



امنیت در شبکه‌های Ad Hoc

فصلنامه رضائی آرپاتپه

امین: مشایخی شمس

پری‌ناز مشایخی شمس

جواد رضائی آرپاتپه

انتشارات ارتباطات اجتماعی

۱۳۹۶

فرشته رضائی آریاتپه، ۱۳۶۹- امین مشایخی شمس، ۱۳۷۵- پری‌ناز مشایخی شمس، ۱۳۶۹- جواد رضائی آریاتپه، ۱۳۷۵.

امنیت در شبکه‌های Ad Hoc/فرشته رضائی آریاتپه ... [و دیگران]. تهران: نشر ارتباطات اجتماعی، ۱۳۹۶.
۹۶ ص.

شابک: ۹۷۸-۶۰۰-۸۴۳۷-۱۲-۳

موضوع:

۱. شبکه‌های بی‌سیم - تدابیر ایمنی
 ۲. Ad hoc networks (Computer networks) -- Security measures
 ۳. شبکه‌های کامپیوتری -- تدابیر ایمنی
 ۴. Computer networks -- Security measures
 ۵. ارتباطات بی‌سیم - تدابیر ایمنی
 ۶. Wireless communication systems -- Security measures
- ۷۷/۵۱۰۵TK/الف ۸۲۹۶
۶۸/۰۰۴
۴۶۷۳۷۷۷

نام کتاب: امنیت در شبکه‌های Ad Hoc

مؤلفین: فرشته رضائی آریاتپه، امین مشایخی شمس، پری‌ناز مشایخی شمس، جواد رضائی آریاتپه.

ناشر: ارتباطات اجتماعی

چاپ و صحافی: محقق/اردیل

شمارگان: ۱۰۰

نوبت چاپ: اول، ۱۳۹۶

قیمت: ۱۳۰۰۰ تومان

مرکز پخش:

کلیه مراکز فروش کتب مهندسی در سراسر کشور

«تمام حقوق این اثر برای ناشر محفوظ است»

فهرست

صفحه	موضوع
هفت	پیش گفتار
هشت	مقدمه

فصل اول : مفاهیم اولیه

۱	مقدمه
۲	۱-۱ مثال امنیت در شبکه
۳	۱-۲ امنیت در شبکه AD HOC
۵	۳-۱ اهداف امنیت در شبکه های AD HOC
۶	۴-۱ لایه فیزیکی
۶	۵-۱ لایه لینک
۷	۶-۱ لایه شبکه

فصل دوم : نیازها و چالش های امنیت در مسیریابی شبکه های AD HOC

۹	مقدمه
۹	۱-۲ ساختارها و نیازهای جدید امنیتی
۱۰	۱-۱-۲ ناشناسی
۱۰	۲-۱-۲ جلوگیری از خودخواهی
۱۲	۳-۱-۲ تصمیم گیری توزیع شده

۱۲	۴-۱-۲ چند مسیره گی در مسیر یابی
۱۴	۲-۲ طراحی ساختار امن
۱۴	۱-۲-۲ مکانیزم عکس‌العملی: تشخیص نفوذ در شبکه (IDS)
۱۷	۲-۲-۲ مکانیزم‌های پیشگیری

فصل سوم: آسیب پذیری در شبکه‌های AD HOC

۲۱	مقدمه
۲۱	۱-۳ دسته بندی حملات
۲۳	۲-۳ حمله با استفاده از MODIFICATION
۲۳	۱-۲-۳ تغییر مسیر با استفاده از شماره سریال دستکاری شده
۲۴	۲-۲-۳ تغییر مسر با استفاده از شماره پرش دستکاری شده
۲۴	۳-۱-۳ DOS با استفاده از مسیر مبدا دستکاری شده
۲۵	۳-۲ تونل زنی
۲۶	۳-۳ حمله با استفاده از IMPERSONATION
۲۶	۱-۳-۳ تشکیل شبکه با استفاده از SPOOFING
۲۷	۲-۳-۳ حمله با استفاده از سامه سیر یابی غلط (FABRICATION)
۲۷	۳-۳-۳ پیغام خطا در مسیر حملات
۲۸	۴-۳-۳ ایجاد مسیر هتی غلط در جداول مسیریابی نودهای همسایه
۲۸	۴-۳ سایر حملات
۲۸	۱-۴-۳ حمله WORMHOLE
۳۰	۲-۴-۳ حمله RUSHING

فصل چهارم: الگوریتم‌های مسیریابی امن در شبکه‌های AD HOC

۳۳	مقدمه
۳۳	۱-۴ الگوریتم مسیریابی SEAD
۳۵	۱-۱-۴ عملکرد زنجیره HASH
۳۶	۲-۱-۴ اصالت سنجی در متریک و شماره سریال
۳۷	۳-۱-۴ اصالت سنجی برای نودهای همسایه

۳۶	۴-۱-۴ ضعیف‌های SEAD
۳۸	۲-۴ الگوریتم مسیر یابی ARIADNE
۳۹	۱-۲-۴ ویژگی‌های اصلی مسیر یابی در ARIADNE
۴۱	۲-۲-۴ بررسی امنیتی ARIADNE
۴۲	۳-۴ الگوریتم مسیر یابی ARAN
۴۲	۱-۳-۴ ساختار ARAN
۴۴	۲-۳-۴ ضعیف‌های امنیتی ARAN
۴۵	۴-۴ الگوریتم مسیر یابی SAODV

فصل پنجم: الگوریتم‌های پیشنهادی

۴۸	مقدمه
۴۹	۱-۵ الگوریتم پیشنهادی برای توزیع کلید
۵۱	۲-۵ الگوریتم پیشنهادی برای اصالت سنجی در فرآیند مسیر یابی
۵۲	۱-۲-۵ اصالت سنجی نودهای مسایه
۵۲	۲-۲-۵ اصالت سنجی در فرآیند کشف مسیر
۵۶	۳-۲-۵ تحلیل امنیتی الگوریتم پیشنهادی
۵۷	۴-۲-۵ احتمال جعل هویت در ساختار ارائه شده
۶۳	۵-۲-۵ شبیه‌سازی الگوریتم پیشنهادی در یک سناریوی واقعی
۶۴	۳-۵ ساختار پیشنهادی برای ایجاد امضای تصادفی
۶۶	۱-۳-۵ تحلیل امنیتی الگوریتم پیشنهادی
۶۸	۲-۳-۵ شبیه‌سازی الگوریتم پیشنهادی در شرایط واقعی
۶۹	۴-۵ بهینه‌سازی الگوریتم توزیع کلید پیشنهادی
۷۱	۱-۴-۵ تحلیل امنیتی ساختار بهبود یافته توزیع کلید

فصل ششم

۷۴	نتیجه‌گیری و کارهای آینده
----	---------------------------

فصل هفتم: ضمیمه ۱

۷۶	۱-۷ پروتکل‌های مسیر یابی متداول در شبکه‌های AD HOC
----	--

۷۸	DSDV ۲-۷
۷۹	DSR ۳-۷
۸۰	AODV ۴-۷

فصل هشتم : ضمیمه ۲

۸۲	۱-۸ رمزنگاری متقارن
۸۲	۲-۸ رمزنگاری نامتقارن
۸۶	خلاصه
۸۷	مراجع

پیشگفتار

در لغت نامه کلمه Ad Hoc به معنی چیزی است که فوراً و بدون نیاز به شی یا امکانات خاصی ایجاد می شود این معنی در تعریف شبکه های Ad Hoc نیز صادق است. شبکه های Ad Hoc وقتی مورد استفاده قرار می گیرند که امکان و یا دسترسی به شبکه های با ساختار ثابت (infrastructure) مانند آنتن های فرستنده وجود ندارد و یا استفاده از آن ها صرفه اقتصادی ندارد. در چنین شرایطی کار بر نیاز به شبکه خود سازمان دهنده و خود محور هستند که نیازی به سیستم کنترل مرکزی برای برقراری ارتباط ندارند.

شبکه های Ad Hoc از تعدادی node (node: تجهیزاتی که در محیط شبکه از امکانات شبکه استفاده می کنند) تشکیل شده است. محدوده جغرافیایی یا برد شبکه Ad Hoc تمام نقاطی است که nodeها در آن گسترده شده اند.

در شبکه های Ad Hoc هر node مجهز به یک فرستنده و گیرنده است که امکان برقراری ارتباط با سایر nodeهای شبکه وجود دارد. در این نوع شبکه هر node قادر است اطلاعات خود را تولید کرده و به مقصد مورد نظر انتقال دهد. در شبکه Ad Hoc هر node قادر است به عنوان Gateway (گذرگاه خروجی) برنامه ریزی شود. یک node ثابت و پایه اینترنت متصل شود. سایر nodeها نیز می توانند با node ای که به عنوان Gateway شبکه است ارتباط برقرار کرده و اطلاعات خود را با استفاده از آن به بیرون شبکه انتقال دهند.

در شبکه های Ad Hoc به علت عدم وجود سیستم مرکزی، تغییر در توپولوژی های مسیر یابی (Routing Protocols) و نبود زیر ساخت ثابت (infrastructure) مسئله حفظ امنیت از اهمیت بسیار بالایی برخوردار است. این شبکه ها به صورت ذاتی در مقابل حملات امنیتی پذیر است به همین دلیل باید به چالش های امنیتی ایجاد شده توجه ویژه کرد.

در این کتاب سعی شده علاوه بر افزایش معلومات خواننده در زمینه ی شبکه های Ad Hoc، علاقه و شوق فراگیری در خواننده ایجاد شود.

امید است شما خواننده ی گرامی نهایت رضایت و خرسندی را از مطالعه ی این کتاب داشته باشید.

فرشته رضائی آریاتپه

شبکه‌های بی‌سیم موردی یا شبکه‌های بی‌سیم ادهاک (AD hoc Networks)، شامل مجموعه‌ای از گره‌های توزیع شده‌اند که با همدیگر به طور بی‌سیم ارتباط دارند. نودها می‌توانند کامپیوتر میزبان یا مسیریاب باشند. 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 نتیجه 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. شبکه‌های بی‌سیم ادهاک خود بر دو نوع می‌باشند: شبکه‌های حسگر هستند. شبکه‌های موبایل ادهاک. در مسیریابی در شبکه‌های ادهاک نوع حسگر 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. گره منابع کافی نداشت بسته را به آن برای ارسال به مقصد نفرستد.

شبکه‌های موردی شبکه‌هایی هستند که برای مسیریابی از هیچ عنصر کمکی شبکه‌ای استفاده نمی‌کنند. بلکه در این شبکه‌ها خود گره‌های شرکت‌کننده در شبکه وظیفه مسیریابی شبکه را به عهده دارند. امنیت در شبکه‌های موردی از وضعیت ویژه‌ای برخوردار است. زیرا در این شبکه‌ها علاوه بر تمامی مشکلات موجود در شبکه‌های بی‌سیم، مشکلات امنیتی همچون سادگی شنود و تغییر اطلاعات در حال انتقال، امکان جعل هویت افراد، شرکت‌کنندگان یا تخریب عملیات مسیریابی، عدم امکان استفاده از زیرساخت‌های توزیع کلید رمزنگاری و غیره مواجه می‌شود. یکی از مهمترین موارد امنیتی در شبکه‌های موردی، ارائه یک الگوریتم مسیریابی امن در این شبکه‌هاست. در چند سال اخیر تلاش زیادی برای ارائه یک الگوریتم مسیریابی امن در شبکه‌های موردی انجام و نیزه اشاره SRP, Ariadne, SEAD, ARAN, SAODV شده است. از این میان می‌توان به پروتکل‌های AL HC مورد بررسی قرار مشکلات خاص مربوط به خود می‌باشند و همچنین کمبود یک الگوریتم امن از لحاظ امنیت و هم از لحاظ کارایی شبکه در حد قابل قبولی باشد احساس می‌شود.

کتابی که پیش‌رو دارید تلاش دارد مبحث حیاتی امنیت در شبکه‌های AL HC مورد بررسی قرار دهد که حاصل تلاش خانم‌ها دکتر فرشته رضائی آریاتپه و مهندس پری‌ناز مشایخی شمس و آقایان مهندس امین مشایخی شمس و مهندس جواد رضائی آریاتپه می‌باشد.