

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



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 کامپیوتر سترم افزار پیشنهاد می کنند.

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

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 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 پایان‌نامه 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 آئین‌نامه های مصوب انجام شود.

ماده ۴- 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 ۵- این آیین‌نامه در ۵ ماده و یک تبصره در تاریخ ۸۷/۴/۱ 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 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 آئین‌نامه حق مالکیت مادی و معنوی در مورد نتایج پژوهش‌های علمی دانشگاه تربیت مدرس را در انتشار یافته‌های علمی مستخرج از 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»

امضا:.....

تاریخ: ۱۳۹۲/۲/۱۷

آیین نامه چاپ پایان نامه (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 می شوند:

ماده ۱: در صورت اقدام به چاپ پایان نامه (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 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 احمد رضا شرافت و مشاوره جناب آقای دکتر نصرالله مقدم از آن دفاع شده است.»

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

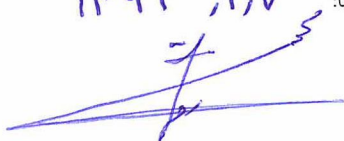
ماده ۴: در صورت عدم رعایت ماده ۳، ۵۰٪ بهای شمارگان چاپ شده را به عنوان خسارت به دانشگاه تربیت مدرس، تأدیه کند.

ماده ۵: دانشجو تعهد و قبول می کند در صورت خودداری از پرداخت بهای خسارت، دانشگاه می تواند خسارت مذکور را از طریق مراجع قضایی مطالبه و وصول کند؛ به علاوه به دانشگاه حق می دهد به منظور استیفای حقوق خود، از طریق دادگاه، معادل وجه مذکور در ماده ۴ را از محل توقیف کتابهای عرضه شده نگارنده برای فروش، تأمین 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

استاد راهنما:

دکتر سعید جلیلی

اساتید مشاور:

دکتر احمد رضا 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 مرحله 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 نداشت 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 آزمایشی وفق‌پذیر باشد. این نداشت 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 بارزتر 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

فصل اول	کلیات	۱
۱-۱	مقدمه	۱
۲-۱	تعریف مساله	۳
۳-۱	اهداف پژوهش	۴
۴-۱	نوآوری های پژوهش	۵
۵-۱	مروری بر فصول رساله	۵
فصل دوم	مفاهیم پایه	۷
۱-۲	مقدمه	۷
۲-۲	ویژگی های شبکه MANET	۷
۳-۲	پروتکل های پایه مسیریابی	۸
۴-۲	فرآیند اجرایی پروتکل AODV	۹
۵-۲	آسیب پذیری های امنیتی پروتکل AODV	۱۴
۶-۲	خوشه بندی در شبکه های اقتضایی	۱۶
۷-۲	دسته بندی های تک کلاسی	۱۷
۸-۲	تصمیم گیری گروهی	۲۰
۱-۸-۲	گونه های مختلف عملگر OWA	۲۱
۲-۸-۲	کاربردهای عملگر OWA	۲۲
۳-۸-۲	تولید وزن عملگر OWA	۲۳
۹-۲	سیستم شهرت	۲۵

۲۵.....	۱-۹-۲ مفاهیم سیستم شهرت
۲۷.....	۲-۹-۲ مدل شهرت
۲۸.....	۱۰-۲ جمع‌بندی
۲۹.....	فصل سوم تاریخچه پژوهش در تشخیص ناهنجاری در MANET
۲۹.....	۱-۳ مقدمه
۲۹.....	۲-۳ پژوهش‌های انجام شده
۳۴.....	۳-۳ نتیجه‌گیری و جمع‌بندی
۳۶.....	فصل چهارم تعریف خصیصه مبتنی بر رفتار پروتکل AODV و تاثیر حمله‌ها روی آن
۳۶.....	۱-۴ مقدمه
۳۶.....	۲-۴ تحلیل و توصیف پروتکل AODV
۳۷.....	۱-۲-۴ تعریف خصیصه بر مبنای رفتار پروتکل AODV
۳۸.....	۲-۲-۴ خصیصه‌های تعریف شده
۴۵.....	۳-۴ تحلیل حمله‌ها روی پروتکل مسیریابی AODV
۴۵.....	۱-۳-۴ محیط شبیه‌سازی
۴۶.....	۲-۳-۴ تاثیر حمله‌ها روی پارامترهای کارایی شبکه
۴۸.....	۳-۳-۴ رتبه بندی اثرپذیری خصیصه ها
۴۹.....	۴-۳-۴ تحلیل حساسیت خصیصه‌ها
۵۱.....	۵-۳-۴ اندازه‌گیری قدرت تشخیص حمله‌ها با دسته‌بندهای تک کلاسی
۵۲.....	۴-۴ نتیجه‌گیری و جمع‌بندی
۵۴.....	فصل پنجم تشخیص حمله در شبکه‌های مسطح

- ۵-۱ مقدمه ۵۴
- ۵-۲ تشخیص ناهنجاری با دسته‌بندهای تک‌کلاسی به صورت مستقل ۵۵
- ۵-۲-۱ ارزیابی ۵۵
- ۵-۳ ترکیب دسته‌بندهای تک‌کلاسی با روش میانگین‌گیری ۵۸
- ۵-۳-۱ انتخاب دسته‌بندها برای ترکیب ۵۹
- ۵-۳-۲ ترکیب دسته‌بندهای تک‌کلاسی ۶۰
- ۵-۳-۳ ارزیابی ۶۲
- ۵-۳-۴ مباحثی روی ترکیب دسته‌بندها ۶۵
- ۵-۴ ترکیب دسته‌بندهای تک‌کلاسی با روش رای‌گیری ۶۶
- ۵-۴-۱ ارزیابی ۶۷
- ۵-۵ ترکیب دسته‌بندهای تک‌کلاسی با روش رای‌گیری فازی ۶۸
- ۵-۵-۱ ارزیابی ۷۰
- ۵-۶ مقایسه روش‌های مختلف ترکیب دسته‌بندها ۷۲
- ۵-۷ مقایسه با سایر پژوهش‌ها ۷۲
- ۵-۸ نتیجه‌گیری و جمع‌بندی ۷۵
- فصل ششم تشخیص حمله در شبکه‌های مبتنی بر خوشه ۷۷
- ۶-۱ مقدمه ۷۷
- ۶-۲ تشخیص ناهنجاری با دسته‌بندهای تک‌کلاسی به صورت مستقل ۷۸
- ۶-۲-۱ ارزیابی ۷۸
- ۶-۳ ترکیب دسته‌بندهای تک‌کلاسی با روش میانگین‌گیری ۸۰

- ۸۱..... ۱-۳-۶ ارزیابی
- ۸۲..... ۴-۶ ترکیب دسته‌بندهای تک کلاسی با روش رای‌گیری
- ۸۲..... ۱-۴-۶ ارزیابی
- ۸۴..... ۵-۶ ترکیب دسته‌بندهای تک کلاسی با روش میاگین‌گیری فازی
- ۸۵..... ۱-۵-۶ انتساب وزن یکسان به گره‌ها
- ۸۵..... ۲-۵-۶ تولید وزن با توجه به شرایط محیطی شبکه
- ۸۷..... ۳-۵-۶ ارزیابی
- ۸۹..... ۶-۶ مقایسه‌ی روش‌های مختلف ترکیب دسته‌بندها
- ۹۰..... ۷-۶ ارزیابی زمان اجرا
- ۹۱..... ۸-۶ مقایسه با سایر پژوهش‌ها
- ۹۲..... ۹-۶ سیستم شهرت
- ۹۲..... ۱-۹-۶ مدل شهرت
- ۹۴..... ۲-۹-۶ جمع‌بندی نظرات اعضای خوشه در گره سرخوشه
- ۹۴..... ۳-۹-۶ ارزیابی
- ۹۶..... ۱۰-۶ نتیجه‌گیری و جمع‌بندی
- ۹۷..... فصل هفتم توصیف وفق‌پذیر داده‌ها با استفاده از بردارهای پشتیبان
- ۹۷..... ۱-۷ مقدمه
- ۹۸..... ۲-۷ تاریخچه پژوهش در رابطه با SVDD
- ۹۹..... ۳-۷ SVDD سه مرحله‌ای
- ۱۰۱..... ۱-۳-۷ تجزیه فاصله در SVDD

- ۱۰۲..... OWS-SVDD و WS-SVDD تک کلاسی ۲-۳-۷
- ۱۰۵..... OWS-SVDD از استفاده پویا با خصیصه‌ی ۳-۳-۷ انتخاب
- ۱۰۶..... روش پیشنهادی در فضای کرنل ۴-۷
- ۱۰۷..... ارزیابی ۵-۷
- ۱۰۷..... مقیاس کردن داده‌ها ۱-۵-۷
- ۱۰۷..... نتایج شبیه‌سازی ۲-۵-۷
- ۱۰۹..... تحلیل Δ ۳-۵-۷
- ۱۱۰..... شبیه‌سازی در فضای ۴۰ خصیصه‌ای ۴-۵-۷
- ۱۱۲..... مقایسه با سایر دسته‌بندها ۵-۵-۷
- ۱۱۳..... نتیجه‌گیری و جمع‌بندی ۶-۷
- ۱۱۵..... فصل هشتم نتیجه‌گیری و پیشنهاد کارهای آینده ۱۱۵
- ۱۲۰..... مقالات مستخرج از رساله ۱۲۰
- ۱۲۱..... مراجع ۱۲۱

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 Gaussian 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

- شکل ۱-۲. قالب بسته‌ی RouteRequest در پروتکل AODV ۱۰
- شکل ۲-۲. قالب بسته‌ی RouteReply در پروتکل AODV ۱۲
- شکل ۳-۲. قالب بسته‌ی RouteError در پروتکل AODV ۱۳
- شکل ۴-۲. سناریوهای پایش مستقیم (a) و دریافت توصیه‌نامه (b) برای جمع‌آوری شواهد ۲۶
- شکل ۱-۴. فرآیند تعریف خصیصه بر مبنای پروتکل ۳۸
- شکل ۲-۴. اثرات اعمال حمله‌های مختلف در شبکه ۴۷
- شکل ۳-۴. تحلیل حساسیت خصیصه برای حمله‌های مختلف ۵۰
- شکل ۱-۵. نمودار سیستم تشخیص ناهنجاری پیشنهادی در هر گره ۵۵
- شکل ۲-۵. نمودار ROC برای حمله‌های مختلف با دسته‌بندهای متفاوت ۵۶
- شکل ۳-۵. مقدار $WAUC$ برای حمله‌های مختلف با دسته‌بندهای متفاوت ۵۷
- شکل ۴-۵. مقایسه مقدار PoC برای دسته‌بندهای مختلف ۵۸
- شکل ۵-۵. روش میانگین‌گیری برای ترکیب دسته‌بندها در هر گره ۵۹
- شکل ۶-۵. الگوریتم پیشنهادی برای انتخاب دسته‌بندها ۶۱
- شکل ۷-۵. الگوریتم پیشنهادی برای ترکیب L دسته‌بند انتخاب شده ۶۲
- شکل ۸-۵. مقدار $IPoC$ برای SVDD-RBF و دسته‌بندهای دیگر ۶۳
- شکل ۹-۵. مقدار $IPoC$ برای Fused(MoG-PPCA, SVDD-RBF) و دسته‌بندهای دیگر ۶۳
- شکل ۱۰-۵. نمودار ROC برای حمله‌های مختلف با دسته‌بند Average(MoG-PPCA, SVDD-RBF) ۶۴
- شکل ۱۱-۵. مقایسه کارایی دسته‌بندهای SVDD-RBF, MoG-PPCA و Fused Classifier = Average(MoG-PPCA, SVDD-RBF) ۶۵

- شکل ۵-۱۲. مقادیر PoC برای قویترین دسته‌بند برای اندازه‌های مختلف ترکیب دسته‌بندها ۶۵
- شکل ۵-۱۳. روش رای‌گیری برای ترکیب دسته‌بندها در هر گره ۶۶
- شکل ۵-۱۴. نمودار ROC برای حمله‌های مختلف با دسته‌بند (Vote(MoG-PPCA, SVDD-RBF, SOM) ۶۷
- شکل ۵-۱۵. مقایسه کارایی دسته‌بندهای SOM, SVDD-RBF, MoG-PPCA و Fused Classifier = Vote(MoG-PPCA, SVDD-RBF, SOM) ۶۷
- شکل ۵-۱۶. روش رای‌گیری فازی برای ترکیب دسته‌بندها در هر گره ۶۹
- شکل ۵-۱۷. توابع عضویت برای فازی‌سازی خروجی دسته‌بندها ۷۰
- شکل ۵-۱۸. نمودار ROC برای حمله‌های مختلف با دسته‌بند (Fuzzy Vote(MoG-PPCA, SVDD-RBF, SOM) ۷۱
- شکل ۵-۱۹. مقایسه کارایی دسته‌بندهای SOM, SVDD-RBF, MoG-PPCA و Fused Classifier = Fuzzy Vote(MoG-PPCA, SVDD-RBF, SOM) ۷۱
- شکل ۵-۲۰. مقایسه روش‌های مختلف ترکیب دسته‌بندها در شبکه‌های مسطح ۷۲
- شکل ۵-۲۱. تقسیم زمان برای راه‌اندازی حمله در شبکه در [۱۰۴] ۷۴
- شکل ۵-۲۲. تعداد بازه‌های زمانی در هر کدام از قسمت‌های ۲۵۰۰ ثانیه‌ای که برچسب "غیرعادی" خورده‌اند نسبت به بازه‌ی اول، با استفاده از روش [۱۰۴] برای حمله‌های سیاه‌چاله (نمودار سمت چپ) و سوراخ کرم (نمودار سمت راست) ۷۴
- شکل ۵-۲۳. نمودار ROC برای حمله‌ی سوراخ کرم با دسته‌بند (Average(MoG-PPCA, SVDD-RBF) و بردار خصیصه متفاوت ۷۴
- شکل ۶-۱. جمع‌بندی نظرات گره‌های هر خوشه در گره سرخوشه ۷۸
- شکل ۶-۲. نمودار سیستم تشخیص ناهنجاری پیشنهادی در هر گره ۷۹
- شکل ۶-۳. نمودار ROC برای حمله‌های مختلف با دسته‌بندهای متفاوت ۷۹
- شکل ۶-۴. مقایسه کارایی دسته‌بندهای SOM, SVDD-RBF و MoG-PPCA ۸۰

- شکل ۵-۶. ترکیب دسته‌بندهای تک‌کلاسی در هر گره با روش میانگین‌گیری ۸۰
- شکل ۶-۶. نمودار ROC برای حمله‌های مختلف با دسته‌بند Average(MoG-PPCA, SVDD-RBF) ... ۸۱
- شکل ۶-۷. مقایسه کارایی دسته‌بندهای SVDD-RBF, MoG-PPCA و Fused Classifier = Average(MoG-PPCA, SVDD-RBF) ۸۱
- شکل ۶-۸. ترکیب دسته‌بندهای تک‌کلاسی در هر گره با روش رای‌گیری ۸۲
- شکل ۶-۹. نمودار ROC برای حمله‌های مختلف با دسته‌بند Vote(MoG-PPCA, SVDD-RBF, SOM) ۸۲
- شکل ۶-۱۰. مقایسه کارایی دسته‌بندهای SOM, SVDD-RBF, MoG-PPCA و Fused Classifier = Vote(MoG-PPCA, SVDD-RBF, SOM) ۸۳
- شکل ۶-۱۱. ترکیب دسته‌بندهای تک‌کلاسی در هر گره با روش میانگین‌گیری فازی ۸۴
- شکل ۶-۱۲. مقایسه روش تولید وزن مبتنی بر شرایط شبکه با روش تولید وزت مبتنی بر کمیت‌سنج با $Q(x) = \sqrt{x}$ ۸۷
- شکل ۶-۱۳. نمودار ROC برای حمله‌های مختلف با دسته‌بند Fuzzy Average(MoG-PPCA, SVDD-RBF, SOM) با انتساب وزن یکسان به گره‌ها ۸۸
- شکل ۶-۱۴. نمودار ROC برای حمله‌های مختلف با دسته‌بند Fuzzy Average(MoG-PPCA, SVDD-RBF, SOM) با انتساب وزن به گره‌ها بر اساس شرایط محیطی شبکه ۸۸
- شکل ۶-۱۵. مقایسه کارایی دسته‌بندهای SOM, SVDD-RBF, MoG-PPCA و Fused Classifier1 = Fuzzy Average(MoG-PPCA, SVDD-RBF, SOM), Same Weights ۸۹
- شکل ۶-۱۶. مقایسه کارایی روش‌های مختلف ترکیب دسته‌بندها در شبکه‌های مسطح و شبکه‌های مبتنی بر خوشه ۹۰
- شکل ۶-۱۷. نمودار ROC برای حمله‌های مختلف با دسته‌بند C4.5 ۹۲
- شکل ۶-۱۸. نمودار ROC برای حمله‌های مختلف با دسته‌بند Fuzzy Average(MoG-PPCA, SVDD-RBF, SOM) در صورت استفاده از سیستم شهرت ۹۵

- شکل ۶-۱۹. مقایسه‌ی کارآیی دسته‌بند (Fuzzy Average, MoG-PPCA, SVDD-RBF, SOM) در دو حالت استفاده از وزن یکسان برای گره‌ها و استفاده از سیستم شهرت ۹۵
- شکل ۷-۱. روند اجرایی SVDD سه مرحله‌ای ۱۰۰
- شکل ۷-۲. مرزهای بدست آمده با استفاده از دسته‌بندهای SVDD, WS-SVDD و OWS-SVDD ۱۰۴
- شکل ۷-۳. نمودار ROC برای حمله‌های مختلف با دسته‌بندهای SVDD و 4DFS-SVDD ۱۰۸
- شکل ۷-۴. مقایسه $WAUC$ برای حمله‌های مختلف با دسته‌بندهای SVDD و 4DFS-SVDD ۱۰۹
- شکل ۷-۵. مقایسه مقدار Δ برای یک مجموعه داده عادی و پنج مجموعه داده حمله ۱۱۰
- شکل ۷-۶. نمودار ROC برای حمله‌های مختلف با دسته‌بندهای SVDD و 4DFS-SVDD روی ۴۰ خصیصه ۱۱۱
- شکل ۷-۷. مقایسه SVDD و 4DFS-SVDD در فضای ورودی ۴۰ خصیصه‌ای ۱۱۲
- شکل ۷-۸. مقایسه مقدار Δ برای یک مجموعه داده عادی و پنج مجموعه داده حمله در فضای ورودی ۴۰ خصیصه‌ای ۱۱۲
- شکل ۷-۹. مقایسه SVDD و 4DFS-SVDD با سایر دسته‌بندها ۱۱۳

فهرست جداول

- جدول ۳-۱. مقایسه‌ی پژوهش‌های انجام شده در تشخیص ناهنجاری در MANET با پروتکل مسیریابی AODV..... ۳۵
- جدول ۴-۱. رتبه‌بندی اثرپذیری خصیصه‌ها با حمله‌های مختلف ۴۸
- جدول ۶-۱. زمان لازم برای یک میلیون عملیات تشخیص با استفاده از دسته‌بندهای مختلف (بر حسب ثانیه) ۹۱
- جدول ۶-۲. خصیصه‌های انتخاب شده از بین ۱۲۱ خصیصه تعریف شده برای پایش رفتار گره‌ها ۹۴
- جدول ۷-۱. خصیصه‌های انتخاب شده از بین ۱۲۱ خصیصه تعریف شده ۱۱۰

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 کاملاً 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 [۳ و ۴] 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 معمولاً روش‌های پیشگیری از حمله یا روش‌های تشخیص حمله به کار گرفته می‌شوند. روش‌های پیشگیری از حمله مانند رمزنگاری و احراز هویت معمولاً قدم اول مقابله با حمله می‌باشد، ولی این روش‌ها عموماً 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^۱: نمایه‌ای^۲ 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^۳ یا تشخیص بر مبنای امضا^۴: این روش امضاها یا توالی^۵های 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 ناهنجاری نامیده می‌شود) در شبکه MANET با پروتکل مسیریابی AODV پیشنهاد می‌کنیم. سیستم‌های تشخیص ناهنجاری^۶ (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 ذاتاً 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 معمولاً 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