
بسم الله الرحمن الرحيم

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

برقراری یک مدل اعتماد توزیع شده مقاوم جهت بکارگیری در شبکه‌های اقتضایی متحرک

پایان نامه کارشناسی ارشد مهندسی برق – مخابرات

صادق بناری

اساتید راهنما

دکتر مهدی برنجکوب

دکتر محمد دخیل علیان

۱۳۹۱

دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

پایان‌نامه کارشناسی ارشد مهندسی برق- مخابرات آقای صادق بناری

تحت عنوان

برقراری یک مدل اعتماد توزیع شده مقاوم جهت بکارگیری در شبکه‌های اقتضایی متحرک

در تاریخ ۹۱/۱۰/۵ توسط کمیته‌ی تخصصی زیر مورد بررسی و تصویب نهایی قرار گرفت.

۱- استاد راهنمای پایان‌نامه	دکتر مهدی برنجکوب
۲- استاد راهنمای پایان‌نامه	دکتر محمد دخیل علیان
۳- استاد داور	دکتر علی فانیان
۴- استاد داور	دکتر محمد حسین منشئی
سرپرست تحصیلات تکمیلی	دکتر مسعود عمومی

تشکر و قدردانی

خداوندا! می خواهم تو را شکر می گویم به خاطر تمامی نعمت هایی که به من ارزانی داشته ای. از اساتید ارجمندم، جناب آقای دکتر مهدی برنجکوب و جناب آقای دکتر محمد دخیل علیان که با راهنمایی های دلسوزانه در طول دوران تحقیق همراه من بودند قدردانی می کنم. از آقایان دکتر فانیان و دکتر منشی که زحمت داوری این پایان نامه را پذیرفتند سپاسگزارم.

تقدیم به:

شهدای دانشگاه صنعتی اصفهان

فهرست مطالب

عنوان **صفحه**

فصل سوم: معرفی انواع مدل‌های اعتماد

فصل چهارم: عدم قابلیت بکارگیری پروتکل‌های به روز رسانی موجود در مدل‌های اعتماد توزیع شده

فهرست اشکال

عنوان **صفحه**

فهرست جداول

عنوان **صفحه**

چکیده

شبکه اقتضایی متحرک یک شبکه بی‌سیم متشکل از گره‌های متحرک است که بر خلاف شبکه‌های مرسوم به هیچ گونه زیرساخت از قبل معین و مدیریت متمرکزی متکی نیست. همانند شبکه‌های معمولی، به سرویس‌های امنیتی جهت تامین امنیت شبکه‌های اقتضایی نیازمندیم. بکارگیری هر سرویس امنیتی مستلزم تعریف یک مدل اعتماد است تا مشخص شود که چه کسی به چه کسی و چگونه اعتماد کند. در شبکه‌های مرسوم دارای زیر ساخت، معمولا یک طرف سوم مورد اعتماد متمرکز با انجام وظایفی مانند مدیریت کلید، سرویس‌های امنیتی را در شبکه برقرار می‌سازد. به علت ساختار خاص شبکه‌های اقتضایی، نمی‌توان از یک طرف سوم مورد اعتماد متمرکز در این شبکه‌ها استفاده کرد. بنابراین از طرف سوم مورد اعتماد توزیع شده برای فراهم آوردن سرویس‌های امنیتی مورد نیاز در شبکه‌های اقتضایی استفاده می‌شود. چهار عملیات تسهیم راز آستانه‌ای، امضای آستانه‌ای، به روز رسانی سهام و اضافه کردن عضو جدید، عملیات‌هایی هستند که به منظور برقراری یک طرف سوم مورد اعتماد توزیع شده مورد استفاده قرار می‌گیرند. در عملیات تسهیم راز آستانه‌ای، کلید خصوصی طرف سوم مورد اعتماد بین تعدادی از گره های شبکه که سرویس‌دهنده نامیده می‌شوند، تسهیم می‌شود. تسهیم کلید خصوصی به گونه‌ای انجام می‌گیرد که برای بازیابی راز باید حداقل تعداد آستانه‌ای از سرویس‌دهنده با هم همکاری داشته باشند. تسهیم راز به تنهایی برای مقابله با دشمن متحرک که قصد تسخیر آستانه‌ای از سرویس‌دهنده‌ها را دارد کافی نیست. به روز رسانی سهام یکی از بخش‌های اساسی در برقراری طرف سوم مورد اعتماد توزیع شده است که برای مقابله با دشمن متحرک از آن استفاده می‌شود. در این پایان نامه با ارائه حملاتی به برخی از پروتکل‌های به روز رسانی موجود، ناکارآمدی این پروتکل‌ها برای بکارگیری در شبکه اقتضایی نشان داده می‌شود. پس از آن یک پروتکل به روز رسانی مقاوم و سازگار با ویژگی‌های منحصر بفرد شبکه‌های اقتضایی، ارائه می‌شود. عملیات به روز رسانی در پروتکل به روز رسانی پیشنهادی به گونه ای است که سرویس دهنده ها در دسته‌های مستقل متشکل از آستانه‌ای از سرویس‌دهنده‌ها می‌توانند عملیات به روز رسانی سهام را انجام دهند. در مقایسه با سایر پروتکل‌های به روز رسانی موجود، پروتکل به روز رسانی پیشنهادی اولاً در مقابل حمله پیشنهادی مقاوم است و ثانیاً از کارآمدی بیشتری برخوردار است. سپس با بکارگیری پروتکل به روز رسانی پیشنهاد شده یک مدل اعتماد مقاوم برای بکارگیری در شبکه‌های اقتضایی ارائه می‌شود.

کلمات کلیدی: ۱- شبکه‌های اقتضایی متحرک ۲- مدل اعتماد توزیع شده ۳- مرجع تولید گواهینامه توزیع شده ۴- رمزنگاری آستانه‌ای ۵- به روز رسانی سهام

فصل اول
مقدمه

۱-۱ مقدمه

بکارگیری هر سرویس امنیتی مستلزم تعریف یک مدل اعتماد است تا مشخص شود که چه کسی به چه کسی و چگونه اعتماد کند. همانند شبکه‌های معمولی، به سرویس‌های امنیتی مانند محرمانگی[۱]، عدم انکار[۲]، احراز اصالت[۳]، تمامیت[۴] و ... جهت تامین امنیت شبکه‌های اقتضایی نیازمندیم. مدیریت کلید یک نیاز اولیه و اساسی جهت برآورده کردن سرویس‌های امنیتی است که این نیز به نوبه خود نیازمند تعریف و برپایی یک مدل اعتماد مقاوم و کارا است. در شبکه‌های معمولی دارای زیر ساخت، معمولا یک طرف سوم مورد اعتماد مرکزی با انجام وظایفی مانند مدیریت کلید، سرویس‌های امنیتی را در شبکه برقرار می‌سازد. به علت ساختار خاص شبکه‌های اقتضایی، بکارگیری مدل‌های اعتماد ارائه شده در شبکه‌های معمولی دارای زیرساخت در این شبکه‌ها غیر ممکن است. به عنوان مثال استفاده از یک طرف سوم مورد اعتماد مرکزی باعث بروز مشکلاتی مانند دسترس پذیری و بوجود آمدن نقطه واحد آسیب-پذیری[۵] می‌شود. بنابراین باید به دنبال راه‌حل مناسبی جهت برقراری یک مدل اعتماد مقاوم دراین شبکه‌ها بود.

---

[1] Confidentiality
[2] Non repudiation
[3] Authentication
[4] Integrity
[5] Single point of failure

۱-۲ شبکه‌های اقتضایی

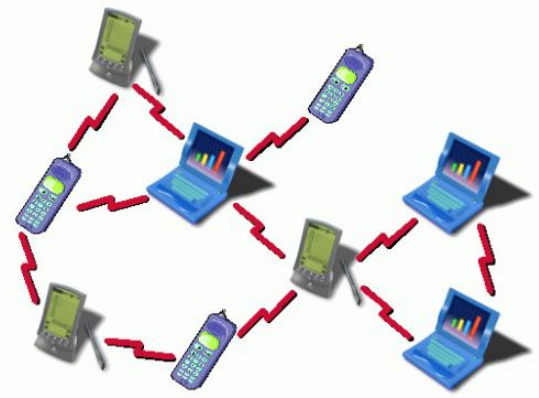
از هنگام ظهور شبکه‌های بی‌سیم از دهه هفتاد میلادی تا کنون شبکه‌های بی‌سیم گسترش زیادی در جوامع بشری داشته‌اند .در حال حاضر دو نوع شبکه بی‌سیم وجود دارد: شبکه‌های با زیر ساخت و شبکه‌های بدون زیرساخت. هر شبکه با زیر ساخت دارای یک دروازه ثابت سیمی یا یک ایستگاه پایه[1] دائمی است که از طریق خطوط سیمی به نظیر خود در شبکه‌های بی‌سیم متصل است و هر گره در این شبکه‌ها در محدوده یک ایستگاه پایه است. از جمله این شبکه‌ها می‌توان به شبکه محلی بی‌سیم[2] و تلفن موبایل اشاره کرد. در **شکل ۱-۱** نمونه‌ای از شبکه‌های داری زیر ساخت نشان داده شده است.

شکل ۱-۱: مثالی از یک شبکه دارای زیرساخت.

نوع دیگر شبکه‌های بی‌سیم که فاقد زیرساخت هستند با نام شبکه‌های اقتضایی متحرک[3] (MANET) شناخته می‌شوند. در این شبکه‌ها مسیریاب اختصاصی وجود ندارد و هر گره خود وظایف مسیریابی را انجام می‌دهد. مسئولیت تشکیل و مدیریت شبکه در بین اعضای شبکه توزیع شده است.کل شبکه قابل جابجایی است و هر گره به طور آزادانه می‌تواند از نقطه‌ای به نقطه دیگر جابجا شود. در این شبکه ممکن است برخی گره‌ها با دیگر گره‌ها رابطه مستقیم نداشته باشند، به چنین شبکه‌ای معمولا شبکه چندگامی[4] یا ذخیره-و- ارسال[5] گفته می‌شود.گره‌های اینگونه شبکه‌ها به عنوان مسیریاب عمل کرده و هر گره به نوبه خود مسئولیت کشف مسیر و نگهداری مسیرها را انجام می‌دهد. این شبکه‌ها ممکن است بر کشتی ها، هواپیماها، ماشین‌ها و بر روی افراد و یا حتی روی ادوات[6] خیلی کوچک قرار گرفته باشند. در **شکل ۱-۲** نمونه‌ای از شبکه اقتضایی نشان داده شده است.

---

[1] Base Station
[2] Local area network
[3] Mobile Ad hoc Networks
[4] Multi-hop
[5] Store-and-forward
[6] Devices



شکل ۱-۲: مثالی از یک شبکه اقتضایی متحرک.

۱-۲-۱ ویژگی های شبکه های اقتضایی

درک ویژگی‌های شبکه‌های اقتضایی امری مهم به شمار می‌رود زیرا این ویژگی‌ها تاثیر زیادی بر طراحی پروتکل-های امنیتی در این شبکه‌ها می‌گذارند.

زیرساخت شبکه

در این شبکه‌ها هیچ زیر ساخت از قبل معینی در نظر گرفته نشده است. همه وظایف مربوط به شبکه مانند مسیریابی، مدیریت شبکه و.... توسط خود گره‌های حاضر در شبکه انجام می‌گیرد. به علت کم بودن محدوده انتقال اطلاعات[۱]، انتقال اطلاعات به صورت چند گامی صورت می‌گیرد. بنابراین هر گره را می‌توان به صورت یک ماشین میزبان یا یک مسیریاب در نظر گرفت. شبکه‌های اقتضایی ممکن است به صورت خود به خود و بدون دانش قبلی نسبت به مکان فیزیکی و محیطی که در آن شبکه بر پا می‌شود، تشکیل گردند. ویژگی بدون زیر ساخت بودن شبکه‌های اقتضایی این شبکه ها را قادر می‌سازد تا سرویس‌های خاصی را که شبکه‌های معمولی قادر به انجام آن نیستند، ارائه کنند.

توپولوژی شبکه

گره‌ها در شبکه‌های اقتضایی به صورت آزادانه جابجا می‌شوند که حاصل آن توپولوژی با اتصال ضعیف است. به علت جابجایی آزادانه و غیر قابل پیش بینی گره‌ها توپولوژی شبکه نیز غیر قابل پیش بینی است. این اتصال ضعیف توپولوژی شبکه حاصل اتصال بی‌سیم گذرا است که باعث می‌شود تا گره‌ها عدم دسترسی به برخی از سرویس‌های حیاتی را تجربه کنند. جابجایی گره‌ها و اتصال بی‌سیم این اجازه را به گره‌ها می‌دهد تا به صورت خود به خود شبکه را ترک کنند و یا به شبکه بپیوندند و این باعث بی نظمی در شبکه می‌شود. سرویس‌های امنیتی باید با این تغییرات سریع و مکرر که در شبکه اتفاق می‌افتد سازگار باشند.

---

[۱] Transmission range

خود- سازماندهی[1]

از آنجا که در شبکه‌های اقتضایی هیچ مدیریت مرکزی برای انجام وظایف شبکه‌ای (مانند مسیریابی) وجود ندارد و این وظایف توسط گره‌های تشکیل دهنده شبکه صورت می‌گیرد، به این شبکه‌ها، شبکه خود-سازمان‌دهنده گفته می‌شود [۴۱].

منابع محدود

گره‌ها در شبکه‌های اقتضایی از منابع محدود تر محاسباتی، حافظه‌ای و انرژی نسبت به گره‌های شبکه‌های معمولی برخوردارند. گره‌ها در این شبکه‌ها ادوات کوچکی هستند که منعی برای جابجایی کاربران ایجاد نمی‌کنند. برای پایین نگه داشتن هزینه این وسایل معمولا در این وسایل از CPU کوچک و حاظه کوچک استفاده می‌شود. محدودیت منابع ممکن است باعث از کارافتادن گره‌ها به علت اتمام باطری شود. در شبکه‌های اقتضایی ممکن است وسایل از پهنای باند محدود و محدوده انتقال کمی برخوردار باشند. برای دست یابی به پهنای باند بیشتر نیاز به نرخ سیگنال به نویز (SNR) بیشتری می‌باشد که به نوبه خود به توان انتفالی بیشتری احتیاج دارد، و توان انتقالی بیشتر باعث مصرف بیشتر باطری می‌شود. بنابراین پروتکل‌های امنیتی در شبکه‌های اقتضایی باید به نحو مناسبی جهت مواجه با منابع محدود گره‌های تشکیل دهنده شبکه بهینه شده باشند. در غیر این صورت این پروتکل‌ها با شکست مواجه خواهند شد .

امنیت فیزیکی ضعیف

در شبکه‌های اقتضایی گره‌ها دارای قابلیت جابجایی هستند و نمی‌توان آنها را در مکان امنی مانند یک اتاق دربسته قرار داد. بنابراین این گره‌ها به خصوص در محیط‌هایی مانند قلمرو دشمن بسیار مستعد تسخیر شدن توسط دشمن هستند.

رسانه فیزیکی ضعیف

رسانه ارتباطی بی‌سیم برای هر موجودیتی که با وسایل مناسب تجهیز شده باشد قابل دسترسی است و برای دسترسی به کانال بی‌سیم محدودیتی وجود ندارد. بنابراین دشمن قادر خواهد بود تا به استراق سمع پیام‌ها پرداخته و پیام‌های جعلی را بدون هیچ محدودیتی در شبکه پخش کند.کانال مشترک و امنیت فیزیکی کم مؤیداین هستندکه سازو کارهای امنیتی باید با سرسخت‌ترین نوع دشمن (یعنی دشمن درونی و فعال) مقابله کنند.

سیستم توزیع شده

شبکه اقتضایی متحرک، یک شبکه مبتنی بر همکاری است. به این معنی که وظایف شبکه بین همه گره‌های شبکه توزیع شده است. در چنین فضایی ممکن است برخی گره‌ها به منظور صرفه جویی در مصرف انرژی خود از انجام وظایف شبکه سرباز زنند و به این رفتار گره‌ها رفتار خود خواهانه[2] گفته می‌شود. حال اگر تعداد زیادی از گره‌های

[1] Self-organizing
[2] Selfish

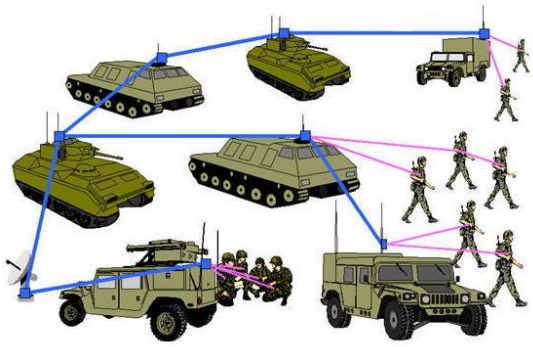
شبکه از خود رفتار خود خواهانه بروز دهند کیفیت سرویس به شدت کاهش خواهد یافت. بنابراین در این شبکه‌ها باید سازو کاری جهت مقابله با رفتار خود خواهانه گره‌ها وجود داشته باشد.

۱-۲-۲ کاربردهای شبکه های اقتضایی

برای درک طبیعت شبکه‌های اقتضایی و خاستگاه ویژگی‌های منحصر به فرد این شبکه‌ها مواردی از کاربرد این شبکه ها به صورت مختصر بیان می‌شود.

کاربردهای نظامی

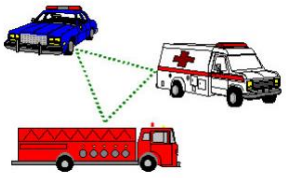
خاستگاه شبکه‌هایی که به زیرساخت‌های از قبل معین متکی نیستند به اوایل دهه هفتاد میلادی و پروژه‌های DARPA[۱] و PRENET[۲] که تمرکز آنها بر اهداف نظامی بود، برمی‌گردد. علت بکارگیری شبکه‌های اقتضایی و جذابیت آن در محیط‌های نظامی عدم نیاز به زیر ساخت از قبل معین و خود سازنده بودن این شبکه‌هاست. شبکه متداولی را در نظر بگیرید که به زیر ساختی مانند ایستگاه پایه متکی است. این زیر ساخت نقطه آسیب پذیری را معرفی می‌کند که ممکن است مورد حمله قرار بگیرد و در نتیجه کل عملیات شبکه مختل گردد. در میدان جنگ ارتباطات تضمین شده و مستحکم بسیار حیاتی هستند و در صورت تسخیر شدن شبکه ممکن است حوادث وخیمی رخ دهد. شبکه‌های اقتضایی با وجود خروج گره‌ها از شبکه به علت‌های مختلفی چون اتصال ضعیف بی‌سیم، خارج شدن از محدوده انتقال و.... همچنان می توانند به کار خود ادامه دهند. نمونه ای از کاربرد نظامی این شبکه‌ها در **شکل ۱-۳** نشان داده شده است.



شکل ۱-۳: کاربرد نظامی شبکه‌های اقتضایی متحرک.

عملیات امداد و نجات

در هنگام حوادث غیر مترقبه ممکن است زیر ساخت‌های شبکه از بین بروند، بنابراین باید بتوان شبکه‌ای را جهت عملیات امداد و نجات در سریعترین زمان ممکن برپا کرد. **شکل ۱-٤** عملیات امداد و نجات را نشان می‌دهد. در این شکل سه اتوموبیل پلیس،آتش نشانی و اورژانس جهت همکاری در عملیات امداد و نجات یک شبکه اقتضایی را بوجود آورده‌اند.



شکل ۱-٤: کاربرد شبکه‌های اقتضایی متحرک در عملیات‌های امداد و نجات.

کاربردهای اقتصادی

کاربردهای اقتصادی شبکه‌های اقتضایی گسترش اتصال در مکان‌هایی که شبکه‌های مرسوم مانند شبکه‌های سلولی از لحاظ اقتصادی نشدنی‌اند یا اینکه نمی‌توانند پوشش مناسب را بدهند، شامل می‌شود. شبکه‌های خصوصی یا شبکه‌های شخصی برای هدف‌هایی مانند ویدئو کنفرانس،ارتباط راه‌دور و.... کاربردهای محتملی از شبکه‌های اقتضایی می-باشند.

۱-۳ مفاهیم کلی امنیت

در این بخش اهم مفاهیم امنیتی مرور می‌شوند.

۱-۳-۱ مؤلفه‌های امنیتی

برای تبیین مفهوم امنیت باید به مؤلفه‌های برقراری امنیت در شبکه‌های کامپیوتری پرداخت. این مؤلفه‌ها شامل محرمانگی، صحت و دسترس‌پذیری هستند که در ادامه معرفی می‌شوند[۳].

محرمانگی

منظور از محرمانگی، عدم افشای محتوای اطلاعات ارسالی برای افراد نامحرم است. این مؤلفه موارد عدم افشای محتوای پیام‌های مبادله شده، عدم امکان تحلیل ترافیک و نیز گمنامی را شامل می‌شود.

تمامیت

صحت، اصالت داده و مبدأ داده را تأمین می‌کند. این مؤلفه موارد اصالت داده‌ها، اصالت سرچشمه داده‌ها، اصالت و حضور موجودیت‌ها و انکارناپذیری را شامل می‌شود.

دسترس‌پذیری

دسترس‌پذیری، امکان دسترسی مجاز را برای کاربران شبکه، تسهیل می‌نماید. این مؤلفه سهولت دسترسی‌های مجاز و مقابله با حملات از کاراندازی سرویس را شامل می‌شود.

۱-۳-۲ سرویس‌های امنیتی

سرویس‌های امنیتی تضمین کننده امنیت حاصل شده با استفاده از مکانیزم‌های امنیتی هستند. سرویس‌های امنیتی با بکارگیری مکانیزم‌های امنیتی مانند رمزنگاری درپی تضمین امنیت برای کاربران هستند. اهم سرویس‌های امنیتی عبارت است از احراز اصالت، حفظ صحت داده‌ها، حفظ محرمانگی داده‌ها، کنترل دسترسی، انکار ناپذیری، دسترس‌پذیری و حفظ حریم خصوصی.

۱-۳-۳ رمزنگاری

محرمانگی یک سرویس امنیتی است که باعث عدم افشای اطلاعات ارسالی برای افراد نامحرم می‌شود. سرویس محرمانگی با بکارگیری یک مکانیسم رمزنگاری مناسب حاصل می‌شود. توانایی محرمانه نگه داشتن اطلاعات وابسته به حفظ کلید رمزنگاری است. کلید رمزنگاری اطلاعاتی است که باید به همراه الگوریتم رمزنگاری به کارگرفته شود تا بتوان عملیات رمزگذاری یا رمزگشایی را انجام داد. همانند محرمانگی بسیاری دیگر از سرویس‌های امنیتی متکی بر مکانیسم‌های رمزنگاری هستند. کلیدهای رمزنگاری دارای دو نوع متفاوت است که باعث به وجود آمدن دو سیستم کاملا متفاوت رمزنگاری شده است:

سیستم رمزنگاری کلید متقارن[1]: شامل یک کلید مخفی است که بین فرستنده و گیرنده به اشتراک گذاشته می‌شود به طوری که سایر کاربران از آن اطلاعی ندارند و هر دو عملیات رمزگذاری و رمزگشایی توسط این کلید انجام می‌شود.

سیستم رمزنگاری کلید نامتقارن[2]: دراین سیستم که سیستم کلید عمومی نیز نامیده می‌شود، هر کاربر دارای یک جفت کلید خصوصی و عمومی است.کلید عمومی برای همه کاربران شبکه قابل دسترسی است و از آن برای عملیات رمزگذاری و احراز اصالت استفاده می‌شود. کلید خصوصی هر کاربر فقط برای همان کاربر قابل دسترسی است و سایر کاربران از آن اطلاعی ندارند، از این کلید برای عملیات‌های رمزگشایی و امضای دیجیتال استفاده می‌شود.

سیستم رمزنگاری کلید متقارن خود به دو دسته مبتنی بر شناسه[3] و مبتنی بر گواهینامه[4] تقسیم می‌شود. در روش‌های مبتنی بر گواهینامه، اصالت کلیدهای عمومی توسط گواهینامه کلید عمومی تأیید می‌شود. گواهینامه کلید عمومی یک داده امضا شده توسط یک طرف سوم مورد اعتماد (مرکز تولید گواهینامه[5](CA)) است که معتبر بودن

[1] Symmetric
[2] Asymmetric
[3] Identity based
[4] Certificate based
[5] Certificate Authority