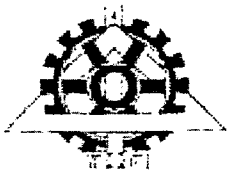
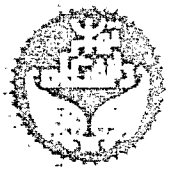
۱۳۸۶/۱۵/۱ -

۸۷۷۹۵





دانشگاه تهران

پردیس دانشکده‌های فنی

دانشکده مهندسی برق و کامپیوتر

عنوان

مسیریابی گمنام در شبکه‌های بی‌سیم بدون‌ساختار متحرک

نگارش

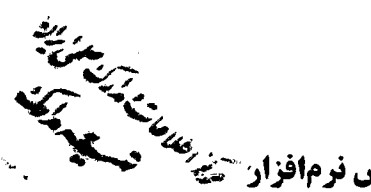
رضا شکری

استاد راهنما

دکتر ناصر یزدانی

استاد مشاور

دکتر مهرداد نورانی



پایان نامه برای دریافت درجهٔ کارشناسی ارشد در مهندسی کامپیوتر گرایش نرم‌افزار

تیر ۱۳۸۶

۱۳۸۶/۵/۱ -

۸۷۷۰۵

به نام خدا

دانشگاه تهران

پردیس دانشکده های فنی

دانشکده مهندسی برق و کامپیوتر

گواهی دفاع از پایان نامه کارشناسی ارشد

هیأت داوران پایان نامه کارشناسی ارشد آقا/خانم رضا شکری در رشته مهندسی برق و کامپیوتر، گرایش : نرم افزار

با عنوان: "ملاحظات امنیتی در شبکه های بی سیم بدون ساختار متحرک"

در تاریخ ۱۳۸۶/۰۴/۱۶ نمره نهایی پایان نامه: به عدد ۲۰ به حروف [illegible]

و درجه عالی ارزیابی نمود.

مشخصات هیأت داوران	نام و نام خانوادگی	مرتبه دانشگاهی	دانشگاه یا موسسه	امضاء
۱-استاد راهنما استاد راهنمای دوم (حسب مورد)	دکتر ناصر یزدانی	دانشیار	تهران	
۲-استاد مشاور	--	--	--	
۳-استاد مدعو خارجی (یا استاد مشاور دوم)	دکتر رسول جلیلی	استادیار	شریف	
۴-استاد مدعو داخلی	دکتراحمد خونساری	استادیار	تهران	
۵-داور و نماینده کمیته تحصیلات تکمیلی دانشکده	دکتر فرشاد لاهوتی	استادیار	تهران	

دانشکده فنی دانشگاه تهران
تحصیلات تکمیلی

تذکر:این برگه پس از تکمیل توسط هیأت داوران در نخستین صفحه پایان نامه درج می گردد.

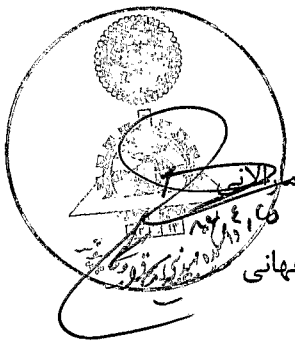
با تصویب هیات داوران و تایید تحصیلات تکمیلی، عنوان پایان‌نامه از "ملاحظات امنیتی در شبکه های بی سیم بدون ساختار متحرک" به "**مسیریابی گمنام در شبکه‌های بی‌سیم بدون ساختار متحرک**" تغییر یافت.

دانشگاه تهران
پردیس دانشکده های فنی
دانشکده مهندسی برق و کامپیوتر

پایان‌نامه برای دریافت درجه کارشناسی ارشد در رشته مهندسی کامپیوتر گرایش نرم افزار
این پایان‌نامه در تاریخ ۸۶/۴/۱۶ در حضور هیأت داوران دفاع گردید و مورد تصویب قرار گرفت.

عنوان: **مسیریابی گمنام در شبکه‌های بی‌سیم بدون‌ساختار متحرک**

نگارش: **رضا شکری**



معاون آموزشی و تحصیلات تکمیلی پردیس دانشکده‌های فنی:	دکتر جواد فیض
رئیس دانشکده مهندسی برق و کامپیوتر:	دکتر پرویز جبه‌دار مارالانی
معاون پژوهشی و تحصیلات تکمیلی دانشکده مهندسی برق و کامپیوتر:	دکتر سعید نادر اصفهانی
استاد راهنما:	دکتر ناصر یزدانی
استاد مشاور:	دکتر مهرداد نورانی
عضو هیأت داوران:	دکتر احمد خوانساری
عضو هیأت داوران:	دکتر فرشاد لاهوتی
عضو هیأت داوران:	دکتر رسول جلیلی

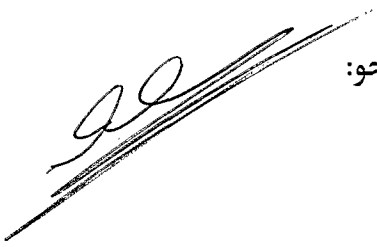
تعهدنامه اصالت اثر

اینجانب رضا شکری تایید می‌کنم که مطالب مندرج در این پایان‌نامه حاصل کار پژوهشی اینجانب بوده و به دستاوردهای پژوهشی دیگران که در این نوشته از آنها استفاده شده است مطابق مقررات ارجاع گردیده است. این پایان‌نامه قبلاً برای احراز هیچ مدرک هم سطح یا بالاتر ارایه نشده است.

کلیه حقوق مادی و معنوی این اثر متعلق به دانشکده فنی دانشگاه تهران می باشد.

نام و نام خانوادگی دانشجو: رضا شکری

امضای دانشجو:



تقدیر و تشکر

از مرکز تحقیقات مخابرات ایران بخاطر حمایت های مالی ایشان تشکر می‌نمایم.
همچنین، از تمامی کسانی که مرا در انجام این پایان نامه یاری نمودند و بطور خاص از استاد راهنمایم آقای دکتر یزدانی تشکر می نمایم.

چکیده

با افزایش تقاضا در استفاده از شبکه‌های بی‌سیم بدون‌ساختار متحرک در سال‌های اخیر، توجه به نیازهای امنیتی اینگونه شبکه‌ها نیز افزایش یافته است. استفاده از بستر بی‌سیم، اتکا بر گره‌های ناشناخته در بستر شبکه برای انتقال اطلاعات، پویایی همبندی شبکه، توان پایین منابع ذخیره‌سازی و پردازشی و عدم پشتیبانی از سرویس مرکزی، از جمله خصوصیات منحصربفرد این شبکه‌ها به شمار می‌آیند و قراردادهای امنیتی جاری در شبکه اینترنت برای آن‌ها ناکافی است. همچنین در برخی از حوزه‌های امنیتی، میزان آسیب‌پذیری بیشتر بوده و نیاز به تدوین قراردادهای جدید کاملاً احساس می‌شود. برای مثال، به علت بستر مشترک و باز ارتباطی، استفاده همه‌گیر این شبکه‌ها در ابزارهای مورد استفاده مردم به منظور برطرف کردن نیازهای واقعی‌شان و همچنین گسترش این شبکه‌ها در سیستم‌های خودکار، آسیب‌پذیری شبکه در مورد لو رفتن اطلاعات محرمانه و شخصی کاربران بالا بوده و نیاز به برقراری مکانیزم‌های حفظ حریم کاملاً بیشتر از شبکه اینترنت حس می‌شود. حملات غیرفعال که در آن مهاجمان اقدام به شنود ارتباطات کرده و اطلاعات کاربران و ارتباطات آن‌ها را ثبت و تحلیل می‌کنند، حریم کاربران و قراردادهای شبکه را نقض می‌کنند. به منظور مقابله با این حملات در شبکه، نیاز به تدوین قراردادهای جدید است. قراردادهای مسیریابی گمنام به منظور پنهان‌سازی اطلاعات گره‌های در حال ارتباط، اعم از شناسه واقعی آن‌ها و گراف ارتباطی گره‌ها در لایه شبکه اقدام به حفظ حریم شبکه در مقابل مهاجمان ناظر بر شبکه می‌کنند. در این پایان‌نامه با بررسی مفاهیم کلی حفظ حریم ارتباطی در شبکه‌های بی‌سیم بدون‌ساختار و با

نگاهی منتقدانه به روش‌های ارائه شده در زمینه مسیریابی گمنام، روش‌های جدیدی در مسیریابی گمنام ارائه شده است. ساختار مسیریابی زنجیره‌ای بر اساس نام مستعار و همچنین قرارداد ارتباطی گمنام در شبکه به منظور فراهم ساختن گمنامی و پیوندناپذیری در شبکه با حداقل سربار و کارایی بالا ارائه شده‌اند. همچنین به کمک روش‌های صوری، درستی کارکرد قرارداد مسیریابی زنجیره‌ای گمنام مورد بررسی قرار گرفته است. با استفاده از مفاهیم نظریه اطلاعات، میزان گمنامی بدست آمده در شبکه نیز اندازه‌گیری شده و توانایی بالای قراردادهای ارائه شده نشان داده شده است.

فهرست مطالب

فهرست جداول و اشکال

۱ مقدمه و تعریف مسئله

۱-۱ شبکه های بی سیم بدون ساختار متحرک

یک شبکه بی سیم بدون ساختار متحرک[1] شبکه‌ای تشکیل یافته از گره های پویا و متحرکی است که در یک محیط بدون ساختار به منظور برقراری ارتباطات شبکه‌ای از بستر بی‌سیم استفاده می‌کنند. اصطلاح بدون ساختار به این دلیل به این‌گونه از شبکه‌ها اتلاق می‌گردد که گره های متحرک در شبکه به صورت پویا مسیرهایی مابین خود بوجود می‌آورند که تنها به منظور انتقال لحظه‌ای و مقطعی بسته‌ها بین دو گره در حال ارتباط شکل می‌گیرد و از ناحیه‌بندی‌های موجود در شبکه‌های با بستر سیمی همانند اینترنت خبری نیست. گره هایی که در دامنه دید آنتن‌های بی‌سیم یکدیگر قرار دارند توانایی ارتباط مستقیم با یکدیگر را خواهند داشت و در غیراین‌صورت می‌بایست از گره های دیگر شبکه به منظور انتقال بسته‌هایشان کمک بگیرند. بنابراین هر گرهی در این نوع از شبکه‌ها نقش مسیریاب را نیز بر عهده خواهد داشت و بسته‌ای که از سوی گره مبداء به سمت مقصد فرستاده می‌شود از گره های دیگر یکی پس از دیگری عبور کرده تا در اختیار گره موردنظر قرار گیرد. در نتیجه همانطور که از نحوه عملکرد شبکه برمی‌آید میزان موفقیت و کارایی ارتباطات شبکه تا حد زیادی به همکاری و هماهنگی گره هایی که تنها نقش عبوردهنده بسته‌ها را بر عهده دارند، بستگی دارد.

از کاربردهای مختلف این گونه از شبکه ها می‌توان به موارد زیر اشاره نمود: سربازانی که در یک منطقه نظامی مشغول انجام یک عملیات و یا جمع‌آوری اطلاعات هستند، نمایندگان تجاری شرکت‌های مختلف که در یک جلسه حضوریافته‌اند و نیاز به انتقال اطلاعات با یکدیگر دارند، شرکت‌کنندگان در یک کنفرانس که از کامپیوترهای همراه خود به منظور مبادله اطلاعات با دیگران

---

[1] Wireless Mobile Ad Hoc Network (MANET)

بهره می‌برند و یا شبکه نیروهای امدادرسانی که پس از وقوع یک حادثه در محل جمع شده‌اند و نیازمند ارتباط مستمر با یکدیگرند. بعلاوه، از انواع دیگر کاربردهای شناخته‌شده برای اینگونه شبکه‌ها، به شبکه‌های خانگی، شبکه‌های سرویس‌دهی ناحیه‌ای و شبکه‌های سنسوری می‌توان اشاره کرد.

۱-۲ ملاحظات امنیتی

نیازهای امنیتی در شبکه های بی سیم بدون ساختار متحرک، همانند دیگر سیستم های ارتباطی کامپیوتری عمدتاً شامل محرمانگی[۱]، جامعیت[۲]، دسترس پذیری[۳]، اصالت سنجی[۴] و عدم انکار[۵] میشود.

- محرمانگی: داده فرستاده شده توسط گره مبدا فقط باید برای گره مقصد قابل فهم باشد و اگر مهاجم به داده ارسالی دسترسی پیدا کرد، نتواند اطلاعات مفیدی از آن داده استخراج کند. یکی از روش های مرسوم برای تضمین کردن محرمانگی استفاده از رمزنگاری داده می باشد.
- جامعیت: داده فرستاده شده توسط گره مبدا باید همان‌گونه که فرستاده شده به گره مقصد برسد و از تغییر مصون باشد. به عبارت دیگر، یک گره بدخواه[۶] در شبکه نمی‌تواند داده در حال انتقال را تغییر دهد.
- دسترس‌پذیری: شبکه باید در هر زمانی به کار خود ادامه دهد. شبکه باید به اندازه کافی مقاوم[۷] باشد تا تحمل شکسته شدن پیوندها[۸] را داشته باشد و همچنین قادر باشد درمقابل حمله های مختلفی که روی آن انجام می شود به بقای خود ادامه دهد. در واقع هر وقت که کاربر احتیاج به سرویسی داشت باید آن را در اختیار او قرار دهد.

---

[1] Confidentiality
[2] Integrity
[3] Accessibility
[4] Authenticity
[5] Non-Repudiation
[6] Malicious Node
[7] Robust
[8] Link Failure

- اصالت سنجی: این خصوصیت، طرفین یک ارتباط را مطمئن می کند که با همان کسی در حال ارتباط هستند که انتظار دارند. بنابراین اصالت سنجی، ارتباط را در برابر جعل هویت ایمن می کند.
- انکارناپذیری: مکانیزمی است که تضمین می کند فرستنده پیغام نمی تواند بعداً فرستادن پیغام را تکذیب کند و همچنین گیرنده پیغام نیز نمی‌تواند دریافت کردن آن را انکار کند. امضای دیجیتالی[1] که به عنوان یک شناسه منحصر به فرد برای هر کاربر عمل می کند، شبیه امضای دستی، معمولاً برای این هدف استفاده می‌شود.

البته حوزه نیاز به این پارامترها دارای فرقهایی به علت ساختار کاملاً متفاوت این شبکه ها هست. به علت عدم وجود ساختار در شبکه‌های مورد بحث و همچنین نیاز هر گره به همکاری و سرویس‌دهی گره های ناشناخته در شبکه برای برقراری ارتباط با گره موردنظر خود، آسیب‌پذیری‌های بسیاری متوجه این‌گونه از شبکه‌ها می‌شود. در حقیقت، خصوصیات منحصر به فرد شبکه باعث به وجود آمدن آسیب پذیری ها و همچنین حملات منحصر به فردی در شبکه های بی سیم بدون ساختار شده است. همچنین، طراحی قراردادهای امنیتی و قراردادهای شبکه امن دارای مسائل زیادی است. از این خصوصیات میتوان به کانال رادیویی به اشتراک گذاشته شده، محیط عملیاتی نا امن، فقدان اختیارات مرکزی، فقدان مسیر ارتباطی دقیق و مشخص میان گره ها، محدود بودن منابع، و ناامنی بسیار بالای لایه فیزیکی اشاره کرد. مشکلات ناشی از هر یک از این خصوصیات نامبرده به طور مختصر در زیر بررسی شده است:

- **کانال رادیویی به اشتراک گذاشته شده:** برخلاف شبکه های سیمی، جایی که خطوط اختصاصی[2] مجزا می توان بین دو کاربر ایجاد کرد، کانال رادیویی مورد استفاده برای ارتباط در شبکه‌های بی‌سیم دارای طبیعت منتشر شونده و همه‌پخشی[3] است که توسط همه گره ها در شبکه به اشتراک گذاشته شده است. داده منتقل شده توسط یک گره، توسط همه گره های

---

[1] Digital Signature
[2] Dedicated Lines
[3] Broadcast

درون محدوده انتقال آن گره قابل دریافت است. بنابراین یک مهاجم به راحتی می تواند داده در حال انتقال در شبکه را بدست آورد. البته این مشکل را می توان تا حدی با استفاده از آنتن‌های یک جهته[1] کم کرد.

- **محیط عملیاتی نا امن:** محیط عملیاتی که شبکه‌های بی‌سیم در آن مورد استفاده قرار می‌گیرند، ممکن است همیشه امن نباشد. یکی از کاربردهای مهم این شبکه ها در میدان جنگ است. در این کاربردها ممکن است گره‌ها به قلمرو ناامن دشمن وارد و یا خارج شوند، جایی که می‌تواند گره‌ها را در مقابل حمله های امنیتی بسیار رخنه پذیر سازد.
- **فقدان اختیارات مرکزی:** در شبکه های سیمی و شبکه‌های بی‌سیم دارای زیر ساخت، می توان ترافیک شبکه را توسط نقاط مرکزی (مانند مسیریاب‌ها و نقاط اتصال[2]) زیر نظر گرفت و مکانیزم های امنیتی را در این نقاط پیاده سازی کرد. از آنجا که شبکه‌های بی‌سیم بدون ساختار دارای چنین نقاط مرکزی نیستند، از این مکانیزم‌ها نمی‌توان در شبکه استفاده کرد.
- **فقدان ارتباط میان نودها:** از آنجا که این شبکه‌ها طبیعت پویا دارند، نودها می توانند در هر لحظه از زمان وارد شبکه شوند و یا شبکه را ترک کنند. اگر هیچ مکانیزم اصالت‌سنجی[3] مناسبی برای ارتباط دادن نودها با شبکه استفاده نشود، مهاجم می‌تواند به راحتی به شبکه ملحق شود و حمله‌های خود را انجام دهد.
- **محدود بودن منابع:** منابعی مانند پهنای باند، توان باتری، و توان محاسباتی در شبکه‌های بی‌سیم محدود هستند. در نتیجه، پیاده سازی یک مکانیزم امنیتی پیچیده مبتنی بر رمزنگاری در این شبکه‌ها مشکل است.
- **رخنه‌پذیری‌های فیزیکی:** نودها در این شبکه ها معمولاً کوچک و دستی هستند. این نودها به راحتی می توانند خراب شوند و یا دزدیده شوند.

---

[1] Directional Antennas
[2] Access Points
[3] Authentication

با توجه به نکات ذکر شده، واضح است که روشهای به کار گرفته شده در شبکه های سیمی و اینترنت به سادگی قابل اعمال بر شبکه های مورد بحث نبوده و نیازمند تغییر برای اجرا در محیط جدید میباشند. همچنین، رویکرد صحیح به حل مسائل امنیتی و یا مسائل شبکه ای رویکرد ارائه راه حل به هدف اجرا در شبکه های بی سیم است و نه تغییر روشهای موجود در اینترنت و اجرای آنها در این شبکه ها. لازم به ذکر است که اگرچه این تغییرات باعث نیاز به تولید و تدوین روشهای جدید است، ولیکن تعاریف و دسته بندی های انجام شده در حوزه امنیت شامل این گونه از شبکه ها نیز میشود.

حمله‌های شناخته شده در شبکه های بیسیم متحرک را می توان به دو دسته بزرگ تقسیم کرد: حملات فعال[1] و حملات غیرفعال[2]. اگرچه این دسته بندی به طور کلی در مورد کلیه شبکه ها صادق است، ولیکن در هر فیلد، متاثر از خصوصیات منحصر به فرد نوع شبکه، میتوان تعریف دقیقتری برای آنها ارائه داد.

حملات غیرفعال یک دسته بزرگ از حملات شبکه را تشکیل میدهند و خصوصیت اصلی آنها این است که در عین حمله در عملکرد شبکه خللی وارد نمی کنند. به عبارت دیگر مهاجم فقط به داده ای که در شبکه رد و بدل می شود گوش می دهد بدون این که در آن تغییری ایجاد کند. در حقیقت کار مهاجم شنود است. در صورتی که ترافیک شنیده شده توسط مهاجم حاوی اطلاعاتی باشد و مهاجم قادر باشد که از داده جمع آوری شده آن اطلاعات را استخراج کند، محرمانگی شبکه و ارتباطات به خطر خواهد افتاد. ازآنرو که عملکرد شبکه پس از یک حمله غیرفعال تحت تاثیر قرار نمیگیرد و در نتیجه آثاری از حمله در شبکه به جای گذاشته نمیشود، کشف اینگونه حملات بسیار مشکلتر از حملات فعال است.

رویکرد غالب، استفاده از مکانیزمهای پیشگیرانه است، به این معنی که ارتباطات شبکه کمترین اطلاعات را برای یک ناظر خارجی داشته باشد. به طور دقیقتر کانال ارتباطی شبکه به مهاجم کمترین ظرفیت ممکن را داشته باشد. این کانال ارتباطی را میتوان به کانال *داده* و کانال *ترافیک*

---

[1] Active Attacks
[2] Passive Attacks