگی‌ها و کاربردهای این شبکه‌ها شرح داده می‌شوند. بدین منظور، ابتدا پشته پروتکلی در مدل TCP/IP که متشکل از پنج لایه کاربرد، انتقال، شبکه، پیوند داده‌ها و فیزیکی است بررسی می‌شود. سپس لایه شبکه که یکی از مهمترین لایه‌ها در این شبکه‌ها بوده و به عنوان یک زمینه پژوهشی مطرح است شرح داده می‌شود. در نهایت، پروتکل‌های مسیریابی در شبکه‌های اقتضایی متحرک به دو دسته پیش‌گستر و واکنشی تقسیم می‌شوند. پروتکل‌های مسیریابی WRP، DSDV، FSR و OLSR به عنوان پروتکل‌های پیش‌گستر و پروتکل‌های مسیریابی AODV و DSR به عنوان پروتکل‌های واکنشی معرفی می‌شوند.

در فصل سوم حملات مختلف در شبکه‌های اقتضایی متحرک معرفی می‌شوند. حملات بر اساس ماهیت‌شان به دو دسته فعال و غیرفعال تقسیم می‌شوند. همچنین، مبتنی بر لایه‌های مختلف در پشته پروتکلی و نحوه عملکرد حمله روی آن لایه دسته‌بندی دیگری برای حملات انجام می‌گیرد. در ادامه، تعدادی از روش‌های موجود برای تشخیص حملات (نفوذ) در شبکه‌های اقتضایی متحرک شرح داده می‌شوند. این روش‌ها به دو دسته تشخیص مبتنی بر امضاء و تشخیص ناهنجاری تقسیم می‌شوند. در نهایت، معماری‌های خوداتکا، توزیع‌شده و سلسله‌مراتبی برای سیستم‌های تشخیص نفوذ معرفی می‌شوند.

در فصل چهارم، ابتدا ویژگی‌های به‌کار رفته برای مدل کردن رفتار پروتکل مسیریابی AODV تعریف می‌شوند. این ویژگی‌ها به چهار دسته ویژگی‌های وابسته به ترافیک داده‌ها در شبکه، ویژگی‌های وابسته به فرآیند کشف مسیر، ویژگی‌های وابسته به انقطاع مسیر و ویژگی وابسته به رفتار خاص پروتکل مسیریابی طبقه‌بندی می‌شوند. سپس، دو روش پیشنهادی به نام‌های DCAD و IPCAAD برای تشخیص ناهنجاری پویا در شبکه‌های اقتضایی متحرک شرح داده می‌شوند. در روش DCAD برای ایجاد و به‌روزرسانی نمای عادی از الگوریتم خوشه‌بندی وزن‌دار WFWC استفاده می‌شود. در روش IPCAAD و نسخه تقریبی آن به نام IAPCAAD با استفاده از تحلیل مولفه‌های اصلی افزایشی نمای عادی ایجاد و به‌روزرسانی می‌شود.

در فصل پنجم، ابتدا ابزار شبیه‌ساز NS2 به عنوان یکی از پرکاربردترین شبیه‌سازهای شبکه‌های کامپیوتری در پروژه‌های دانشگاهی و محیط‌های پژوهشی معرفی می‌شود. سپس، تاثیرگذاری حملات بر کارآیی شبکه و میزان انرژی مصرفی گره‌های شبکه مورد بررسی قرار می‌گیرد. بدین منظور از پارامترهای نرخ تحویل بسته‌ها (*PDR*) و تاخیر انتها-به-انتها (End-to-End Delay) استفاده می‌شود. در نهایت، کارآیی روش‌های پیشنهادی برای تشخیص چهار حمله مسیریابی سیاه‌چاله، سریع، همسایه

و ارسال سیل‌آسای بسته‌های RREQ مورد ارزیابی قرار می‌گیرند. بدین منظور از پارامترهای نرخ تشخیص و نرخ هشدار نادرست استفاده می‌شود. نتایج آزمایش‌های انجام‌شده نشان می‌دهند که روش‌های پیشنهادی از کارآیی خوبی در تشخیص حملات برخوردار هستند.

در پایان در فصل ششم، کارهای انجام شده در این پژوهش جمع‌بندی شده و پیشنهادهایی برای پژوهش‌های آتی ارائه می‌شود.