دانشگاه صنعتی شیراز

دانشکده مهندسی کامپیوتر و فناوری اطلاعات و کامپیوتر

پایان نامه کارشناسی ارشد

در رشته مهندسی فناوری اطلاعات گرایش شبکه های کامپیوتری

تشخیص گره متخاصم در حمله‌ی سوراخ سیاه بر روی پروتکل مسیریابی AODV

به وسیله:

حمید شفیعی نژاد قهرود

استاد راهنما:

مهندس محمد رفیع خوارزمی

استاد مشاور:

دکتر رضا جاویدان

آذر ماه ۱۳۹۱


بسم الله الرحمن الرحيم

بسمه تعالی

تشخیص گره متخاصم درحمله‌ی سوراخ سیاه بر روی پروتکل مسیریابی AODV

به‌وسیله:

حمید شفیعی نژاد

برای اخذ درجه کارشناسی ارشد

گروه فناوری اطلاعات دانشکده مهندسی کامپیوتر و فناوری اطلاعات دانشگاه صنعتی شیراز

ارزیابی پایان‌نامه توسط هیأت داوران:

مهندس محمدرفیع خوارزمی	مربی	مهندسی کامپیوتر	(استاد راهنما)	.....
دکتر رضا جاویدان	استادیار	مهندسی کامپیوتر	(استاد مشاور)	.....
دکتر منیژه کشتگری	استادیار	مهندسی کامپیوتر	(داور)	.....

مدیرامورآموزشی وتحصیلات تکمیلی دانشگاه

تقدیم به

شریک زندگی ام، همراه همیشگی ام

همسر مهربانم

و

دو گوهر گرانبها

پدرم و مادرم

سپاسگزاری

با سپاس فراوان از استاد عزیزم، جناب آقای دکتر محمد رفیع خوارزمی که در مدت تهیه پایان نامه همواره مشوق و راهنمای اینجانب بوده اند.

و

از زحمات دلسوزانه ی

سرکار خانم دکتر منیژه گشتکری که از هیچ زحمتی برای بالابردن سطح علمی بنده دریغ نکردند

و

سایر اساتید گروه مهندسی کامپیوتر و فناوری اطلاعات

چکیده

تشخیص گره متخاصم در حمله‌ی سوراخ سیاه بر روی پروتکل مسیریابی AODV

به وسیله‌ی :

حمید شفیعی نژاد قهرود

شبکه‌های موردی سیار ترکیبی از گره‌های مستقل‌اند که فاقد هر گونه زیر ساختی می‌باشند. گره‌های این شبکه می‌توانند پیرامون محیط خود حرکت کرده و با استفاده از برقراری ارتباط با گره‌های دیگر به انتقال داده بپردازند. محدودیت در انرژی گره‌ها و نیز محیط کاربرد، این شبکه‌ها را با چالش‌هایی مواجه ساخته است. یکی از این چالش‌ها، امنیت در این شبکه‌هاست. بی‌سیم بودن، مستقل بودن گره‌ها و محدودیت توان آنها نقاط آسیب‌پذیری متعددی را در آنها ایجاد نموده است. حمله بر علیه فرایند مسیریابی در شبکه‌های موردی سیار یکی از انواع حملاتی است که در آن گره متخاصم سعی در ایجاد مسیر ناامن جهت اختلال در کارایی شبکه می‌کند.

پروتکل مسیریابی AODV یکی از مشهورترین پروتکل‌های مسیریابی در شبکه‌های موردی متحرک است. مکانیزم‌هایی که AODV برای برقراری ارتباط بین گره‌ها بکار می‌برد استفاده از این پروتکل را در شبکه‌هایی که در آن گره‌ها متحرک‌اند را مناسب می‌سازد. از طرفی بکارگیری این مکانیزم‌ها رخنه‌های امنیتی را ایجاد می‌کند. حمله‌ی سوراخ سیاه یکی از حملاتی است که از این رخنه‌ها استفاده کرده است. در این حمله گره متخاصم سعی می‌کند تا با استفاده از ترفندهایی خود را به عنوان مسیر بهینه معرفی کرده و از این طریق داده‌های ارسالی را سمت خود جذب کند. این پایان نامه یک پروتکل امن در مقابل حمله‌ی سوراخ سیاه به نام Without Black Hole AODV (WBHAODV) پیشنهاد می‌دهد. در پروتکل

پیشنهادی مکانیزمی جهت شناسایی گره متخاصم ارائه شده است. در طراحی پروتکل پیشنهادی سعی شده تا کمترین سربار ترافیکی و تاخیر زمانی نسبت به پروتکل AODV ایجاد شود. در نهایت پروتکل پیشنهادی در نرم‌افزار شبیه‌ساز NS2 پیاده‌سازی شده و بعدی از شبیه‌سازی در کاربردهای مختلف، نتایج حاصل برای ارزیابی الگوریتم از نظر مقاومت در مقابل حمله و نیز کارایی آن نسبت به پروتکل AODV مورد بحث و بررسی قرار گرفته است.

فهرست مطالب

عنوان صفحه

۱- مقدمه ۲

۱-۱- پیشگفتار ۲

۱-۲- شبکه‌های موردی سیار ۳

۱-۲-۱- انواع شبکه‌های موردی ۳

۱-۲-۲- کاربرد شبکه‌های موردی متحرک ۳

۱-۲-۳- خصوصیات شبکه‌های موردی متحرک ۴

۱-۳- امنیت در شبکه‌های موردی سیار ۵

۱-۴- انگیزه پایان‌نامه ۵

۱-۴-۱- اهداف پایان نامه ۶

۱-۴-۲- ساختار پایان نامه ۶

فصل ۲ ۷

۲- حمله سوراخ سیاه در پروتکل مسیریابی AODV ۸

۲-۱- مسیریابی در شبکه‌های موردی سیار ۸

۲-۲- پروتکل مسیریابی AODV ۱۴

۲-۲-۱- فرایند کشف مسیر ۱۴

۲-۲-۲- نگهداری مسیر ۱۸

۲-۳- امنیت در مسیریابی ۱۹

۲-۳-۱- حملات مبتنی بر تغییر ۲۰

۲-۳-۲- حملات مبتنی بر جعل ۲۰

۲-۳-۳- حمله سوراخ کرم ۲۱

۲-۳-۴- حمله سیل آسا ۲۲

۲-۳-۵- حمله هجوم ۲۳

۲-۴- حمله سوراخ سیاه ۲۵
۲-۴-۱- نقاط ضعف پروتکل مسیریابی AODV ۲۵
۲-۴-۲- حمله‌ی سوراخ سیاه ۲۶
۲-۵- مروری بر تحقیقات انجام شده ۲۷
۲-۵-۱- مکانیزم‌های مبتنی بر رمزنگاری ۲۷
۲-۵-۲- پروتکل SAODV ۳۵
۲-۵-۳- روش‌های مبتنی بر تشخیص حمله ۳۵
فصل سوم ۴۵
۳- روش پیشنهادی برای جلوگیری از حمله‌ی سوراخ سیاه بر روی پروتکل AODV ۴۶
۳-۱- مقدمه ۴۶
۳-۲- روش پیشنهادی ۴۷
۳-۳- نحوه عملکرد پروتکل پیشنهادی ۴۹
۳-۴- مرحله‌ی پیاده‌سازی ۵۰
۳-۴-۱- پیاده‌سازی حمله سوراخ سیاه ۵۰
۳-۴-۲- پیاده‌سازی پروتکل پیشنهادی ۵۱
فصل ۴ ۵۴
۴- شبیه سازی و بررسی نتایج ۵۵
۴-۱- محیط شبیه‌سازی ۵۵
۴-۲- مقاومت الگوریتم در برابر حمله‌ی سوراخ سیاه ۵۶
۴-۳- ارزیابی کارایی الگوریتم ۵۸
۴-۳-۱- بررسی تاثیر الگوریتم در تاخیر شبکه ۵۸
۴-۳-۲- بررسی تاثیر الگوریتم در خروجی شبکه ۶۰
۴-۳-۳- بررسی تاثیر الگوریتم در نرخ تحویل بسته ۶۳
فصل ۵ ۶۵
۵- نتیجه گیری و پیشنهادات ۶۶

۵-۱- نتیجه گیری ۶۶
۵-۲- پیشنهادات :..... ۶۷
پیوست یک ۷۰
پیوست دو..... ۷۴

فهرست شکل‌ها

شکل ۲-۱ الف: محدوده‌ی پوشش پخش فراگیرA. ب: پس از آنکه B و D پخش فراگیر A را دریافت کردند. ج: پس از آنکه C و F و G پخش فراگیر A را دریافت کردند . د: پس از آنکه E و H و I پخش فراگیر A را دریافت کردند.گره‌های سایه دار دریافت کنندگان جدید هر مرحله محسوب می‌شوند. فلش‌ها مسیر معکوس (مسیر برگشت) را نشان می‌دهند..... ۱۵

شکل ۲-۲ قالب بسته ROUTE REQUEST..... ۱۵

شکل ۲-۳ قالب بسته RREP..... ۱۷

شکل ۲-۴ الف: جدول مسیریابیD قبل از آنکه G از کار بیافتد. ب: گراف پس از حذف G شبکه..... ۱۹

شکل ۲-۵ حملات امنیتی در شبکه‌های موردی متحرک..... ۲۰

شکل ۲-۶ حمله‌ی جعل؛ گره متخاصم M آدرس دیگر نودها را جعل کرده و در فرایند مسیریابی اختلال ایجاد می کند..... ۲۱

شکل ۲-۷ حمله سوراخ کرم؛ خط نقطه‌چین یک ارتباط سریع بین دو گره متخاصم را نشان می‌دهد..... ۲۱

شکل ۲-۸ حمله‌ی JAMMING: گره مهاجم با ارسال مقدار بسته‌های RREQ بی هدف سعی در بالا بردن ترافیک شبکه و در نهایت کاهش انرژی گره‌ها شود..... ۲۲

شکل ۲-۹ حمله سیل آسا؛ فلش های پررنگ نشان دهنده‌ی مسیر حرکت بسته‌های RREQ هستند..... ۲۳

شکل ۲-۱۰ ارسال بسته‌ی RREP توسط گره متخاصم (M)..... ۲۶

شکل ۳-۱ گره N1 خواستار ارتباط با گره N8. الف- ارسال پیام RREQ توسط N1. ب: ارسال بسته RREP از طرف گره مقصد(N8) و گره متخاصم..... ۴۹

شکل ۳-۲ جدول مسیریابی گره N3..... ۵۰

شکل ۳-۳ مرحله ی بررسی بسته RREP در تابع RECVREPLY. در صورتیکه مقدار شمارنده‌ی گام کوچکتر از ۲ باشد بسته RREP در جدول مسیر ذخیره شده و از طریق تابع SENDVALIDTORREQUEST جهت اعتبارسنجی فرستنده‌ی RREP اقدام می‌شود..... ۵۲

شکل ۳-۴ مرحله اعتبارسنجی فرستنده‌ی RREP. در صورتیکه آدرس مقصد بسته برابر با ادرس گره(INDEX) باشد اعتبار سنجی از طریق شماره دنباله صورت می‌گیرد..... ۵۳

شکل ۴-۱ میانگین خروجی شبکه در حضور تعداد گره‌های متخاصم مختلف..... ۵۶

شکل ۴-۲ نرخ تحویل بسته در حضور تعداد گره‌های متخاصم مختلف..... ۵۷

شکل ۴-۳ شکل میانگین بسته‌های حذف شده در حضور تعداد گره‌های مختلف..... ۵۷

شکل ۴-۴ میانگین تاخیر در تعداد گره‌های مختلف. (گره‌ها ثابت هستند)..... ۵۸

شکل ۴-۵ میانگین تاخیر در تعداد گره‌های مختلف. (سرعت ۵ متر بر ثانیه)..... ۵۹

شکل ۴-۶ میانگین تاخیر در تعداد گره‌های مختلف. (سرعت ۱۰ متر بر ثانیه)..... ۵۹

شکل ۴-۷ مقایسه بین میانگین تاخییر شبکه در سرعت‌های مختلف (تعداد گره‌ها : ۴۰)..... ۶۰

شکل ۴-۸ خروجی شبکه در تعداد گره‌های مختلف (گره‌های ثابت هستند)..... ۶۱

شکل ۴-۹ خروجی شبکه در تعداد گره‌های مختلف (سرعت ۵ متر بر ثانیه)..... ۶۱

شکل ۴-۱۰ خروجی شبکه در تعداد گره‌های مختلف (سرعت ۱۰ متر بر ثانیه)..... ۶۲
شکل ۴-۱۱ مقایسه بین میانگین خروجی شبکه در سرعت‌های مختلف..... ۶۲
شکل ۴-۱۲ مقایسه نرخ تحویل بسته (PDR) در تعداد گره‌های مختلف (گره‌ها ثابت هستند)..... ۶۳
شکل ۴-۱۳ مقایسه نرخ تحویل بسته در تعداد گره‌های مختلف (سرعت ۵ متر بر ثانیه)..... ۶۳
شکل ۴-۱۴ مقایسه نرخ تحویل بسته در تعداد گره‌های مختلف (سرعت ۱۰ متر بر ثانیه)..... ۶۴

فهرست جداول

جدول ۱. مقایسه روش‌های تشخیص حمله‌ی سوراخ سیاه ۴۲
جدول ۲. پارامترها مشترک در محیط شبیه‌سازی..... ۵۵
جدول ۳ تغییر نسبت به الگوریتم AODV..... ۶۶

نشانه‌های اختصاری

MANET	Mobile Ad hoc Network
DSR	Dynamic Source Routing
DSDV	Destination Sequenced Distance Vector
WRP	Wireless Routing Protocol
CGSR	Cluster Switch Gateway Routing
SSR	Scalable Source Routing
ABR	Associativity-Based Routing
RDMAR	Relative Distance Microdiscovery Ad-Hoc Routing
TORA	Temporally Ordered Routing Algorithm
ZRP	Zone Routing Protocol
ZHLS	Zone-Based Hierarchical Link State
AODV	Ad hoc On demand Distance Vector
WBHAODV	Without Black Hole AODV
RREQ	Route Request
RREP	Route Reply
PDR	Packet Delivery Ratio
DoS	Denial of Dervice
TTL	Time To Live
IDS	Intrusion Detection System
MAC	Message Authentication Code

فصل ۱

مقدمه

۱- مقدمه

۱-۱- پیشگفتار

امروزه شبکه‌های کامپیوتری نقش مهمی را در دنیای اطلاعات دارند به طوریکه انتقال داده‌ها بدون در نظر گرفتن شبکه‌ها امکان پذیر نیست. محیط‌های مختلف و کاربردهای مختلف در آن، شبکه‌های گوناگونی را با ویژگی‌های فیزیکی و ساختاری متفاوت به وجود آورده است. شبکه‌های موردی سیار یکی از انواع شبکه‌هاست که اجزای آن را مجموعه‌ای از گره‌های خودمختار تشکیل می‌دهند که می‌توانند پیرامون محیط خود حرکت کرده و به رد و بدل کردن اطلاعات بپردازند. این نوع شبکه‌ها بدون زیرساخت هستند و گره‌های شبکه، برای برقراری ارتباط با یکدیگر از گره‌های دیگر استفاده می‌کنند. به عبارت دیگر هر کدام از گره‌ها می‌توانند نقش یک مسیریاب را داشته باشند[۱].

امروزه کاربردهای شبکه‌های موردی سیار فراوانی پیدا کرده است. بخصوص جمع‌آوری اطلاعات از محیط‌هایی که دسترسی انسان برای بدست آوردن اطلاعات محدود و یا مشکل است. جمع آوری اطلاعات از محیط‌های نظامی، جمع آوری اطلاعات از محیط‌هایی با کاربرد علمی مانند آتشفشان‌ها و استفاده در عملیات‌های جستجو و نجات از قبیل کاربردهای این نوع شبکه‌ها می‌باشد.

اهمیت کاربردهای شبکه‌های موردی سیار، موضوع امنیت اطلاعات در این شبکه‌ها را بسیار حیاتی می‌سازد. از طرفی ویژگی‌های این نوع شبکه‌ها مانند بی‌سیم بودن، متحرک بودن گره‌ها، بدون زیرساخت بودن و مهم‌تر از همه محدودیت انرژی گره‌های شبکه، چالش‌های امنیتی خاص این شبکه ها را بوجود آورده است. ایجاد امنیت در فرایند مسیریابی یکی از این چالش‌هاست. یک مسیر امن مسیری است که هیچ گره متخاصمی دخالتی در ایجاد آن نداشته باشد.

حمله‌ی سوراخ سیاه یکی از حملاتی است که برعلیه پروتکل‌های مسیریابی اجرا می‌شود. در این حمله گره‌ی متخاصم با استفاده از تغییر در بسته‌های مسیریابی یک مسیر کاذب را به عنوان مسیر بهینه معرفی کرده و از این طریق سعی در جذب بسته‌های داده به سمت خود می‌کند و بدین صورت از رساندن بسته‌های داده به مقصد جلوگیری کرده و کارایی شبکه را به شدت تحت تاثیر قرار می‌دهد. بنابراین ممانعت از این حمله، بخصوص در شبکه‌های با کاربردهای حساس یک امر مهم تلقی می‌شود.

پروتکل مسیریابی AODV یکی از پرکاربردترین پروتکل‌های مسیریابی در شبکه‌های موردی سیار است که به شدت در مقابل حمله‌ی سوراخ سیاه دچار ضعف است و با توجه اهمیت این پروتکل، امن نمودن آن در مقابل این حمله یکی از ملزومات حفظ کارایی این پروتکل در شبکه است. هدف از این مقاله ارائه‌ی روشی جهت امن نمودن پروتکل مسیریابی AODV در مقابل حمله‌ی سوراخ سیاه است. در این روش، مکانیزمی جهت شناسایی حمله، طراحی و پیاده سازی شده است و نیز سعی شده تا روش پیشنهادی کمترین سربار را در شبکه داشته باشد و با کمترین هزینه در معیارهایی همچون تاخیر در شبکه، سطح بالایی از مقاومت در مقابل این حمله ایجاد کند. همچنین در طراحی مکانیزم، حفظ نقاط قوت پروتکل مسیریابی AODV در نظر گرفته شده است.

در این تحقیق قصد داریم پس از بررسی چالش‌های امنیتی در مسیریابی شبکه‌های موردی متحرک، الگوریتم مسیریابی که در آن ملاحظات امنیتی گنجانده شده باشد را ارائه دهیم.

۱-۲- شبکه‌های موردی سیار

شبکه‌ی موردی متحرک به شبکه‌ای گفته می‌شود که در آن تجهیزات متحرک با استفاده از رسانه‌ی بی‌سیم با هم ارتباط برقرار می‌کنند و هیچ مدیریت متمرکز و زیر ساخت شبکه‌ای ثابتی در آن موجود نمی‌باشد به عبارت دیگر این شبکه‌ها فاقد زیرساخت ارتباطی می‌باشند. هر گره در یک شبکه‌ی موردی بایستی قادر باشد مانند یک مسیریاب برای ارسال بسته‌ها عمل کند[۱] نودها به طور مستقیم بدون هیچگونه نقطه دسترسی با همدیگر ارتباط برقرار می‌کنند و سازمان ثابتی ندارند و بنابراین در یک توپولوژی دلخواه شکل گرفته‌اند. هر نودی مجهز به یک فرستنده و گیرنده می‌باشد. مهم‌ترین ویژگی این شبکه‌ها وجود یک توپولوژی پویا و متغیر می‌باشد که نتیجه‌ی تحرک نودها می‌باشد. نودها در این شبکه‌ها به طور پیوسته موقعیت خود را تغییر می‌دهند که این خود نیاز به یک پروتکل مسیریابی که توانایی سازگاری با این تغییرات را داشته، نمایان می‌کند. مسیریابی و امنیت در این شبکه از چالش‌های امروز این شبکه هاست. در مسیریابی در برخی از کاربردهای شبکه‌های موردی، نوع سخت‌افزار محدودیت‌هایی را بر شبکه اعمال می‌کند که باید در انتخاب روش مسیریابی مد نظر قرار بگیرند ازجمله اینکه منبع تغذیه در گره‌ها محدود می‌باشد و در عمل، امکان تعویض یا شارژ مجدد آن مقدور نیست؛ لذا روش مسیریابی پیشنهادی در این شبکه‌ها بایستی از انرژی موجود به بهترین نحو ممکن استفاده کند یعنی باید مطلع از منابع گره باشد و اگر گره منابع کافی نداشت بسته را به آن گره برای ارسال به مقصد نفرستد.

۱-۲-۱- انواع شبکه‌های موردی

شبکه‌های حسگر هوشمند : متشکل از چندین حسگر هستند که در محدوده جغرافیایی معینی قرار گرفته‌اند. هر حسگر دارای قابلیت ارتباطی بی سیم و هوش کافی برای پردازش سیگنال‌ها و امکان شبکه سازی است.

شبکه‌های موردی متحرک: مجموعه مستقلی شامل کاربران متحرک است که از طریق لینک‌های بی سیم با یکدیگر ارتباط برقرار می‌کنند. برای اتفاقات غیر قابل پیش بینی، اتصالات و شبکه‌های متمرکز کارا نبوده و قابلیت اطمینان کافی را ندارند. لذا شبکه‌های موردی متحرک راه حل مناسبی است، گره‌های واقع در شبکه‌های موردی متحرک مجهز به گیرنده و فرستنده‌های بی سیم بوده و از آنتن‌هایی استفاده می‌کنند که ممکن است از نوع همه‌پخشی و یا نقطه به نقطه[1] باشند.

۱-۲-۲- کاربرد شبکه‌های موردی متحرک

کاربرد این شبکه‌ها در محیط‌های محاسباتی با استفاده از وسایل محاسباتی قابل حمل روز به روز در حال پیشرفت است. به طور کلی زمانی که زیرساختاری قابل دسترس نیست و ایجاد و احداث زیرساختار غیرعملی بوده و همچنین مقرون به صرفه نباشد، استفاده از شبکه‌ی موردی مفید است. از جمله این کاربردها می‌توان به موارد زیر اشاره نمود:

نمونه‌هایی از این کاربردها در ذیل آمده است:

---

[1] Point to Point

- تلفن‌های سلولی، کامپیوترهای کیفی، ساعت‌های مچی، ear phone
- محیط‌های نظامی
- محیط‌های غیرنظامی
- شبکه ترافیک شهری
- اتاق‌های ملاقات
- کاربردهای فوری
- عملیات جستجو و نجات
- بدست آوردن اطلاعات در حوادث بد و غیرمترقبه مانند وقوع بلایای طبیعی چون سیل و طوفان و زلزله
- محیط‌های علمی
- مانیتور کردن طبیعت مانند آتشفشان‌ها

۱-۲-۳- خصوصیات شبکه‌های موردی متحرک

شبکه‌های موردی متحرک با توجه به خاصیت بدون زیرساخت بودنشان و نیز محدودیت‌های منابع فیزیکی باچالش‌ها و موانع گوناگونی مواجه هستند[۲] که مهمترین آنها عبارتند از:

- رسانه‌ی بی سیم:

از آنجا که از رسانه‌ی بی سیم برای تبادل اطلاعات استفاده می‌شود، پایداری این ارتباط بسیار سست بوده، به گونه‌ای که وابسته به شرایط آب و هوا خواهد بود.

- محدودیت توان: گره‌های متحرک از توان محدود و کمی برخوردار می‌باشند بنابراین باید الگوریتم‌ها و پروتکل‌های طراحی شده برای این شبکه‌ها، تا حد امکان توان کمتری مصرف کنند.
- نبود زیرساخت ثابت ارتباطی: بدون وجود زیر ساخت شبکه، برقراری و مدیریت ارتباطات شبکه‌ها کار دشواری خواهد بود. این شکاف در طراحی پروتکل‌ها، باید بگونه‌ای پوشش داده شود.
- نبود مدیریت متمرکز: در شبکه‌های موردی هیچ سیستم یا سرور متمرکزی وجود ندارد. بنابراین جهت ارائه‌ی سرویس‌های مختلف باید از روش‌های توزیع شده استفاده شود که این امر چالش‌های خاص خود را به همراه دارد. برای مثال باید راه حل مناسبی برای مسائلی چون گرسنگی[۱]، بن‌بست[۲] و ... ارائه شود.
- تحرک گره‌ها: گره‌ها در شبکه‌های موردی، متحرک می‌باشند و بنابراین توپولوژی این شبکه‌ها به طور دائم در حال تغییر است. از این رو باید این مشخصه در طراحی پروتکل‌ها لحاظ شود.

---

[1] Starvation

[2] Deadlock

- امنیت: این نوع شبکه‌ها علاوه بر مشکلات امنیتی شبکه‌های سیمی، چالش‌های امنیتی مختص شبکه‌های بی‌سیم را نیز دارند در حالیکه بسیاری از راهکارهای امنیتی در شبکه‌های سیمی به علت محدودیت‌هایی که در بالا آمده است قابل پیاده سازی نیستند.

۱-۳- امنیت در شبکه‌های موردی سیار

مشکلات امنیتی در شبکه‌های موردی از آن جهت خاص شده و جداگانه مورد بررسی قرار می‌گیرد که در این شبکه‌ها، علاوه بر این که تمامی مشکلات موجود در یک شبکه‌ی با سیم وجود دارد، مشکلات بیشتری نیز دیده می‌شود. از آنجا که تمامی ارتباطات به صورت بی سیم انجام می شوند، می‌توان اطلاعات رد و بدل شده را به آسانی شنود کرد و یا تغییر داد. همچنین از آنجایی که خود گره‌ها در عمل مسیریابی شرکت می کنند، وجود یک گره‌ی متخاصم می‌تواند به نابودی شبکه بیانجامد. از طرفی پیاده سازی راه کارهای امنیتی که برای شبکه‌های سیمی طراحی شده‌اند برای شبکه‌های موردی مشکل و در برخی موارد غیر ممکن است. برای مثال تصور یک واحد توزیع کلید و یا زیرساخت کلید عمومی و غیره مشکل است. زیرا این شبکه‌ها اغلب بدون برنامه‌ریزی قبلی ایجاد می‌شوند و نیز بدون زیر ساخت بودن این شبکه‌ها مدیریت کلیدها را مشکل می‌سازد. از این رو امنیت در این شبکه‌ها به صورت جداگانه مورد بحث و بررسی قرار می گیرد.

به طوری کلی می‌توان مسائل امنیتی در شبکه‌های موردی را به صورت زیر دسته‌بندی نمود:

مدیریت کلیدهای رمزنگاری

مسیریابی امن

تصدیق اصالت پیام

جلوگیری از حملات ممانعت از سرویس

تشخیص سوء رفتار

تشخیص نفوذ

۱-۴- انگیزه پایان‌نامه

کاربردهای حساس شبکه‌های موردی سیار مانند کاربردهای نظامی، اهمیت امنیت در این شبکه‌ها را دوچندان می‌کند و مسیریابی امن یکی از ملزومات برقراری امنیت در این شبکه‌ها محسوب می‌شود زیرا اگر گره غیر مجازی توانایی اخلال در فرایند مسیریابی به نفع خود را داشته باشد در اینصورت می‌توان گفت که امنیت شبکه را در مخاطره انداخته است.

در حمله‌ی سوراخ سیاه گره متخاصم با استفاده از ترفندهایی یک مسیر کاذب را به عنوان مسیر بهینه معرفی کرده و از این طریق سعی در جذب بسته‌های داده به سمت خود می‌کند و بدین صورت از رساندن بسته‌های داده به مقصد جلوگیری کرده و کارایی شبکه را به شدت تحت تاثیر قرار می‌دهد. بنابراین ممانعت از این حمله، بخصوص در شبکه‌هایی با کاربردهای حساس یک امر مهم تلقی می‌شود.

پروتکل مسیریابی AODV یکی از پرکاربردترین پروتکل‌های مسیریابی در شبکه‌های موردی سیار است که به شدت در مقابل حمله‌ی سوراخ سیاه دچار ضعف است و با توجه اهمیت این پروتکل، امن نمودن آن

در مقابل این حمله یکی از ملزومات حفظ کارایی این پروتکل در شبکه است که انگیزه‌ی اصلی این پایان‌نامه را به وجود آورده است.

۱-۴-۱- اهداف پایان نامه

هدف از این پایان‌نامه ارائه روشی جهت امن نمودن پروتکل مسیریابی AODV در مقابل حمله‌ی سوراخ سیاه است. در این روش، مکانیزمی جهت شناسایی حمله طراحی و پیاده سازی شده است و نیز سعی شده تا روش پیشنهادی کمترین سربار را در شبکه داشته باشد و با کمترین هزینه در معیارهایی همچون تاخیر در شبکه، سطح بالایی از مقاومت در مقابل این حمله ایجاد کند. همچنین در طراحی مکانیزم، حفظ نقاط قوت پروتکل مسیریابی AODV در نظر گرفته شده است.

۱-۴-۲- ساختار پایان نامه

در فصل دو ابتدا به مفاهیم اساسی که مبنای پروتکل پیشنهادی هستند همچون مسیریابی در شبکه‌های موردی، پروتکل مسیریابی AODV و و نحوه‌ی عملکرد گره متخاصم برای اجرای حمله‌ی سوراخ سیاه پرداخته شده است. در فصل سوم به تحقیقات انجام شده در زمینه‌ی جلوگیری از حمله‌ی سوراخ سیاه اشاره شده و در نهایت نقاط ضعف و قوت این تحقیقات بررسی انجام گرفته است.

در فصل چهارم ابتدا به بیان ایده اصلی پروتکل پیشنهادی پرداخته شده است و در ادامه به نحوه‌ی طراحی و پیاده‌سازی این پروتکل پرداخت خواهد شد و در نهایت با بررسی سناریوهای مختلف حمله سوراخ سیاه، مقاومت روش پیشنهادی از جنبه تئوریک بررسی می‌شود.

نهایتا فصل پنجم به شبیه سازی روش پیشنهادی و تحلیل نتایج حاصل از آن می‌پردازد و در پایان پیشنهاداتی برای ادامه کار ارائه خواهد شد.