دانشگاه صنعتی امیرکبیر(پلی تکنیک تهران)
دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان‌نامه کارشناسی ارشد
مهندسی فناوری اطلاعات گرایش امنیت اطلاعات

ایجاد همکاری بین گره ها و افزایش قابلیت دسترسی به سرویس در شبکه های سیار بی سیم موردی با استفاده از نظریه بازی ها

نگارش
آزاده عمرانی

استاد راهنما
دکتر مهران سلیمان فلاح
استاد مشاور
دکتر مهدی دهقان

اردیبهشت ۱۳۸٦

PDF-XChange
Click to buy NOW!
www.docu-track.com

بسمه تعالی

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)

فرم اطلاعات پایان‌نامه
کارشناسی - ارشد و دکترا

تاریخ:
شماره:

معاونت پژوهشی
فرم پروژه تحصیلات تکمیلی 7

مشخصات دانشجو:

نام و نام خانوادگی: آزاده عمرانی | دانشجوی آزاد ● | بورسیه ○ | معادل ○

شماره دانشجوئی: 83131140 | دانشکده: مهندسی کامپیوتر و فناوری اطلاعات | رشته تحصیلی: فناوری اطلاعات | گروه: امنیت

مشخصات استاد راهنما:

نام و نام خانوادگی: دکتر مهران سلیمان فلاح | درجه و رتبه: دانشیار

مشخصات استاد مشاور:

نام و نام خانوادگی: دکتر مهدی دهقان | درجه و رتبه: استادیار

عنوان پایان‌نامه به فارسی :

ایجاد همکاری بین گره ها و افزایش قابلیت دسترسی به سرویس در شبکه های سیار بی سیم موردی با استفاده از نظریه بازی ها

عنوان پایان‌نامه به انگلیسی:

Enforcing Cooperation among Nodes and Improving Service Availability in MANETs Using Game Theory

نوع پروژه: کارشناسی ○ | ارشد ● | دکتر ا ○ | سال تحصیلی: 85-86

کاربردی ○ | بنیادی ○ | توسعه‌ای ● | نظری ○

تاریخ شروع : خرداد 85 | تاریخ خاتمه : اردیبهشت 86 | تعداد واحد :6 | سازمان تأمین کننده اعتبار : مرکز تحقیقات مخابرات ایران

واژه‌های کلیدی به فارسی: شبکه‌های سیار موردی، گره‌های خودخواه، مسأله همکاری، نظریه‌بازی‌ها

واژه‌های کلیدی به انگلیسی : Cooperation problem, Game theory, Mobile ad hoc networks, Selfish nodes

مشخصات ظاهری	تعداد صفحات							تعداد مراجع	تعداد صفحات ضمائم
	135	تصویر ●	جدول ●	نمودار ●	نقشه ○	واژه‌نامه ●		62	14
زبان متن	فارسی ●		انگلیسی ○		چکیده			فارسی ●	انگلیسی ●

یادداشت

نظرها و پیشنهادها به منظور بهبود فعالیت‌های پژوهشی دانشگاه

استاد:

دانشجو:

امضاء استاد راهنما: **تاریخ:**

1 : ارائه به معاونت پژوهشی به همراه یک نسخه الکترونیکی از پایان‌نامه و فرم اطلاعات پایان‌نامه بصورت **PDF** همراه چاپ چکیده (فارسی انگلیسی) و فرم اطلاعات پایان‌نامه

2 : ارائه به کتابخانه دانشکده (شامل دو جلد پایان نامه به همراه نسخه الکترونیکی فرم در لوح فشرده طبق نمونه اعلام شده در صفحه خانگی کتابخانه مرکزی)

به نام خدا

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

تعهدنامه اصالت اثر

تاریخ:

اینجانب آزاده عمرانی متعهد می‌شوم که مطالب مندرج در این پایان‌نامه حاصل کار پژوهشی اینجانب تحت نظارت و راهنمایی اساتید دانشگاه صنعتی امیرکبیر بوده و به دستاوردهای دیگران که در این پژوهش از آنها استفاده شده است مطابق مقررات و روال متعارف ارجاع و در فهرست منابع و مآخذ ذکر گردیده است. این پایان‌نامه قبلاً برای احراز هیچ مدرک هم‌سطح یا بالاتر ارائه نگردیده است.

در صورت اثبات تخلف در هر زمان، مدرک تحصیلی صادر شده توسط دانشگاه از درجه اعتبار ساقط بوده و دانشگاه حق پیگیری قانونی خواهد داشت.

کلیه نتایج و حقوق حاصل از این پایان‌نامه متعلق به دانشگاه صنعتی امیرکبیر می‌باشد. هرگونه استفاده از نتایج علمی و عملی، واگذاری اطلاعات به دیگران یا چاپ و تکثیر، نسخه‌برداری، ترجمه و اقتباس از این پایان‌نامه بدون موافقت کتبی دانشگاه صنعتی امیرکبیر ممنوع است. نقل مطالب با ذکر مآخذ بلامانع است.

آزاده عمرانی

امضا

تقدیم به

مادر و پدر نازنینم

که ترکیب زیبای وجودشان

بذر نامم را در نهادم پروراند.

سپاسگزاری

از استاد راهنمای گرامیم، جناب آقای دکتر مهران سلیمان فلاح، به خاطر تمام زحمات و راهنمایی‌های دقیقشان تشکر و قدردانی می‌کنم. ایشان با صبر و شکیبایی بسیار، در طول مدتی که افتخار شاگردیشان را داشتم، اساس تفکر علمی و زیبایی‌های یک کار تحقیقاتی را به خوبی به من نمایاندند. از استاد محترم، جناب آقای دکتر مهدی دهقان، بخاطر کمک‌ها و رهنمودهایشان در مشاورهٔ این پایان‌نامه کمال تشکر را دارم. همچنین وظیفه خود می‌دانم از تمامی اساتید دانشمند و بزرگواری که در سراسر دوران تحصیلم مرا یاری داده‌اند سپاسگزاری کنم. از این میان، برخود لازم می‌دانم از استاد مهربان و فاضلم جناب آقای دکتر بابک صادقیان که در تکوین دیدگاه من در دوره کارشناسی ارشد نقش اساسی داشته‌اند با احترام فراوان تشکر کنم. همین طور از یاری دوستان خوبم خانم‌ها مریم بخت، زهرا جباری، فرزانه احمدی، و مهرناز سادات اخوی که در طول انجام این پایان نامه همراه و مشوق من بوده‌اند صمیمانه قدردانی می‌کنم.

این پایان نامه بر اساس نامه شماره ۵۰۰/۹۲۴۹/ت مورخ ۸۵/۷/۲۴ تحت حمایت مرکز تحقیقات مخابرات ایران انجام پذیرفته است.

چکیده

شبکه‌های سیار موردی[1] نوعی از شبکه‌های بی‌سیم بدون زیرساخت هستند که با ویژگی‌های ارتباط چندگام، ماهیت نامتمرکز، توپولوژی پویا، و محدودیت منابع شناخته می‌شوند. در این شبکه‌ها، هر گره نقش مسیریاب[2] را نیز ایفا می‌کند که منجر به مصرف میزان قابل توجهی از انرژی در گره خواهد شد. بنابراین، گره‌های خودخواه، برای حفظ منابع انرژی خود، ترجیح می‌دهند با دیگران همکاری نکنند و به این ترتیب موجب نوعی ممانعت از سرویس غیر فعال در شبکه می شوند. در این پایان نامه، روشی برای تشویق گره‌های خودخواه به همکاری در شبکه‌های موردی پیشنهاد می‌شود. ابتدا نشان می‌دهیم که در یک پروتکل مسیریابی مانند Ad hoc-VCG، پروتکلی که مسیر بهینه را از نظر مصرف انرژی شناسایی کرده و برای همکاری گره‌ها روی این مسیر انگیزه فراهم می‌کند، تبانی گره‌ها تهدیدی برای پایداری مسیر بهینه است. سپس، با به کار گیری مدل بازی‌های ائتلافی[3]، مکانیزمی جدید، مبتنی بر قیمت، و نیز مقاوم در برابر تبانی طراحی می‌کنیم. این مکانیزم پایداری مسیر بهینه را از نظر مصرف انرژی تضمین کرده و در عین حال انگیزهٔ لازم را برای همکاری گره‌ها در شبکه فراهم می‌کند. دراین مکانیزم، از مفهوم بازی ـ محورِ[4] هسته برای توزیع بهرهٔ حاصل از همکاری بین اعضای یک ائتلاف استفاده می‌شود که طبق آن تبانی، هیچ بهره اضافی برای بازیکنان نخواهد داشت.

واژه‌های کلیدی: شبکه‌های سیار موردی، مسیریابی، نظریه‌بازی‌ها، همکاری

---

[1] Mobile Ad hoc Network (MANET)
[2] router
[3] coalitional games
[4] game-theoretic

علائم اختصاری

DSR	Dynamic Source Routing
AODV	Ad hoc On-demand Distance Vector
RFC	Request For Comments
DoS	Denial of Service
CCS	Credit Clearance Service
VCG	Vickrey-Clark-Groves
OPR	OverPayment Ratio
ASTR	Ad hoc STable Routing
RREQ	Route REQuest packet
RREP	Route REPly packet

فهرست مطالب

۱ مقدمه ۱

۱-۱ مسیریابی آگاه از انرژی ۳

۱-۲ قابلیت دسترسی به سرویس و مسألهٔ همکاری ۳

۱-۳ ایجاد همکاری ۸

۱-٤ اهداف و نوآوری‌ها ۱۱

۱-۵ سازمان مطالب پایان نامه ۱۲

۲ شبکه‌های سیار موردی، محدودیت انرژی، و مسأله همکاری ۱٤

۲-۱ پروتکل‌های مسیریابی در شبکه‌های سیار موردی ۱٤

۲-۱-۱ مسیریابی پویا از مبدأ (DSR) ۱٦

۲-۲ مصرف انرژی در شبکه‌های موردی ۱۸

۲-۲-۱ مسیریابی آگاه از انرژی ۲۰

۲-۳ ایجاد همکاری در شبکه‌های موردی ۲۱

۲-۳-۱ مکانیزم‌های مبتنی بر اشتهار ۲۳

۲-۳-۲ مکانیزم‌های مبتنی بر اعتبار ۲۸

۲-۳-۳ بحث و مقایسه ۳٤

۲-٤ خلاصه و نتیجه گیری ٤۳

۳ نظریه بازی‌ها ٤٦

۳-۱ تاریخچه ٤٦

۳-۲ بازی کلاسیک معمای زندانی ٤۷

۳-۳ فرضیات و تعاریف ٤۸

۳-٤ دسته بندی بازی‌ها ۵۰

۳-٤-۱ بازی‌های مشارکتی و بازی‌های غیر مشارکتی ۵۱

۳-٤-۲ بازی‌های استراتژیک و بازی‌های گسترده ۵۲

۳-٤-۳ بازی‌های با اطلاعات کامل و نا کامل ۵۲

۳-٤-٤ بازی‌های با اطلاعات تمام و ناتمام ۵۳

۳-۵ تعادل نَش ۵۳

۳-٦ انواع بازی‌های مزایده ۵۵

۳-۶-۱ مزایدهٔ ویکری ۵۷
۳-۷ بازی های ائتلافی ۵۸
۳-۷-۱ تعاریف اولیه ۵۹
۳-۷-۲ راه‌حل‌ها ۶۱
۳-۸ خلاصه و نتیجه‌گیری ۶۳
٤ نظریه بازی‌ها و مسألهٔ همکاری در شبکه‌های سیار موردی ٦٥
٤-١ چرا از نظریه بازی‌ها برای تحلیل شبکه‌های موردی استفاده کنیم؟ ٦٦
٤-٢ راه‌حل میچیاردی و مولوا ٦٨
٤-٣ روش سرینیواسان ٦٩
٤-٤ سیستم Sprite ٧٠
٤-٥ پروتکل Ad hoc-VCG ٧٢
٤-٥-١ مکانیزم ویکری-کلارک-گرووز (VCG) ٧٣
٤-٥-٢ مسیریابی Ad hoc-VCG ٧٤
٤-٥-٣ اضافه پرداخت در Ad hoc-VCG ٧٥
٤-٥-٤ مسائل مطرح در روش Ad hoc-VCG ٧٦
٤-٦ خلاصه و نتیجه گیری ٧٦
٥ مدل‌سازی مسألهٔ همکاری با استفاده از بازی‌های ائتلافی ٨٠
٥-١ پیش زمینه ٨١
٥-١-١ بهبود مصرف انرژی ٨١
٥-١-٢ خودخواهی و پرداخت اعتبار ٨٢
٥-١-٣ مسألهٔ تبانی ٨٣
٥-٢ تعاریف و فرضیات ٨٣
٥-٣ مدل شبکه ٨٥
٥-٤ مسألهٔ تبانی در پروتکل Ad hoc-VCG ٨٨
٥-٥ پروتکل مسیریابیASTR ٩٠
٥-٥-١ اکتشاف مسیر ٩٠
٥-٥-٢ انتقال داده ٩٤
٥-٥-٣ بازیابی مسیر ٩٤
٥-٦ طرح پرداخت ASTR برای پایداری مسیر بهینه در برابر تبانی گره‌ها ٩٥
٥-٦-١ نسبت اضافه پرداخت ١٠٠
٥-٧ خلاصه و نتیجه‌گیری ١٠٢
٦ نتایج شبیه‌سازی ١٠٦
٦-١ شرایط شبیه‌سازی ١٠٦

٦-٢ تحلیل نتایج ١٠٨
٦-٣ خلاصه و نتیجه‌گیری ١١٥
٧ نتیجه‌گیری و کارهای آینده ١١٧
فهرست منابع ١٢١
واژه‌نامه ١٢٦

فهرست شکل‌ها

شکل ۱-۱ مثالی از کاربرد شبکه‌های سیار موردی..... ۲
شکل ۲-۱ طبقه بندی پروتکلهای مسیریابی شبکه‌های موردی بی سیم [۲]..... ۱۵
شکل ۲-۲ مسیریابی در DSR..... ۱۷
شکل ۲-۳ دسته بندی مکانیزم‌های پیشنهاد شده برای اعمال همکاری ۲۳
شکل ۲-٤ مکانیزم دیده‌بانی ۳۷
شکل ۳-۱ نمایش بازی معمای زندانی..... ٤۸
شکل ۳-۲ تعادل نش: بازیکنان جرأت تعویض بازیشان را ندارند..... ۵۵
شکل ٤-۱ نگاشت اجزای تشکیل دهندهٔ یک شبکه سیار موردی با مؤلفه‌های یک بازی..... ٦٦
شکل ۵-۱ مقایسهٔ میزان تداخل در (الف) ارتباط مستقیم (ب) ارتباط از طریق مسیر بهینه مصرف انرژی ۸۲
شکل ۵-۲ مدل گرافی از یک شبکه موردی ۸٦
شکل ۵-۳ بازی اکتشاف مسیر بین گرهٔ مبدأ و هر گرهٔ میانی ۹۳
شکل ۵-٤ مجموعهٔ بازیکنان در بازی ائتلافی..... ۹٦
شکل ۵-۵ شرایط خاص در مقایسه نسبت اضافه پرداخت ۱۰۱
شکل ٦-۱ مقایسهٔ میانگین نسبت اضافه پرداخت (درجهٔ میرایی سیگنال=٤)..... ۱۱۱
شکل ٦-۲ مقایسهٔ میانگین زمان اجرا (درجهٔ میرایی سیگنال=٤)..... ۱۱۱
شکل ٦-۳ به صرفه بودن طرح ASTR (درجهٔ میرایی سیگنال=٤)..... ۱۱۲
شکل ٦-٤ مقایسهٔ میانگین نسبت اضافه پرداخت (درجهٔ میرایی سیگنال=۲) ۱۱۲
شکل ٦-۵ مقایسهٔ میانگین زمان اجرا (درجهٔ میرایی سیگنال=۲) ۱۱۳
شکل ٦-٦ به صرفه بودن طرحASTR (درجهٔ میرایی سیگنال=۲) ۱۱۳
شکل ٦-۷ مقایسهٔ میانگین نسبت اضافه پرداخت (درجهٔ میرایی سیگنال=٦) ۱۱٤
شکل ٦-۸ مقایسهٔ میانگین زمان اجرا (درجهٔ میرایی سیگنال=٦) ۱۱٤
شکل ٦-۹ به صرفه بودن طرحASTR (درجهٔ میرایی سیگنال=٦) ۱۱۵

فصل ۱

مقدمه

۱ مقدمه

امروزه رشد چشمگیری در استفاده از فناوری ارتباطات بی‌سیم حاصل شده است و در آیندهٔ نزدیک گسترهٔ کاربردهای این فناوری از ارتباطات ماهواره‌ای تا منازل شخصی، فضاهای عمومی، سازمان‌ها و شبکه‌های خصوصی خواهد بود. در بسیاری از کاربردها، شبکه‌های بی‌سیم نسبت به شبکه‌های سیمی انتخاب‌های بهتری هستند. این امر به دلیل سهولت دسترسی، کاهش هزینه‌ها، و امکان حرکت در شبکه‌های بی‌سیم است. شبکه‌های بی‌سیم به دو دسته طبقه‌بندی می‌شوند: شبکه‌های بی‌سیم با زیرساخت (شبکه‌های سلولی، شبکه‌های بی‌سیم محلی[۱] و ماهواره‌ها)، و شبکه‌های بی‌سیم بدون زیرساخت که برای کاربرد در جایی‌که امکان برپایی زیرساخت وجود ندارد پدید آمده‌اند[۱]. شبکه‌های حسگر[۲] و شبکه‌های سیار موردی[۳] که شباهت‌های بسیاری با هم دارند، نمونه‌هایی از شبکه‌های بی‌سیم بدون زیرساخت هستند.

یک شبکه حسگر مجموعه‌ای از حسگرهای کوچک و کم‌هزینه است که معمولاً توان محاسباتی پایین و انرژی باتری بسیار محدودی دارند و در بیشتر موارد حرکت نمی‌کنند. این حسگرها در محیط‌های مورد نظر(مثلاً محیط‌های نظامی، صنعتی یا زیستی) توزیع شده و کار حفاظت و یا نظارت بر این محیط‌ها را انجام می‌دهند. حسگرها اطلاعات مورد نظر را از محیط جمع آوری کرده و به‌صورت چندگام[٤] به کاربر خود مخابره می‌کنند. یک شبکهٔ سیار موردی مجموعه‌ای از وسایل محاسباتی متحرک،

---

[1] Wireless Local Area Network (WLAN)

[2] sensor network

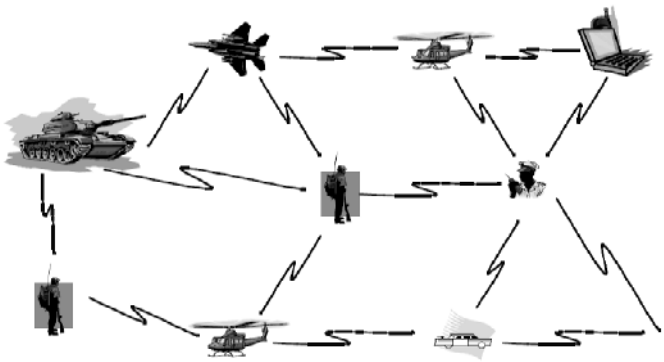
[3] Mobile Ad hoc Network (MANET)

[٤] در ارتباط چندگام (multi-hop) ترافیک مبدأ با کمک چند گرهٔ میانی و پس از عبور از آنها به مقصد می‌رسد.

است که با هم یک شبکه رادیویی خاص منظوره، چندگام، و نامتمرکز می‌سازند. از این پس، این وسایل محاسباتی را گره‌های شبکه می‌نامیم. از آنجایی که این شبکه‌ها معمولاً کاربردهای خاصی دارند، به آنها شبکه‌های خاص منظوره یا موردی گفته می‌شود. در این شبکه‌ها هیچ زیر ساختی مثل مرکز راه‌گزینی[1]، ایستگاه پایه[2]، نقطهٔ دسترسی[3]، و دیگر تجهیزات متمرکز، که در شبکه‌های بی‌سیم با زیرساخت استفاده می‌شود، وجود ندارد.

دو ویژگی عمدهٔ شبکه‌های سیار موردی عبارتند از:

- توپولوژی پویا – حرکت گره‌ها و وجود یا عدم وجود آنها در شبکهٔ سیار موردی منجر به یک توپولوژی پویا می‌شود. همچنین در این شبکه‌ها، گره‌ها با همکاری یکدیگر نقش زیرساخت شبکه را بازی می‌کنند و بنابراین وجود توپولوژی پویا مشکلاتی در این رابطه ایجاد خواهد کرد.
- منابع محدود – گره‌های شبکه به دلیل قابلیت جابجایی از باتری، که یک منبع محدود است، به‌عنوان منبع انرژی خود استفاده می‌کنند. همچنین به دلیل استفادهٔ همزمان گره‌ها از رسانهٔ بی‌سیم، پهنای باند در دسترس هر گره نیز محدودیت دارد.



شکل ۱۱-- مثالی از کاربرد شبکه‌های سیار موردی

[1] switching center
[2] base station
[3] access point

شکل ۱-۱ نمونه‌ای از کاربرد شبکه‌های سیار موردی است که در آن ادوات و نیروهای نظامی باید در محیطی بدون زیرساخت با هم در ارتباط باشند. علاوه بر عملیات نظامی، عملیات امداد و نجات، کلاس‌های درس مجازی، کنفرانس‌ها، و شبکه‌های شهری از دیگر کاربردهای این شبکه‌ها هستند.

۱-۱ مسیریابی آگاه از انرژی

در شبکه‌های سیار موردی، گرهٔ مبدأ برای ارسال داده به مقصدی که در داخل محدودهٔ ارسالِ بی‌سیم وی قرار ندارد، از گره‌های واقع در حد فاصل این دو گره استفاده می‌کند. به عبارت دیگر، گره‌های میانی نقش مسیریاب[1] را ایفا می‌کنند. تا کنون پروتکل‌های مسیریابی متعددی با توجه به شرایط خاص شبکه‌های سیار موردی پیشنهاد شده‌اند[۲]. پروتکل‌های ارائه شده از معیارهای متفاوتی در انتخاب مسیر استفاده می‌کنند. در دسته‌ای از پروتکل‌های پیشنهادی (پروتکل‌های آگاه از انرژی[2])، مسیریابی با توجه به معیار مصرف انرژی انجام می‌شود. این موضوع به دلیل آن است که معمولاً گره‌های شبکه برای مدت زمان طولانی امکان شارژ مجدد باتری خود را ندارند و انرژی باتری یکی از منابع با ارزش تلقی می‌شود. از سوی دیگر، در نسل جدید وسایل بی‌سیم، قدرت سیگنال ارسالی و در نتیجه میزان انرژی مصرفی در ارسال پیام قابل کنترل است. به این ترتیب، گره‌های شبکه می‌توانند با تنظیم قدرت ارسال خود توپولوژی شبکه و نحوهٔ مسیریابی را تحت تأثیر قرار دهند.

پروتکل مسیریابی پیشنهاد شده در این پایان نامه، بر اساس این فرض طراحی شده که شبکه‌های سیار موردی محدودیت انرژی داشته و گره‌های شبکه می‌توانند قدرت ارسالی خود را تنظیم کنند. همچنین، پروتکل ارائه شده علاوه بر مصرف بهینهٔ انرژی، موارد دیگری را نیز مانند ایجاد انگیزهٔ همکاری و جلوگیری از تبانی گره‌ها فراهم می‌آورد.

۱-۲ قابلیت دسترسی به سرویس و مسألهٔ همکاری

یکی از مهم‌ترین جنبه‌ها در بررسی عملکرد هر شبکهٔ ارتباطی، امنیت آن است. عدم ملاحظه امنیت در طراحی شبکه، ممکن است به سادگی امکان خرابکاری را در آن فراهم کند. فاش شدن یا

---

[1] router
[2] energy aware

دستکاری اطلاعات رد و بدل شده به دست افراد غیر مجاز، و یا قطع دسترسی به سرویس مورد انتظار از شبکه نمونه‌هایی از این خرابکاری‌هاست. به طور کلی، برای تأمین امنیت باید سه ویژگی زیر برقرار باشد:

۱) محرمانگی اطلاعات[1]،

۲) صحت داده‌ها[2]،

۳) قابلیت دسترسی به سرویس[3].

به دلیل خصوصیات ذاتی شبکه‌های بی‌سیم و به ویژه شبکه‌های سیار موردی، تأمین این ویژگی‌ها و برقراری امنیت در آنها نسبت به سایر شبکه‌ها مشکل‌تر است. غیر قابل اعتماد بودن پیوندهای بی‌سیم میان گره‌ها و در دسترس بودن رسانه ارتباطی برای همگان، توپولوژی پویا، عدم وجود زیرساخت برای مدیریت امنیت، و همین طور وابستگی عملکرد شبکه به همکاری درست گره‌ها باعث آسیب پذیری بیشتر این شبکه‌ها در مقابل حملات می‌شود. اگرچه بسیاری از راه‌حل‌های امنیتی ارائه شده برای شبکه‌های بی‌سیم با زیرساخت[4] در شبکه‌های موردی نیز قابل اعمال است، ولی استفاده از این راه‌حل‌ها برای از بین بردن تمامی آسیب‌پذیری‌ها در این شبکه‌ها کافی نیست. بنابراین، لزوم طراحی روش‌های امنیتی خاص شبکه‌های موردی احساس می‌شود. برخی از راه حل‌های امنیتی که تا کنون به طور خاص برای شبکه‌های موردی ارائه شده‌اند در مراجع [٤] و [٥] یافت می‌شوند. در مرجع [٦]، مروری بر انواع پروتکل‌های مسیریابی امن در شبکه‌های موردی ارائه شده است.

این پایان نامه، از بین سه ویژگی امنیتی مطرح شده، روی ویژگی امنیتی سوم یعنی قابلیت دسترسی به سرویس در شبکه‌های سیار موردی تمرکز دارد و سعی می‌کند نوع خاصی از مسائل را که منجر به نقض این ویژگی می‌شود حل کند. این مسأله، عدم همکاری گره‌ها در شبکه است. لازم به ذکر است که عدم قابلیت دسترسی به سرویس در شبکه‌های سیار موردی ممکن است به دلایلی غیر از نقض امنیت در سیستم نیز به وقوع پیوندد و به عبارت دیگر، قصد و نیت خاصی در وقوع آن در کار نباشد. حوادث طبیعی یا خرابی غیر عمدی سخت افزار یا نرم افزار در گره‌های شبکه از جملهٔ این دلایل هستند.

---

[1] information confidentiality

[2] data integrity

[3] service availability

[4] برای بررسی جامع این راه حل‌ها به مرجع [۳] رجوع شود.

بررسی و بهبود کارایی شبکه‌ها، با در نظر گرفتن وجود چنین مشکلاتی، در طراحی سیستم‌های تحمل‌پذیر خطا[1] هدف قرار می‌گیرد. در این پایان‌نامه، از چنین مباحثی صرف‌نظر شده و تنها جنبهٔ امنیتی مورد هدف قرار گرفته است.

حملهٔ ممانعت از سرویس[2] هنگامی اتفاق می‌افتد که قابلیت دسترسی به سرویس به صورت آگاهانه نقض شود. این مسأله ممکن است در لایه‌های مختلف پشتهٔ پروتکل شبکه، اتفاق بیفتد. آسیب پذیری شبکه‌های موردی در مقابل حملات ممانعت از سرویس در لایه‌های پایین، مشابه آسیب پذیری سایر شبکه‌های بی‌سیم و در لایه‌های بالا، مشابه دیگر شبکه‌ها است. با وجود این، بیشتر حملات ممانعت از سرویسی که در لایهٔ شبکه در شبکه‌های موردی انجام می‌شوند از ویژگی‌های ذاتی خاص این شبکه‌ها بهره‌برداری می‌کنند. مسألهٔ عدم همکاری گره‌ها در شبکه‌های سیار موردی منجر به نوعی ممانعت از سرویس در لایهٔ شبکه می‌شود.

یک حملهٔ ممانعت از سرویس می‌تواند توسط موجودیت‌های خارج شبکه و یا توسط موجودیت‌های داخل شبکه انجام شود. موجودیت‌های خارج شبکه افراد یا وسایلی هستند که برای عضویت در شبکه و استفاده از آن غیر مجاز شمرده می‌شوند. حملات خارجی نسبت به حملات داخلی، که از سوی گره‌های مجاز شبکه انجام می‌شود، ساده‌تر تشخیص داده می‌شوند. در صورتی‌که از پروتکل‌های تصدیق اصالت[3] در لایه‌های بالاتر شبکه استفاده شود، حملات خارجی تنها می‌توانند کارکردهای لایهٔ پیوند[4] و لایهٔ فیزیکی را هدف قرار دهند. از بین انواع حملات خارجی، حملهٔ تداخل فعال[5] می‌تواند با سوء استفاده از ماهیت رسانهٔ بی‌سیم، منجر به انسداد کانال ارتباطی بی‌سیم و در نتیجه ایجاد اختلال در سرویس‌دهی شبکه شود[۷]. استفاده از تکنولوژی طیف وسیع[6][۸] راه حل مناسبی برای مقابله با این نوع حملات است.

همان‌طور که گفته شد، تشخیص و جلوگیری از حملات ممانعت از سرویس داخلی بسیار مشکل‌تر از حملات خارجی است. این حملات می‌توانند روی تمام لایه‌های پشتهٔ پروتکل اثرات جدی داشته باشند، زیرا از سوی گره یا گره‌های مجاز شبکه، که به اطلاعات شبکه نیز دسترسی دارند، انجام

---

[1] fault tolerant systems
[2] Denial of Service (DoS)
[3] authentication protocols
[4] data link layer
[5] active interference
[6] spread spectrum

می‌شوند. بدرفتاری[1] گره‌های داخلی می‌تواند صورت‌های مختلفی داشته باشد. در یک طبقه بندی، گره‌های بدرفتار را به دو دسته تقسیم می‌کنیم: گره‌های بدنهاد[2] و گره‌های خودخواه[3].

- گره‌های بدنهاد: این دسته از گره‌ها قصد دارند در عملکرد درست شبکه اختلال ایجاد کنند و در صورت امکان، سرویس دهی شبکه را متوقف نمایند. ممکن است گره یا مجموعه‌ای ازگره‌های داخلی شبکه، تحت کنترل دشمن در آیند و به این ترتیب به گره‌های بدنهاد تبدیل شوند. این گره‌ها با وجود این که جزو گره‌های مجاز شبکه شناخته می‌شوند، می‌توانند به راحتی با انحراف از رفتار درست مطابق پروتکل‌های مورد نظر، در کار شبکه اختلال ایجاد کنند. به چنین حملاتی که دشمن کنترل کامل یک گرهٔ تصدیق هویت شده را در اختیار داشته و می‌تواند رفتار دلخواهی را برای مختل کردن کار شبکه در پیش بگیرد، حملات بیزانسی[4] گفته می‌شود [۹]. به عنوان مثال، انتشار اطلاعات نادرست از سوی گرهٔ بدنهاد ممکن است به ناکارامدی سرویس‌های شبکه بینجامد. در حملهٔ شکنجهٔ محرومیت از خواب[5]، گرهٔ بدنهاد با ارائهٔ اطلاعات نادرست، سایر گره‌ها را وادار به انجام پردازش‌های سنگین و غیر لازم می‌کند تا به این ترتیب منابع محدود گره‌ها کاهش یافته و نتوانند عملکرد طبیعی خود را داشته باشند. در لایهٔ شبکه، فرایند مسیریابی ممکن است با دستکاری در بسته‌های کنترلیِ مربوط به مسیریابی متوقف شود. یک گرهٔ بدنهاد می‌تواند با ارسال بسته‌های درخواست مسیر به صورت افراطی در کارکرد شبکه اختلال ایجاد کند. ایجاد حلقه در مسیر، دور انداختنِ انتخابیِ بسته‌ها، سرریز کردن جداول مسیریابی و مسموم کردن اطلاعات مربوطه نیز می‌تواند فرایند مسیریابی را متوقف کند. یکی از اصلی‌ترین حملات بیزانسی لایهٔ شبکه، حملهٔ سیاه‌چاله[6] است. در این نوع حمله، گرهٔ بدنهاد در مسیریابی شرکت می‌کند و با این‌کار

---

[1] misbehavior
[2] malicious
[3] selfish
[4] Byzantine
[5] sleep deprivation torture
[6] black hole attack

سعی می‌کند تا خود را در مسیر انتقال بسته‌ها قرار دهد، اما پس از اتمام مرحله مسیریابی از انتقال بسته‌های داده خودداری می‌کند تا در عملکرد شبکه اختلال ایجاد شود.

- گره‌های خودخواه: این دسته از گره‌ها برخلاف گره‌های بدنهاد تحت نفوذ دشمن قرار ندارند و بنابراین خرابکاری در شبکه هدف آنها نیست. خودخواهی در واقع یک نوع رفتار ناشی از شرایط است. همان طور که اشاره شد، یکی از ویژگی‌های خاص گره‌ها در شبکه‌های سیار موردی، محدودیت منابعی چون پهنای باند و انرژی باتری است. در شبکه‌های موردی، ارتباط تک‌گام بین دو گرهٔ همسایه از طریق پروتکل لایهٔ پیوند صورت می‌پذیرد. پروتکل لایهٔ شبکه این ارتباط را گسترش می‌دهد تا گره‌های خارج از محدودهٔ یکدیگر نیز بتوانند با هم ارتباط برقرار کنند. یک گرهٔ خودخواه در لایهٔ پیوند سعی دارد گذردهی خود را حداکثر کرده و بیشترین پهنای باند کانال را مشغول به ارتباطات خود نگه دارد. در نتیجهٔ این عمل، سایر گره‌ها نخواهند توانست از کانال استفاده کنند و به این ترتیب یک حملهٔ ممانعت از سرویس توسط گرهٔ خودخواه انجام می‌شود. این نوع از خودخواهی در مراجع [۱۰] و [۱۱] بررسی شده‌اند. از سوی دیگر، برقراری ارتباط رادیویی یکی از عمده‌ترین عملیات مصرف کنندهٔ انرژی (به خصوص برای گرهٔ فرستنده) محسوب می‌شود. همان‌طورکه اشاره شد، گره‌ها باید در لایهٔ شبکه به عنوان مسیریاب برای ایجاد ارتباط میان دو گرهٔ دیگر عمل کنند ولی انجام عملیات مسیریابی و جلورانی[1] ترافیک دیگران انرژی گره را به میزان قابل توجهی مصرف خواهد کرد. گرهٔ خودخواه، در صورتی که امکان انتخاب داشته باشد، ترجیح می‌دهد از انرژی محدود خود برای سرویس دادن به دیگران استفاده نکرده و در عوض تنها در جهت اهداف شخصی خود انرژی مصرف کند. دور ریزی بسته‌ها[2]ی دیگران، شایع‌ترین حملهٔ ممانعت از سرویسی است که می‌تواند توسط گره‌های خودخواه انجام شود. عدم همکاری برخی گره‌ها در سرویس دادن به دیگران بر پارامترهای کارایی شبکه تأثیر منفی

---

[1] forwarding
[2] packet dropping