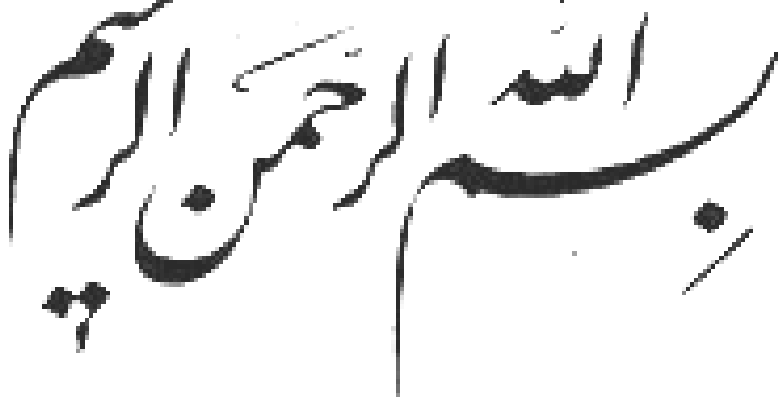
بسم الله الرحمن الرحيم

دانشگاه تربیت مدرس
دانشکده مهندسی برق و کامپیوتر

بسمه تعالی

تاییدیه اعضای هیات داوران حاضر در جلسه دفاع از رساله دکتری

آقای محمد رحمانی منش رساله ۲۴ واحدی خود را با عنوان **تشخیص ناهنجاری در شبکه های اقتضایی مبتنی بر پروتکل AODV** در تاریخ ۱۳۹۱/۱۲/۱۴ ارائه کردند.

اعضای هیات داوران نسخه نهایی این رساله را از نظر فرم و محتوا تایید کرده، پذیرش آنرا برای اخذ درجه دکتری مهندسی کامپیوترـنرم افزار پیشنهاد می کنند.

عضو هیات داوران	نام و نام خانوادگی	رتبه علمی	امضا
استاد راهنما	دکتر سعید جلیلی	دانشیار	
استاد مشاور	دکتر احمدرضا شرافت	استاد	
استاد مشاور	دکتر نصراله مقدم چرکری	استادیار	
استاد ناظر	دکتر مهدی آبادی	استادیار	
استاد ناظر	دکتر مهدی شجری	استادیار	
استاد ناظر	دکتر رسول جلیلی	دانشیار	
مدیر گروه (یا نماینده گروه تخصصی)	دکتر مهدی آبادی	استادیار	

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 پایان نامه/ رساله و درآمدهای حاصل از آنها متعلق به دانشگاه می باشد 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 پایان نامه و رساله به عهده اساتید راهنما و دانشجو می باشد.

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 دانشکده ها، مراکز تحقیقاتی، پژوهشکده ها، پارک علم و فناوری و دیگر واحدها باید با مجوز کتبی صادره از معاونت پژوهشی دانشگاه و براساس آئین نامه های مصوب انجام شود.

ماده ٤- ثبت اختراع و تدوین دانش فنی و یا ارائه یافته ها 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 ٥- این آیین‌نامه در ٥ ماده و یک تبصره در تاریخ۸۷/٤/۱ در شورای پژوهشی و در تاریخ ۸۷/٤/۲۳ 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 محمد رحمانی منش دانشجوی رشته مهندسی کامپیوتر - نرم افزار ورودی سال تحصیلی ۱۳۸۶ مقطع دکتری دانشکده مهندسی برق و کامپیوتر متعهد می شوم کلیه نکات مندرج در آئین نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش های علمی دانشگاه تربیت مدرس را در انتشار یافته های علمی مستخرج از رساله تحصیلی خود رعایت نمایم. در صورت تخلف از مفاد آئین نامه فوق الاشعار به دانشگاه وکالت و نمایندگی می دهم 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»

امضا:.....

تاریخ: ۱۳۹۲/۲/۷

آیین نامه چاپ پایان‌نامه (رساله)های دانشجویان دانشگاه تربیت مدرس

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

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

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

«کتاب حاضر، حاصل رساله دکتری نگارنده در رشته مهندسی کامپیوتر - نرم افزار است که در سال ۱۳۹۱ در دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس به راهنمایی جناب آقای دکتر سعید جلیلی، مشاوره جناب آقای دکتر احمدرضا شرافت و مشاوره جناب آقای دکتر نصرالله مقدم از آن دفاع شده است.»

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

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

ماده ۵: دانشجو تعهد و قبول می کند 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 محمد رحمانی منش دانشجوی رشته مهندسی کامپیوتر - نرم افزار مقطع دکتری تعهد فوق و ضمانت اجرایی آن را قبول کرده، به آن ملتزم می شوم.

نام و نام خانوادگی: محمد رحمانی منش

تاریخ و امضا: ۱۳۹۲/۲/۷

دانشکده مهندسی برق و کامپیوتر

رساله دکتری مهندسی کامپیوتر

تشخیص ناهنجاری در شبکه‌های اقتضایی مبتنی بر پروتکل AODV

محمد رحمانی‌منش

استادراهنما:

دکتر سعید جلیلی

اساتید مشاور:

دکتر احمدرضا شرافت

دکتر نصرالله مقدم

اسفند ۱۳۹۱

تقدیر و تشکر

این رساله با حمایت مالی مرکز تحقیقات مخابرات ایران انجام شده است.

چکیده

پروتکل AODV به عنوان یکی از معروفترین پروتکل‌های مسیریابی شبکه‌های بی‌سیم اقتضایی (MANET) در مقابل شماری از حمله‌ها و سوءرفتارها آسیب‌پذیر می‌باشد. در این رساله یک سیستم تشخیص حمله با رویکرد تشخیص ناهنجاری (ADS) در MANET با پروتکل مسیریابی AODV پیشنهاد می‌شود. در طرح پیشنهادی ۱) خصیصه‌های لازم برای توصیف رفتار پروتکل AODV با رویکردی مبتنی بر رهگیری مرحله به مرحله‌ی ویژگی‌ها و رفتار پروتکل تعریف می‌شود. این امر باعث می‌شود توصیف بهتر و کاملتری از رفتار AODV به دست آید و الگوی حمله‌ها در حالت کلی نسبت به الگوی رفتار عادی قابل تمایز شود. ۲) برای یادگیری رفتار عادی پروتکل AODV دسته‌ی وسیعی از دسته‌بندهای تک‌کلاسی به کار گرفته می‌شود و نقاط قوت و ضعف آن‌ها ارزیابی می‌شود. همچنین روش‌های مبتنی بر ترکیب دسته‌بندها نیز مورد توجه قرار می‌گیرند، به این دلیل که اغلب کارآیی بالاتر و استحکام بیشتری دارند. به جای ترکیب همه‌ی دسته‌بندهای به کار گرفته شده، روشی برای انتخاب دسته‌بندها برای ترکیب با در نظر گرفتن قدرت و تنوع آن‌ها ارائه می‌شود که هدف آن انتخاب زیرمجموعه‌ای از دسته‌بندها برای ترکیب با حداکثر افزایش کارآیی در ازای حداقل افزایش پیچیدگی محاسباتی می‌باشد. ۳) روش‌های دسته‌بندی با خروجی‌های فازی مورد بررسی قرار می‌گیرد که باعث می‌شود کارآیی دسته‌بندها در تشخیص حمله‌ها نسبت به دسته‌بندهای مبتنی بر حد آستانه افزایش قابل توجهی داشته باشد. ۴) یک ADS برای هر دو حالت شبکه‌ی مسطح و شبکه‌ی مبتنی بر خوشه پیشنهاد می‌شود. در شبکه‌های مبتنی بر خوشه روش‌های مختلفی برای تجمیع نظرات اعضای خوشه در گره سرخوشه به کار گرفته می‌شود. ارزیابی‌های ما نشان می‌دهد که بالاترین کارآیی هنگامی به دست می‌آید که از عملگر OWA برای تجمیع نظرات گره‌ها استفاده شود. همچنین کارآیی ADS در حالت کلی در شبکه‌های مبتنی بر خوشه به طور محسوسی از شبکه‌های مسطح بالاتر می‌باشد. ۵) با نگاشت مساله‌ی تشخیص اشیاء خارجی توسط دسته‌بند SVDD به مساله‌ی تصمیم‌گیری گروهی، دسته‌بند SVDD به نحوی تغییر داده می‌شود که مرزهای تصمیم آن با توجه به توزیع داده‌های آزمایش وفق‌پذیر باشد. این نگاشت قابلیت‌های زیادی را در اختیار ما قرار می‌دهد که انتخاب خصیصه‌ی پویا برای تشخیص ناهنجاری از آن جمله است، بدین معنی که با به کارگیری آن می‌توان هر حمله را با خصیصه‌های مجزایی تشخیص داد که برای آن حمله باارزشتر هستند. این امر باعث می‌شود کارآیی دسته‌بند SVDD در تشخیص حمله‌ها افزایش یابد.

کلمات کلیدی: شبکه‌ی بی‌سیم اقتضایی، AODV، تشخیص ناهنجاری، دسته‌بند تک‌کلاسی، ترکیب دسته‌بندها، تصمیم‌گیری گروهی، SVDD.

فهرست مطالب

فهرست اصطلاحات

ADS	Anomaly detection system
AODV	Ad hoc on-demand distance vector routing
LIC	Lowest id clustering
MANET	Mobile ad hoc network
MoG	Mixture of Gausian models
OWA	Ordered weighted averaging
OWS	Ordered weighted sum
PCA	Principle component analysis
PDE	Parzen density estimation
ROC	Reciever operating characteristic curve
RS	Reputation system
SOM	Selp-organizing maps
SVDD	Support vector data description
SVM	Support vector machine
WA	Weighted averaging
WS	Weighted sum

فهرست شکل‌ها

فهرست جداول

فصل اول

کلیات

۱-۱ مقدمه

شبکه‌ی بی‌سیم اقتضایی[۱] یا شبکه‌ی سیار اقتضایی[۲] (MANET) عبارت است از یک شبکه‌ی بدون زیرساختار ثابت[۳] که از تعدادی گره بی‌سیم تشکیل شده است که به طور کاملا پویا شبکه‌ی خود را بدون هیچ مدیریت مرکزی تشکیل می‌دهند [۱]. تامین امنیت در شبکه‌های MANET به دلایلی مانند آسیب‌پذیری اتصالات بی‌سیم، تغییرات پویای توپولوژی، عدم وجود مرکز تایید گواهی[۴]، حفاظت فیزیکی محدود گره‌ها، فقدان نقطه مدیریت یا پایش[۵] مرکزی و محدودیت منابع مانند انرژی، حافظه و توان محاسباتی مشکل است [۲].

مطالعات اولیه‌ای که روی شبکه‌های بی‌سیم اقتضایی صورت گرفته است، به پیشنهاد پروتکل‌هایی برای مسایل پایه‌ای شبکه مثل مسیریابی منجر شده است. یکی از معروفترین پروتکل‌های مسیریابی در MANET، پروتکل AODV[۶] [۳و۴] می‌باشد که با این فرض طراحی شده است که تمامی گره‌ها با صداقت کار خود را انجام می‌دهند و بنابراین ویژگی‌های امنیتی در آن لحاظ نشده است. در نتیجه این پروتکل در مقابل تعدادی از حمله‌ها و سوءرفتارهایی که شبکه را تهدید می‌کنند، آسیب‌پذیر می‌باشد.

برای مقابله با این حمله‌ها معمولا روش‌های پیشگیری از حمله یا روش‌های تشخیص حمله به کار گرفته می‌شوند. روش‌های پیشگیری از حمله مانند رمزنگاری و احراز هویت معمولا قدم اول مقابله با حمله می‌باشد، ولی این روش‌ها عموما پاسخگوی نیاز ما برای پیکربندی شبکه‌ای عاری از رفتارهای سوء نمی‌باشد. اگر چه این مکانیزم‌ها از برخی حمله‌ها از جانب گره‌های خارجی، جلوگیری می‌کنند، ولی نمی‌توانند از حمله‌هایی که از جانب گره‌های داخلی متخاصم که کلیدهای رمزگشایی لازم را در اختیار دارند و شبکه را تهدید می‌کنند، جلوگیری کنند. مکانیزم‌های تشخیص حمله لازم است تا این حمله‌ها را تشخیص دهند [۵].

سیستم‌های تشخیص حمله به دو روش عمده کار می‌کنند [۶]. این دو روش عبارتند از:

---

[1] ad hoc wireless network
[2] mobile ad hoc network
[3] infrastructureless
[4] certificate authority
[5] monitoring
[6] ad hoc on-demand distance vector routing

۱- تشخیص ناهنجاری[1]: نمایه‌ای[2] از رفتار عادی شبکه را تعریف می‌کند و هر انحرافی از این نمایه را به عنوان ناهنجاری در نظر می‌گیرد. این تکنیک می‌تواند حمله‌هایی که تا به حال ناشناخته بودند را هم تشخیص دهد.

۲- تشخیص سوءاستفاده[3] یا تشخیص بر مبنای امضا[4]: این روش امضاها یا توالی[5]های از پیش تعریف شده که یک حمله را نشان می‌دهد را تعریف می‌کند. در حقیقت رفتارهای غیرمعمول از پیش تعریف می‌شوند و رفتارهای مشاهده شده با این رفتارهای از پیش تعریف شده مقایسه می‌شوند. بدیهی است این روش نمی‌تواند حمله‌های ناشناخته را تشخیص دهد.

در این رساله یک سیستم تشخیص حمله با رویکرد تشخیص ناهنجاری (که به اختصار سیستم تشخیص ناهنحاری نامیده می‌شود) در شبکه MANET با پروتکل مسیریابی AODV پیشنهاد می‌کنیم. سیستم‌های تشخیص ناهنجاری[6] (ADS) در MANET با چالش‌های بیشتری نسبت به شبکه‌های معمول سیمی روبرو می‌باشند [۷]. بدون نقطه بازرسی متمرکز مثل مسیریاب‌ها و دروازه‌ها، یک ADS برای MANET محدود به استفاده از ترافیک ورودی و خروجی یک گره خاص می‌باشد. همچنین الگوریتم‌هایی که ADS در MANET استفاده می‌کند باید ذاتا توزیع شده باشند و باید این مساله را در نظر داشته باشند که آنها فقط بخشی از ترافیک شبکه را مشاهده می‌کنند. علاوه بر آن به خاطر پهنای باند پایین در دسترس گره‌ها، سیستم‌های ADS باید مبادلات بین گره‌های شبکه را محدود نمایند.

همانطور که گفته شد، سیستم‌های تشخیص ناهنجاری، نمایه‌ای از رفتار عادی شبکه را تعریف می‌کنند و هر انحرافی از آن را به عنوان ناهنجاری در نظر می‌گیرند. در این صورت مهمترین مساله‌ای که در طراحی ADS در این رساله با آن روبرو هستیم، این است که چگونه می‌توان رفتار عادی شبکه مبتنی بر پروتکل AODV را توصیف کرد و با توجه به آن به دنباله رخدادهای شبکه در طول یک بازه زمانی در هنگام کارکرد شبکه برچسب "عادی" یا "غیرعادی" زد.

توصیف رفتار پروتکل AODV به عنوان زیربنای اصلی طراحی ADS می‌باشد، بدین معنی که تمامی رویکردهای یادگیری رفتار عادی و تشخیص حمله از آن بهره می‌گیرند. در سیستم‌های تشخیص ناهنجاری، توصیف رفتار معمولا با تعریف خصیصه انجام می‌شود و به تبع آن رفتار عادی به عنوان قیدی روی این

---

[1] anomaly detection
[2] profile
[3] misuse detection
[4] signature based detection
[5] sequence
[6] anomaly detection systems