
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

امنیت مسیریابی در شبکه‌های بی‌سیم اقتضایی

پایان‌نامه کارشناسی ارشد مهندسی برق - مخابرات

محمد فنایی

استاد راهنما

دکتر مهدی برنجکوب

بهار ۱۳۸۷

دانشگاه صنعتی اصفهان

دانشکده برق و کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی برق - مخابرات آقای محمد فنایی

تحت عنوان

امنیت مسیریابی در شبکه‌های بی‌سیم اقتضایی

در تاریخ ۱۳۸۷/۴/۱ توسط کمیته تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان‌نامه	دکتر مهدی برنجکوب
۲- استاد مشاور پایان‌نامه	دکتر مسعود رضا هاشمی
۳- استاد داور	دکتر حسین سعیدی
۴- استاد داور	دکتر پژمان خدیوی
سرپرست تحصیلات تکمیلی دانشکده	دکتر علی‌محمد دوست‌حسینی

تشکر و قدردانی

حمد، سپاس و ستایش بی حد خدای متعال را که بار دیگر مرا مرهون الطاف بی بدیل و بی کران خود قرار داد و در مسیر تعالی قدمی دیگر، همنون شدم و دریچه‌ای تازه از علم و دانش را در برابر من گشود. با بهره وجود با خضوع و خشوع، خداوند منان بی نیاز را شاکرم و سر به آستان پر مهرش می سایم برای هر آنچه به لطف و رحمت خویش به من ارزانی داشته و هر آنچه به حکمت خویش از من دریغ کرده است.

اکنون که توانسته‌ام به یاری ذات پاک حق تعالی و در سایه خوان الطاف گسترده‌اش مقطعی دیگر از تحصیلاتم را پشت سر گذاشته و قدمی دیگر در راستای اعتلای خود و جامعه‌ام بردارم بر خود واجب می دانم مراتب تشکر، تقدیر و امتنان قلبی خود را از تمامی کسانی که به هر نحو ممکن و به هر میزان همراه، یاریگر و مشوق من بوده‌اند و طی این طریق سراسر پر مخاطره را مرهون وجود، تلاش، کمک و محبت های بی شائبه آنها هستم، اعلام دارم.

پیش از هر کس لازم است از اعضای محیط سراسر پر مهر خانواده‌ام و به ویژه از پدر و مادر عزیز و گرامی‌ام که نه تنها در این مقطع، که در تمامی مراحل زندگی یار، همراه، پشتیبان و مشوقم بوده‌اند و همواره با همیاری کردن شرایطی مساعد، زمینه رشد، تعالی و بالندگی مرا فراهم ساخته‌اند، خاضعانه و خاشعانه تشکر و سپاسگزاری نمایم. پدر و مادر بزرگوارم بزرگترین معلمان زندگی‌ام بوده‌اند و با وجود همه سختی ها، مشکلات و رنج های طاقت فرسای خویش لحظه‌ای چهره گشاده و لبخند پر مهر و امید بخش خویش را از من دریغ ننموده‌اند. به درگاه حضرت باری تعالی چشم امید دوخته‌ام که همواره مراقبردان این عزیزان قرار دهد و راه و رسم خاکساری، تواضع و فروتنی در برابر مقام، منزلت و عظمت روحی ایشان را به من بیاموزد و توفیق خدمتگزاری شایسته ایشان را از درگاه لطف و کرم لایزال خویش به این بنده کمترین عطا فرماید.

در کلیه مراحل تحقیق و تدوین این پایان نامه از کمک و راهنمایی اساتید ارجمند و بزرگواری برخوردار بوده‌ام که لازم است مراتب قدردانی و تشکر خالصانه خود را نسبت به آنان ابراز دارم. از آقای دکتر مهدی برنجکوب، استاد راهنمای پایان نامه که در طی این مدت نظرات سودمند ایشان حلال مشکلات فراوان بود، کمال تشکر و تقدیر قلبی را دارم. بی شک بدون راهنمایی های ارزنده و پیگیری های مداوم ایشان، انجام این پایان نامه میسر نبود. امید آن دارم که شایسته زحمات همیشگی ایشان بوده باشم و روزی بتوانم به نحو شایسته جبران گوشه‌ای از محبت های بی دریغ ایشان را نمایم. از آقای دکتر مسعود رضا هاشمی، استاد مشاور پایان نامه که در تدوین هر چه بهتر این پایان نامه از راهنمایی های ارزشمند ایشان استفاده بسیار نمودم، سپاسگزاری و قدردانی می نمایم. همچنین، از آقایان دکتر حسین سعیدی و دکتر پژمان خدیوی که زحمت داوری این پایان نامه را متقبل شدند و با حضور در جلسه دفاع از پایان نامه، نکات مفیدی را یادآوری نمودند، تشکر می کنم.

از همه اساتید محترمی که در طول بیش از شش سال تحصیل در دانشگاه صنعتی اصفهان از محضر پر فیض ایشان بهره فراوان بردم و همه اندوخته علمی خود را مرهون تلاش خستگی ناپذیر و از خودگذشتگی زاید الوصف ایشان هستم، کمال تشکر و سپاسگزاری را می نمایم و برای ایشان آرزوی موفقیت روز افزون می کنم.

از آقای مهندس علی فانیان به خاطر همراهی و مساعدت های همیشگی ایشان در طول مدت انجام این پایان نامه سپاس فراوان دارم. مراحل اولیه انجام این پایان نامه مرهون پیگیری ها و مشارکت ایشان در جلسات بحث و تبادل نظر گروهی بود. آرزومند توفیق و موفقیت همیشگی ایشان در همه مراحل زندگی هستم.

از همه دوستان ارجمند و بزرگوارم که دوران تحصیل در این دانشگاه را به دوره‌ای سرشار از نشاط، شادابی و خاطره تبدیل نمودند، صمیمانه تشکر می کنم. همراهی با این عزیزان، این دوره را به یکی از بهترین و پر خاطره ترین دوره های زندگی‌ام مبدل ساخته است. صفحه ذهنم همواره منقش به خاطرات شیرین این عزیزان خواهد بود. سرفرازی، شادکامی، پیروزی و موفقیت روز افزون این عزیزان، آرزوی همیشگی من است.

محمد فانی، دانشگاه صنعتی اصفهان، تیرماه ۱۳۸۷

هر آبروی که اندوختم ز دانش و دین　　نثار خاک ره آن نگار خواهم کرد

آنان که آفتاب را به زندگی دیگران ارزانی می دارند، نمی توانند خود از آن بی بهره باشند.

تقدیم به

پدر و مادر عزیز و مهربانم

آنان که راستی قامتم در شکستگی قامتشان تجلی یافته است

در برابر وجود گرامیشان زانوی ادب بر زمین می نهم و با دلی سرشار از عشق و محبت بر دستان پر مهرشان بوسه می زنم.

فهرست مطالب

عنوان **صفحه**

فصل ششم: ارتقای عملکرد پردازشی پروتکل مسیریابی امن ARAN

فصل هفتم: نتیجه‌گیری

فهرست شکل‌ها

عنوان **صفحه**

فهرست اختصارات

A

Access Point ..... AP
Ad hoc On-demand Distance Vector routing ..... AODV
Authenticated Routing for Ad hoc Networks ..... ARAN

C

Carrier Sense Multiple Access ..... CSMA
Certificate Authority ..... CA
Clear To Send ..... CTS

D

Denial of Service ..... DoS
Destination-Sequenced Distance Vector routing ..... DSDV
Destination-Sequenced Distance Vector routing - Sequence number ..... DSDV-SQ
Distance Routing Effect Algorithm for Mobility ..... DREAM
Dynamic Source Routing ..... DSR

G

Global Positioning System ..... GPS
Greedy Face Greedy ..... GFG
Greedy Perimeter Stateless Routing ..... GPSR

I

Institute of Electrical and Electronics Engineering ..... IEEE
Internet Control Message Protocol ..... ICMP
Internet Engineering Task Force ..... IETF
Intrusion Detection System ..... IDS
IP Security protocol ..... IPSec

K

Key Distribution Center ..... KDC
Keyed-Hashing for Message Authentication Code ..... HMAC

L

Link State Advertisement ..... LSA
Link State Update ..... LSU
Location Aided Routing ..... LAR

M

Medium Access Control ..... MAC
Message Authentication Code ..... MAC/HashMAC
Message Digest ..... MD
Mobile Ad Hoc Network ..... MANET
Most Forward within Radius ..... MFR

N

Nearest with Forward Progress ..... NFP

O

On-Demand Source routing with Byzantine Robustness ……. ODSBR
Optimized Link-State Routing ……..... OLSR

P

Public Key Infrastructure …… PKI

Q

Quality of Service ……... QoS

R

Request To Send …… RTS
Route Discovery Packet ……..... RDP
Route Error ……..... RERR
Route Reply ……..... RREP
Route Request ……..... RREQ

S

Secure Ad hoc On-demand Distance Vector routing ……..... SAODV
Secure Dynamic Source Routing …… SDSR
Secure Efficient Distance vector routing …… SEAD
Secure Hash Algorithm ……. SHA
Secure Link State routing Protocol ……..... SLSP
Secure Routing Protocol ……..... SRP
Security Association ……. SA
Security Aware ad hoc Routing ……. SAR

T

TESLA with Instant Key disclosure ……... TIK
TESLA with Instant Key disclosure ARAN ……... TIKARAN
Time Division Multiple Access ……..... TDMA
Time To Live ……. TTL
Timed Efficient Stream Loss-tolerant Authentication ……..... TESLA
Trusted Third Party …… TTP
Tunneling Resistant endairA ……... TRendairA

W

Wireless Local Area Network …… WLAN

چکیده

مسیریابی چندگامی را می‌توان به عنوان یکی از اساسی‌ترین پروتکل‌های مورد نیاز برای برپایی یک شبکه بی‌سیم اقتضایی در نظر گرفت. به منظور غلبه بر مشکلات ناشی از حرکت گره‌ها و امکان تغییر مکرر توپولوژی شبکه، طبیعت توزیع شده و همچنین عدم اتکای شبکه بی‌سیم اقتضایی به زیرساختار متمرکز از پیش طراحی شده، پروتکل‌های مسیریابی متعددی جهت استفاده در این شبکه‌ها پیشنهاد گردیده‌اند. طراحان این پروتکل‌ها، با فرض کانال بی‌سیم امن و بر مبنای همکاری کامل گره‌های قابل اعتماد در اجرای پروتکل‌های مورد نظر، تمام تلاش خود را به ارتقای عملکرد آنها در یافتن هرچه سریع‌تر بهترین مسیر بین مبدأ و مقصد ضمن نیاز به کمترین تعداد ممکن پیام‌های مسیریابی و استفاده از حداقل منابع شبکه معطوف داشته‌اند. با این وجود، در عمل فرضیات مذکور در یک شبکه بی‌سیم اقتضایی، چندان معتبر نیستند. در حقیقت، در چنین شبکه‌ای، وجود گره‌های دشمن که قصد دارند از درون یا بیرون شبکه، عملکرد عادی پروتکل مسیریابی را مختل سازند یا به منظور حفظ منابع محدود انرژی خود، از همکاری کامل با دیگر گره‌های موجود در شبکه سر باز زنند، موجب می‌شود این پروتکل‌ها در معرض تهدید جدی قرار گیرند. از سوی دیگر، با در نظر گرفتن کاربردهای خاص شبکه‌های بی‌سیم اقتضایی، که به طور عمده در محیط‌های نظامی و عملیات‌های امداد و نجات در مناطق فاجعه زده و دور افتاده فاقد زیرساختارهای مرسوم در شکل‌گیری دیگر انواع شبکه‌های بی‌سیم به کار گرفته می‌شوند، تضمین امنیت مسیریابی در این شبکه‌ها حایز اهمیت فراوان است. در این پایان‌نامه، با بررسی امنیت مسیریابی در شبکه‌های بی‌سیم اقتضایی، روش‌های امن‌سازی پروتکل‌های مسیریابی در این شبکه‌ها مورد بررسی دقیق قرار گرفته‌اند. در این راستا، اهم پروتکل‌های مسیریابی امن پیشنهاد شده مطالعه و ارزیابی گردیده‌اند و عملکرد آنها در دستیابی به اهداف امنیتی مورد نظر، ارتقا یافته است. به طور خاص، در این پایان‌نامه اثبات شده است که بر خلاف ادعاهای قبلی مبنی بر امنیت اثبات‌پذیر پروتکل مسیریابی امن endairA به عنوان یکی از امن‌ترین پروتکل‌های مسیریابی امن مبتنی بر مبدأ، این پروتکل نسبت به حمله تونل آسیب‌پذیر است. همچنین، یک مکانیزم امنیتی جدید جهت پیشگیری از اجرای موفقیت‌آمیز حمله تونل علیه پروتکل‌های مسیریابی مورد استفاده در شبکه‌های بی‌سیم اقتضایی و به طور خاص پروتکل endairA، ارائه گردیده است. به کار گیری این مکانیزم امنیتی در پروتکل endairA، منجر به تدوین نسخه ارتقا یافته مقاوم نسبت به حمله تونل این پروتکل، TRendairA، شده است. در بخش دیگری از این پایان‌نامه پیشنهاد شده است در پروتکل مسیریابی امن ARAN، به عنوان یکی از امن‌ترین پروتکل‌های مسیریابی مبتنی بر بردار فاصله، برای احراز اصالت گره‌های میانی قرار گرفته بین مبدأ و مقصد، به جای امضای دیجیتال از پروتکل احراز اصالت همه‌پخشی TIK استفاده شود. چون پروتکل TIK بر مبنای محاسبه سریع و کم هزینه توابع رمزنگاری کلید متقارن استوار است، استفاده از آن در پروتکل ARAN می‌تواند سربار محاسباتی و پردازشی این پروتکل را به میزان قابل ملاحظه کاهش دهد. با در نظر گرفتن محدودیت‌های محاسباتی، پردازشی و انرژی محدود گره‌های موجود در یک شبکه بی‌سیم اقتضایی، ارتقای عملکرد پردازشی پروتکل ARAN می‌تواند زمینه پیاده‌سازی هرچه کم هزینه‌تر و گسترده‌تر این پروتکل مسیریابی امن اثبات‌پذیر در شبکه‌های بی‌سیم اقتضایی را فراهم کند.

فصل اول

مقدمه

۱-۱ مقدمه

شبکه بی‌سیم اقتضایی[۱] مجموعه‌ای از گره‌های بی‌سیم است که بدون کمک هرگونه زیرساختار متمرکز از پیش برپا شده و تنها به کمک یکدیگر، آن شبکه را شکل می‌دهند. در چنین شبکه‌ای، گره‌ها به خودی خود و عمدتاً از طریق استفاده از الگوریتم‌های کنترلی توزیع شده، عملیات‌های کنترلی و شبکه‌ای مورد نیاز برای برپایی شبکه را انجام می‌دهند. مشخصات و ویژگی‌های منحصر به فرد شبکه‌های بی‌سیم اقتضایی، از یک سو تلاش در جهت گسترش روز افزون به کارگیری آنها در برقراری ارتباطات بی‌سیم کاربران، به ویژه کاربران متحرک، را تشدید کرده است و از سوی دیگر، طراحی پروتکل‌های کارآمد مورد نیاز برای تسهیل پیاده‌سازی گسترده آنها را برای محققین دشوار ساخته است. از جمله مهمترین ویژگی‌های این نوع شبکه‌ها که گسترش به کارگیری آنها را در کاربردهای مختلف در پی داشته است آن است که می‌توان آنها را برای کاربردهای خاص طراحی و پیاده‌سازی نمود و همچنین، می‌توان آنها را با استفاده از هر نوع گره شبکه که در اختیار باشد، تشکیل داد. علاوه بر آن، پیاده‌سازی چنین شبکه‌هایی هزینه نصب و نگهداری زیرساختار متمرکز کنترل کننده گره‌های شبکه را مرتفع می‌سازد و برپایی و پیکربندی مجدد آنها را تسریع و تسهیل می‌کند. همچنین، شبکه‌های بی‌سیم اقتضایی به دلیل طبیعت توزیع شده، افزونگی گره‌ها و نداشتن یک نقطه‌ی اتکای تنها، نسبت به از کار افتادگی بسیار مقاوم می‌باشند. در عین حال، هر یک از ویژگی‌های فوق را می‌توان به عنوان یک محدودیت در طراحی پروتکل‌های کارآمد جهت کنترل اینگونه شبکه‌ها در نظر گرفت.

---

[۱] Wireless ad hoc network

محدودیت منابع انرژی و منابع پردازشی و محاسباتی گره‌های متحرک شبکه، تغییر مکرر توپولوژی شبکه به دلیل پیوستن و جدا شدن مکرر گره‌ها و پیچیدگی مدیریت عملیات‌های کنترلی و شبکه‌ای چنین ساختار پویا و متحرکی بدون تکیه بر یک زیرساختار کنترلی متمرکز در شبکه را می‌توان از جمله مهمترین موانع و محدودیت‌های موجود بر سر راه محققین در طراحی پروتکل‌های کارآمد مورد نیاز برای تسهیل پیاده‌سازی گسترده اینگونه شبکه‌ها برشمرد.

با گذشت زمان و جهت‌گیری بخش قابل توجهی از فعالیت‌های گروه‌های مختلف تحقیقاتی به سمت طراحی، ارزیابی، توسعه، بهینه‌سازی و پیاده‌سازی پروتکل‌های مورد نیاز در ارتقای عملکرد شبکه‌های بی‌سیم اقتضایی، بستری مناسب جهت فراگیر شدن هرچه بیشتر کاربرد این شبکه‌ها در حیطه‌های مختلف، فراهم گردیده است. از جمله مهمترین این کاربردها می‌توان به پیاده‌سازی‌های گسترده شبکه‌های بی‌سیم اقتضایی در میدان‌های نبرد، عملیات‌های امداد و نجات در مناطق مصیبت‌زده، کاربردهای تجاری در مناطق دور افتاده‌ای که امکان نصب و نگهداری زیرساختارهای مرسوم در شکل‌گیری دیگر انواع شبکه‌های بی‌سیم وجود ندارد، کاربردهایی در برپایی شبکه‌های بی‌سیم موقتی و غیردائمی به منظور فراهم کردن امکان برقراری ارتباط بی‌سیم شرکت کنندگان در کنفرانس‌ها، مجامع علمی و فعالیت‌های تفریحی، شبکه‌های بی‌سیم حسگر، شبکه‌های خودرویی و ده‌ها کاربرد دیگر، اشاره کرد.

یکی از مهمترین پروتکل‌های مورد نیاز برای برپایی و فراهم کردن امکان مدیریت و کنترل مؤثر و کارآمد یک شبکه کامپیوتری، مسیریابی است. در حقیقت، مسیریابی به عنوان یکی از ارکان اساسی شکل‌گیری یک شبکه بی‌سیم اقتضایی در نظر گرفته می‌شود. به دلیل اهمیت فراوان و تأثیر عمده مسیریابی بر عملکرد یک شبکه بی‌سیم اقتضایی و نقش تأثیرگذاری که مسیریابی در شکل‌گیری و دوام برپایی چنین شبکه‌ای ایفا می‌کند، بخش گسترده‌ای از تحقیقات بر روی این شبکه‌ها به سمت طراحی، ارزیابی، ارتقا و بهینه‌سازی پروتکل‌های مسیریابی خاص جهت غلبه بر مشکلات منحصر به فرد این شبکه‌ها تخصیص یافته است. به دلیل همین ویژگی‌های منحصر به فرد شبکه‌های بی‌سیم اقتضایی، مسیریابی در این شبکه‌ها به صورت چندگامی انجام می‌شود. در این نوع مسیریابی، گره‌های میانی موجود در مسیر بین مبدأ و مقصد، با همکاری با یکدیگر، بسته‌ها را به سمت مقصد نهایی آنها هدایت می‌نمایند و بدین ترتیب، گذردهی[1] و بازده توانی شبکه را بهبود می‌بخشند.

به منظور غلبه بر مشکلات ناشی از حرکت گره‌ها و امکان تغییر مکرر توپولوژی شبکه در شبکه‌های بی‌سیم اقتضایی متحرک و همچنین عدم اتکای شبکه بی‌سیم اقتضایی به زیرساختار متمرکز از پیش طراحی شده، پروتکل‌های مسیریابی متعددی جهت استفاده در این شبکه‌ها پیشنهاد گردیده‌اند. طراحان این پروتکل‌ها، با فرض کانال بی‌سیم امن و بر مبنای همکاری کامل گره‌های قابل اعتماد در اجرای پروتکل‌های مورد نظر، تمام تلاش خود را به ارتقای عملکرد آنها معطوف داشته‌اند. این ارتقای عملکرد در زمینه‌های مختلف از قبیل یافتن هرچه سریع‌تر بهینه‌ترین مسیر بین مبدأ و مقصد (بر اساس معیار بهینگی مورد نظر در طراحی آن پروتکل)، نیاز به کمترین تعداد ممکن پیام‌های مسیریابی و استفاده از حداقل منابع شبکه (از قبیل انرژی مصرفی، توان محاسباتی پردازنده، حافظه، پهنای باند شبکه و

[1] Throughput

غیره) مد نظر بوده است. از جمله مهمترین پروتکل‌های مسیریابی مورد استفاده در شبکه‌های بی‌سیم اقتضایی می‌توان پروتکل‌های DSR[۱] [۱]، AODV[۲] [۲] و DSDV[۳] [۳] را نام برد.

در عمل فرض کانال بی‌سیم امن و همکاری کامل گره‌های قابل اعتماد در اجرای پروتکل‌های مسیریابی مورد استفاده در یک شبکه بی‌سیم اقتضایی، فرض معتبری نمی‌باشد. در حقیقت، در چنین شبکه‌ای، وجود گره‌های دشمن که قصد دارند از درون یا بیرون شبکه عملکرد عادی پروتکل مسیریابی را مختل سازند یا با کسب اطلاعات اضافی از پیام‌های کنترلی مبادله شده بین گره‌های شبکه، در جهت از کار اندازی آن اقدام کنند، موجب می‌شود این پروتکل‌های مسیریابی که در حقیقت رکن اساسی برپایی چنین شبکه‌ای هستند، در معرض تهدید جدی حمله گره‌های دشمن قرار گیرند. از سوی دیگر، با در نظر گرفتن کاربردهای خاص شبکه‌های بی‌سیم اقتضایی، که به طور عمده در محیط‌های نظامی یا عملیات‌های امداد و نجات در مناطق فاجعه زده و دور افتاده‌ی فاقد زیرساختارهای مرسوم در شکل‌گیری دیگر انواع شبکه‌های بی‌سیم به کار گرفته می‌شوند، تضمین امنیت مسیریابی در این شبکه‌ها حایز اهمیت فراوان است.

در این پایان‌نامه هدف آن است که با بررسی امنیت مسیریابی در شبکه‌های بی‌سیم اقتضایی، روش‌های امن‌سازی پروتکل‌های مسیریابی در این شبکه‌ها مورد بررسی دقیق قرار گیرند، پروتکل‌های مسیریابی امن پیشنهاد شده جهت استفاده در آنها مطالعه و ارزیابی گردند و عملکرد آنها در دستیابی به اهداف امنیتی مورد نظر، ارتقا یابد. در ادامه این فصل، ابتدا در بخش ۱-۲ مروری بر اهم تحقیقات انجام شده در حوزه امنیت مسیریابی شبکه‌های بی‌سیم اقتضایی ارائه خواهد شد و مهمترین نوآوری‌های پیشنهادی در این پایان‌نامه به اختصار تبیین خواهد گردید. سپس در بخش ۱-۳، ضمن تشریح ساختار پایان‌نامه، رئوس کلی مطالب مورد بررسی در فصل‌های آینده معرفی خواهد شد.

۱-۲ مروری بر کارهای انجام شده و اهم نوآوری‌های پایان‌نامه

با در نظر گرفتن عدم وجود یک زیرساختار متمرکز کنترل کننده شبکه بی‌سیم اقتضایی و نیز آزادی عمل نسبی گره‌های مختلف در پیوستن به شبکه و جدا شدن از آن و با عنایت به کاربردهای خاص این نوع شبکه، امکان وجود گره‌های بد رفتار در شبکه بی‌سیم اقتضایی بسیار محتمل و غیر قابل انکار می‌باشد. گره‌های بد رفتار موجود در چنین شبکه‌ای یا از طریق عدم تبعیت از اصول کلی حاکم بر اجرای پروتکل مسیریابی مورد استفاده در آن و اعمال تغییرات متخاصمانه در جهت سوء استفاده از آنها، در صدد مختل ساختن عملکرد عادی آن پروتکل مسیریابی هستند و قصد دارند از این طریق شبکه مذکور را از کار بیندازند و یا به منظور حفظ منابع محدود انرژی خود، از همکاری کامل با دیگر گره‌های موجود در شبکه بر اساس آن پروتکل مسیریابی سر باز می‌زنند و بدین ترتیب، امکان سرویس‌دهی شبکه به برخی کاربران آن را از بین می‌برند. این عملکرد گره‌های بد رفتار موجود در شبکه بی‌سیم اقتضایی باعث می‌شود پروتکل مسیریابی که بر مبنای همکاری کامل گره‌های قابل اعتماد در اجرای آن پروتکل طراحی گردیده‌است، کارآیی خود را از دست بدهد و عملکرد عادی آن شبکه به کلی مختل شود.

---

[۱] Dynamic Source Routing (DSR)
[۲] Ad hoc On-demand Distance Vector (AODV)
[۳] Destination–Sequenced Distance Vector (DSDV)

با در نظر گرفتن ملاحظات فوق و به دنبال آشکار شدن ضعف‌های اساسی پروتکل‌های مسیریابی پیشنهادی جهت استفاده در شبکه‌های بی‌سیم اقتضایی در مقابله با خرابکاری‌های گره‌های بد رفتار موجود در این شبکه‌ها، از آخرین سال‌های دهه ۱۹۹۰ میلادی، تحقیقات گسترده‌ای در راستای افزایش امنیت این پروتکل‌ها آغاز شده است. بیشتر تحقیقات انجام شده در این زمینه با هدف تغییر و دستکاری پروتکل‌های مسیریابی پایه مورد استفاده در شبکه‌های بی‌سیم اقتضایی و افزودن قابلیت‌های امنیتی خاص به آنها به منظور دشوارتر نمودن و یا غیرممکن ساختن انجام عملیات‌های خرابکارانه و یا عدم تبعیت از اصول کلی حاکم بر پروتکل‌های مذکور از سوی گره‌های بد رفتار مورد نظر، صورت پذیرفته است. در حقیقت، طراحان پروتکل‌های مسیریابی امن پیشنهادی جهت استفاده در این شبکه‌ها به دنبال آن بوده‌اند که به پروتکل‌های مسیریابی پایه مورد استفاده در آنها قابلیت‌هایی اضافه کنند که گره‌های شبکه را از عدم تبعیت و سوء استفاده از پیام‌ها و پردازش‌های تعریف شده در طرح کلی آن پروتکل‌ها باز دارند. بدیهی است ارتقای امنیتی پروتکل‌های مسیریابی مورد استفاده در شبکه‌های بی‌سیم اقتضایی مستلزم به کار گیری ابزارهای رمزنگاری و پروتکل‌های امنیتی در آنها است که می‌تواند منجر به افزایش تعداد پیام‌های کنترلی مبادله شده بین گره‌های موجود در شبکه، افزایش سربار ارتباطی تحمیل شده بر شبکه، افزایش سربار محاسباتی و پردازشی تحمیل شده به گره‌های شبکه، افزایش تأخیر در یافتن مسیر بین دو گره ارتباط برقرار کننده موجود در شبکه، افزایش تأخیر در تحویل بسته‌های داده ارسالی آنها و به طور کلی، تنزل عملکرد پروتکل مسیریابی پایه در آن شبکه شود؛ با این وجود، در صورتی که در یک شبکه بی‌سیم اقتضایی در بر گیرنده گره‌های بد رفتار، از این پروتکل‌های امنیتی استفاده نشود، تنزل کیفیت عملکرد پروتکل مسیریابی مورد استفاده در حضور گره‌های بد رفتار بسیار بیشتر از تنزل کیفیت آن ناشی از به کار گیری ابزارهای رمزنگاری و پروتکل‌های امنیتی خواهد بود و در عین حال، اطلاعات حیاتی رد و بدل شده بین گره‌های موجود در شبکه، و در حالت کلی‌تر، کل عملکرد و سرویس‌دهی عادی آن شبکه در معرض تهدید جدی فروپاشی قرار خواهد گرفت.

به منظور تأمین امنیت مسیریابی در شبکه‌های بی‌سیم اقتضایی، پروتکل‌های مسیریابی امن متعددی طراحی، تحلیل و ارزیابی گردیده‌اند. در [۴ و ۵] خلاصه‌ای از مهمترین این پروتکل‌ها به همراه فرضیات و دستاوردهای امنیتی آنها و نیز نقاط قوت و ضعف آنها، بیان گردیده است. به دلیل عدم امکان تشریح و ارزیابی نحوه عملکرد همه پروتکل‌های مسیریابی امن پیشنهادی جهت استفاده در شبکه‌های بی‌سیم اقتضایی در این پایان‌نامه، بر آن شدیم تا مهمترین و تأثیرگذارترین این پروتکل‌ها را به طور کامل مطالعه و ارزیابی کنیم و دستاوردهای امنیتی و عملکرد پردازشی آنها را در راستای نیل به بازده و کارایی بیشتر ارتقا دهیم. پروتکل‌های مسیریابی امن تشریح شده در این پایان‌نامه را می‌توان در سه گروه کلی زیر تقسیم‌بندی نمود:

- پروتکل‌های مسیریابی امن مبتنی بر پروتکل DSR [۱] که شامل پروتکل‌های SRP[۱] [۶]، Ariadne [۷] و endairA [۸] می‌باشد.

[۱] Secure Routing Protocol (SRP)

- پروتکل‌های مسیریابی امن مبتنی بر پروتکل AODV [۲] که شامل پروتکل‌های SAODV[۱] [۹] و ARAN[۲] [۱۰] می‌باشد.
- پروتکل‌های مسیریابی امن مبتنی بر پروتکل DSDV [۳] که شامل پروتکل‌های SEAD[۳] و SuperSEAD [۱۱] می‌باشد.

در کنار طراحی و ارائه پروتکل‌های مسیریابی امن مبتنی بر نسخه‌های پایه و ناامن پروتکل‌های مسیریابی مورد استفاده در شبکه‌های بی‌سیم اقتضایی و تحلیل و ارزیابی امنیت آنها بر مبنای مستندات و استنباط‌های شهودی و شبیه‌سازی، گروهی از محققین نیز تحلیل و ارزیابی امنیت محقق شده در این پروتکل‌ها با استفاده از روش‌های صوری[۴] و بر مبنای چارچوب‌های طراحی شده مدون برای چنین منظوری را دنبال کرده‌اند. به عنوان مثال، در [۸] و [۱۲] به ترتیب چارچوب‌های مشابهی برای تحلیل و ارزیابی منظم و دقیق میزان امنیت یک پروتکل مسیریابی امن مبتنی بر مبدأ و یک پروتکل مسیریابی امن مبتنی بر بردار فاصله، که در فصل دوم به طور کامل معرفی خواهند شد، ارائه شده است. بر این اساس می‌توان انتظار داشت برخی از پروتکل‌های مسیریابی امن طراحی شده برای استفاده در شبکه‌های بی‌سیم اقتضایی در مقایسه با سایرین به سطح بالاتری از امنیت دست یابند و در به چالش کشیدن گره‌های بد رفتار شبکه هنگام ایجاد اختلال در عملیات مسیریابی، عملکرد بسیار مطلوب‌تری داشته باشند. به عنوان مثال، در [۸] ادعا شده است پروتکل مسیریابی امن endairA بر مبنای چارچوب کلی تحلیل امنیت پروتکل‌های مسیریابی امن مبتنی بر مبدأ، امنیت آماری دارد. همچنین، در [۱۲] اثبات شده است پروتکل مسیریابی امن ARAN بر مبنای چارچوب کلی تحلیل امنیت پروتکل‌های مسیریابی امن مبتنی بر بردار فاصله، امنیت آماری دارد.

در این پایان‌نامه تلاش شده است امن‌ترین پروتکل‌های مسیریابی امن ارائه شده جهت استفاده در شبکه‌های بی‌سیم اقتضایی مورد بررسی، تحلیل و ارزیابی دقیق‌تر قرار گیرند و عملکرد آنها تا حد ممکن ارتقا یابد. به همین منظور، پروتکل‌های مسیریابی امن endairA و ARAN که به ترتیب به عنوان امن‌ترین پروتکل‌های مسیریابی از گروه پروتکل‌های مسیریابی امن مبتنی بر مبدأ و پروتکل‌های مسیریابی امن مبتنی بر بردار فاصله در نظر گرفته می‌شوند، انتخاب گردیده‌اند و عملکرد آنها از دیدگاه‌های مختلف ارتقا یافته است.

به طور خاص، در این پایان‌نامه اثبات خواهد شد بر خلاف ادعای نویسندگان [۸]، پروتکل مسیریابی امن endairA نسبت به حمله تونل آسیب‌پذیر است و توانایی مقابله با این حمله بسیار قدرتمند و تأثیر گذار بر از کار اندازی عملیات مسیریابی در شبکه‌های بی‌سیم اقتضایی را ندارد. همچنین، یک مکانیزم امنیتی جدید جهت پیشگیری از اجرای موفقیت‌آمیز حمله تونل علیه پروتکل‌های مسیریابی مورد استفاده در شبکه‌های بی‌سیم اقتضایی، و به طور خاص پروتکل endairA، ارائه خواهد گردید. به کار گیری این مکانیزم امنیتی بدیع در پروتکل endairA، منجر به تدوین نسخه ارتقا یافته مقاوم نسبت به حمله تونل این پروتکل، TRendairA[۵]، خواهد شد. تحلیل امنیتی ارائه شده

---

[۱] Secure Ad hoc On-demand Distance Vector routing(SAODV)
[۲] Authenticated Routing for Ad hoc Networks (ARAN)
[۳] Secure Efficient Ad hoc Distance vector routing (SEAD)
[۴] Formal methods
[۵] Tunneling Resistant endairA (TRendairA)

بر عملکرد و قابلیت‌های نسخه مقاوم نسبت به حمله تونل پروتکل مسیریابی امن endairA نشان می‌دهد که این پروتکل قادر است بخش عمده‌ای از حملات تونل تأثیر گذار بر عملکرد پروتکل مسیریابی مذکور را تشخیص دهد و مبدأ را از پذیرش مسیرهای در بر گیرنده چنین تونل‌هایی باز دارد.

علاوه بر آن، در بخش دیگری از این پایان‌نامه پیشنهاد شده است در پروتکل مسیریابی امن ARAN با استفاده از پروتکل احراز اصالت همه‌پخشی TIK[۱] [۱۳]، که بر مبنای محاسبه سریع و کم هزینه توابع رمزنگاری کلید متقارن استوار است، به جای امضای دیجیتال برای احراز اصالت گره‌های میانی قرار گرفته بین مبدأ و مقصد، عملکرد این پروتکل به لحاظ سربار محاسباتی و پردازشی تحمیل شده بر گره‌های شبکه ارتقا یابد. با در نظر گرفتن محدودیت‌های محاسباتی، پردازشی و انرژی محدود گره‌های موجود در یک شبکه بی‌سیم اقتضایی، این ارتقای عملکرد پردازشی پروتکل ARAN می‌تواند زمینه پیاده‌سازی هرچه کم هزینه‌تر، کاراتر و گسترده‌تر یکی از امن‌ترین پروتکل‌های مسیریابی امن اثبات‌پذیر در شبکه‌های بی‌سیم اقتضایی فراهم کند.

۱-۳ ساختار پایان‌نامه

در فصل دوم، ابتدا شبکه‌های بی‌سیم اقتضایی معرفی خواهند شد و مهمترین ویژگی‌های آنها به تفصیل مورد بررسی قرار خواهد گرفت. سپس مسیریابی و نقش آن در برپایی این شبکه‌ها تحلیل خواهد گردید و انواع مختلف پروتکل‌های مسیریابی و طبقه‌بندی‌های آنها از دیدگاه‌های مختلف تشریح خواهند شد. در مرحله بعد، سه پروتکل مسیریابی مهم که طراحی آنها بر دیگر پروتکل‌های مورد استفاده در این شبکه‌ها تأثیرگذار بوده است و پروتکل‌های مسیریابی امن متعددی بر مبنای آنها ارائه گردیده‌اند، به طور کامل و با ذکر جزییات نحوه عملکرد، مورد بحث و بررسی قرار خواهند گرفت. این سه پروتکل شامل پروتکل‌های DSR [۱]، AODV [۲] و DSDV [۳] هستند. معرفی این سه پروتکل، بستر مناسب برای ارائه نتایج تحقیقات انجام شده در این پایان‌نامه را فراهم خواهد کرد و امکان بهره‌گیری هرچه بیشتر از مطالب فصل‌های بعد را ایجاد خواهد نمود.

در فصل سوم، ابتدا اهداف کلی دشمن از حمله به پروتکل‌های مسیریابی در شبکه‌های بی‌سیم اقتضایی بیان خواهد شد و مکانیزم‌هایی که می‌توانند در اجرای حملات مذکور مورد سوء استفاده دشمن واقع شوند، معرفی خواهند گردید. سپس انواع حملات ممکن علیه پروتکل‌های مسیریابی در شبکه‌های بی‌سیم اقتضایی به پنج گروه عمده تقسیم می‌شوند و نحوه اجرای هر یک از آنها در انواع مختلف پروتکل‌های مسیریابی مورد استفاده در این شبکه‌ها تشریح می‌گردد. پس از آن، روش‌های مختلف مقابله با انواع حملات مورد بحث بررسی می‌شوند و کاربرد آنها در طراحی انواع پروتکل‌های مسیریابی امن پیشنهاد شده برای استفاده در شبکه‌های بی‌سیم اقتضایی تشریح می‌گردد.

در فصل چهارم، اهم پروتکل‌های مسیریابی امن پیشنهاد شده بر مبنای پروتکل‌های مسیریابی پایه تشریح شده در فصل دوم، معرفی می‌گردند و نحوه پیشگیری از حملات متصور علیه آنها با استفاده از روش‌های مورد بحث در فصل سوم تبیین می‌شود. پروتکل‌های مسیریابی امن مورد بحث، متناظر با سه پروتکل مسیریابی معرفی شده در فصل دوم، در سه

---

[۱] TESLA with Instant Key disclosure (TIK)

گروه عمده سازمان‌دهی گردیده‌اند. گروه نخست، اهم پروتکل‌های مسیریابی امن مبتنی بر پروتکل DSR [۱] است که شامل پروتکل‌های SRP [۶]، Ariadne [۷] و endairA [۸] می‌باشد. گروه دوم، اهم پروتکل‌های مسیریابی امن مبتنی بر پروتکل AODV [۲] است که شامل پروتکل‌های SAODV [۹] و ARAN [۱۰] می‌باشد. گروه سوم، اهم پروتکل‌های مسیریابی امن مبتنی بر پروتکل DSDV [۳] است که شامل پروتکل‌های SEAD و SuperSEAD [۱۱] می‌باشد.

در فصل پنجم، پروتکل مسیریابی امن endairA که یکی از امن‌ترین و کارآمدترین پروتکل‌های مسیریابی امن تقاضا محور مبتنی بر مبدأ جهت استفاده در شبکه‌های بی‌سیم اقتضایی است، تحلیل گردیده و عملکرد امنیتی آن ارتقا می‌یابد. در این فصل، ضمن ارائه یک سناریوی موفق حمله، آسیب‌پذیری این پروتکل نسبت به یکی از انواع قدرتمند حملات علیه پروتکل‌های مسیریابی در شبکه‌های بی‌سیم اقتضایی، به نام حمله تونل، اثبات خواهد شد. سپس، نسخه ارتقا یافته مقاوم نسبت به حمله تونل این پروتکل با استفاده از یک مکانیزم امنیتی جدید جهت پیشگیری از اجرای موفقیت‌آمیز حمله مذکور علیه پروتکل‌های مسیریابی مورد استفاده در شبکه‌های بی‌سیم اقتضایی، و به طور خاص پروتکل endairA، ارائه خواهد گردید. تحلیل امنیتی ارائه شده بر عملکرد و قابلیت‌های نسخه مقاوم نسبت به حمله تونل پروتکل مسیریابی امن endairA در ادامه این فصل نشان خواهد داد که این پروتکل قادر است بخش عمده‌ای از حملات تونل تأثیر گذار بر عملکرد پروتکل مسیریابی مذکور را تشخیص دهد و مبدأ را از پذیرش مسیرهای در بر گیرنده چنین تونل‌هایی باز دارد.

در فصل ششم، ابتدا پروتکل TIK [۱۳] به عنوان یک پروتکل احراز اصالت همه‌پخشی کارآمد و بهینه با حجم محاسباتی کم معرفی خواهد شد و مراحل اجرای آن به تفصیل تشریح خواهند گردید. سپس، نسخه ارتقا یافته پروتکل مسیریابی امن ARAN به لحاظ محاسباتی و پردازشی ارائه خواهد شد. در این نسخه از پروتکل، با پیشنهاد احراز اصالت گره‌های میانی موجود در شبکه، جز مبدأ و مقصد، با استفاده از پروتکل احراز اصالت همه‌پخشی TIK به جای استفاده از امضای دیجیتال، ارتقای عملکرد محاسباتی و پردازشی پروتکل ARAN به عنوان یک پروتکل مسیریابی امن اثبات‌پذیر محقق خواهد گردید. تحلیل و ارزیابی پروتکل ارتقا یافته و مقایسه آن با پروتکل ARAN نشان می‌دهد این ارتقای محاسباتی چشمگیر، هزینه اضافی عمده‌ای نخواهد داشت و در عین حال، امنیت پروتکل ARAN با بهبود محاسباتی ایجاد شده در آن به هیچ عنوان تنزل نخواهد یافت.

در فصل هفتم، ابتدا نتایج قابل تأمل حاصل از مطالعات گسترده انجام شده در حوزه امنیت مسیریابی در شبکه‌های بی‌سیم اقتضایی، که در فصل‌های قبل به تفصیل مورد بحث و بررسی قرار گرفته‌اند، به اختصار بیان خواهد شد. سپس خلاصه‌ای از مهمترین نوآوری‌های انجام شده در این پایان‌نامه ارائه خواهد گردید. در پایان نیز، پیشنهادهایی برای ادامه تحقیقات در این زمینه بیان خواهد شد.