

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



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



دانشگاه صنعتی اصفهان

دانشکده مهندسی برق و کامپیوتر

پایان نامه 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.

دکتر مهدی برنجکوب

۱- استاد راهنمای پایان نامه

دکتر محمد دخیل علیان

۲- استاد راهنمای پایان نامه

دکتر علی فانیان

۳- استاد داور

دکتر محمد حسین منشی

۴- استاد داور

دکتر مسعود عمومی

سرپرست تحصیلات تکمیلی

کلیه حقوق مادی مترتب بر نتایج مطالعات،  
ابتکارات و نوآوری‌های ناشی از تحقیق  
موضوع این پایان نامه متعلق به دانشگاه  
صنعتی اصفهان است. این پایان با حمایت‌های  
مادی و معنوی مرکز تحقیقات مخارات ایران  
به انجام رسیده است.

## شکر و قدردانی

خداوند! می‌خواهم تو را شکر می‌گویم به خاطر تمامی نعمت‌هایی که بر من ارزانی داشته‌ای. از اساتید ارجمندم، جناب آقای

دکتر مهدی برنجکوب و جناب آقای دکتر محمد خیل علیان که بارها به‌منی‌های دلسوزانه در طول دوران تحقیق همراه من بودند قدردانی

می‌کنم. از آقایان دکتر فانیان و دکتر نشی که زحمت دآوری این پایان‌نامه را پذیرفتند بسیار سپاسگزارم.

تقدیم به:

شهرامی دانشگاه صنعتی اصفهان

## فهرست مطالب

صفحه	عنوان
هشت	فهرست مطالب.....
دوازده	فهرست اشکال.....
سیزده	فهرست جداول.....
۱	چکیده.....

### فصل اول: مقدمه

۲	۱-۱ مقدمه.....
۳	۲-۱ شبکه‌های اقتصادی.....
۴	۱-۲-۱ ویژگی‌های شبکه اقتصادی.....
۶	۲-۲-۱ کاربردهای شبکه اقتصادی.....
۷	۳-۱ مفاهیم کلی امنیت.....
۷	۱-۳-۱ مؤلفه‌های امنیتی.....
۸	۲-۳-۱ سرویس‌های امنیتی.....
۸	۳-۳-۱ رمزنگاری.....
۹	۴-۱ مدیریت کلید در شبکه‌های اقتصادی.....
۱۰	۵-۱ مدل اعتماد در شبکه‌های اقتصادی.....
۱۱	۶-۱ انگیزه انتخاب موضوع.....
۱۲	۷-۱ هدف پایان نامه.....
۱۳	۸-۱ ساختار ادامه پایان نامه.....

### فصل دوم: رمزنگاری آستانه‌ای

۱۴	۱-۲ مقدمه.....
۱۶	۲-۲ تسهیم راز.....
۱۶	۱-۲-۲ شمای تسهیم راز با فرض وجود طرف سوم مورد اعتماد.....
۱۷	۲-۲-۲ شمای تسهیم راز با فرض عدم وجود طرف سوم مورد اعتماد.....
۱۹	۳-۲-۲ مدل دشمن.....
۱۹	۳-۲ امضای آستانه‌ای.....

- ۲-۳-۱ امضاهاى مبتنى بر سختى مسئله تجزيه اعداد ..... ۲۰
- ۲-۳-۲ امضاهاى مبتنى بر سختى حل لگارىتم گسسته ..... ۲۲
- ۲-۴ به روز رسانى سهام ..... ۲۶
- ۲-۴-۱ شماى به روز رسانى مرسوم ..... ۲۷
- ۲-۴-۲ شماهاى به روز رسانى ترتيبى ..... ۲۸
- ۲-۵ پيوستن عضو جديد به گروه ..... ۲۹
- ۲-۵-۱ روش مبتنى بر عامل مخلوط كننده ..... ۲۹
- ۲-۵-۲ روش مبتنى بر چند جمله‌اى صفر شونده ..... ۳۰
- ۲-۶ ارزيايى مقايسه‌اى مكانيزم‌هاى رمزنگارى موجود بكار رفته در TTP توزيع شده ..... ۳۱
- ۲-۷ نتيجه گيرى ..... ۳۲

#### فصل سوم: معرفى انواع مدل‌هاى اعتماد

- ۳-۱ مقدمه ..... ۳۵
- ۳-۲ معرفى طبقه‌بندى مدل‌هاى اعتماد موجود ..... ۳۵
- ۳-۲-۱ طبقه‌بندى مدل‌هاى اعتماد بر اساس مفهوم اعتماد ..... ۳۶
- ۳-۲-۲ طبقه‌بندى مدل‌هاى اعتماد بر اساس ساختار شبكه ..... ۳۷
- ۳-۳ مرجع صدور گواهينامه توزيع شده ..... ۳۸
- ۳-۳-۱ اهداف طراحى ..... ۴۰
- ۳-۳-۲ دسته‌بندى بر اساس نحوه توزيع راز (كليد خصوصى CA) بين گره‌هاى شبكه ..... ۴۱
- ۳-۳-۳ دسته‌بندى بر اساس ساختار شبكه ..... ۴۳
- ۳-۴ بررسى مدل‌هاى اعتماد توزيع شده پايه ..... ۴۵
- ۳-۴-۱ مرجع صدور گواهينامه توزيع شده جزئى ..... ۴۶
- ۳-۴-۲ مرجع صدور گواهينامه كاملا توزيع شده ..... ۴۸
- ۳-۵ نتيجه گيرى ..... ۵۱

#### فصل چهارم: عدم قابليت بكارگيرى پروتكل‌هاى به روز رسانى موجود در مدل‌هاى اعتماد توزيع شده

- ۴-۱ مقدمه ..... ۵۲
- ۴-۲ ناكارآمدى پروتكل‌هاى به روز رسانى موجود ..... ۵۳
- ۴-۲-۱ مقايس پذيرى ..... ۵۳



- ۵۵..... ۲-۲-۴ عدم سازگاری با توپولوژی متغیر شبکه
- ۵۷..... ۳-۲-۴ مسئله انتخاب گره‌های فعال
- ۵۷..... ۳-۴-۳ حمله پیشنهادی علیه پروتکل‌های به روز رسانی
- ۵۷..... ۱-۳-۴ مدل سیستم و دشمن
- ۵۸..... ۲-۳-۴ حمله پیشنهادی علیه پروتکل هرزبرگ
- ۵۹..... ۳-۳-۴ حمله پیشنهادی علیه پروتکل سان و همکاران
- ۵۹..... ۴-۳-۴ حمله پیشنهادی علیه پروتکل به روز رسانی با استفاده از یک گره فعال
- ۶۱..... ۴-۴ نتیجه گیری

#### فصل پنجم: ارائه یک پروتکل به روز رسانی مقاوم جهت بکارگیری در شبکه‌های اقتصای

- ۶۲..... ۱-۵ مقدمه
- ۶۳..... ۲-۵ نسخه اولیه پروتکل پیشنهادی
- ۶۵..... ۳-۵ حالت‌های متفاوت ارتباط بین سرویس دهنده‌ها در نسخه اولیه پروتکل پیشنهادی
- ۶۷..... ۴-۵ ارزیابی کارایی پروتکل پیشنهادی نسخه اولیه
- ۶۷..... ۱-۴-۵ مقیاس پذیری
- ۶۸..... ۲-۴-۵ سازگاری با توپولوژی متغیر شبکه
- ۶۹..... ۳-۴-۵ مسئله انتخاب گره فعال
- ۷۰..... ۵-۵ ضعف امنیتی نسخه اولیه پروتکل پیشنهادی
- ۷۰..... ۶-۵ نسخه بهبود یافته پروتکل پیشنهادی
- ۷۰..... ۱-۶-۵ روند نسخه بهبود یافته پروتکل پیشنهادی
- ۷۲..... ۲-۶-۵ ارزیابی کارآمدی نسخه بهبود یافته پروتکل پیشنهادی
- ۷۲..... ۷-۵ ارزیابی امنیتی نسخه بهبود یافته پروتکل پیشنهادی
- ۷۲..... ۱-۷-۵ مقاومت در مقابل حمله پیشنهادی
- ۷۳..... ۲-۷-۵ عدم امکان بازیابی سهام از چند جمله‌ای‌های جزئی
- ۷۴..... ۳-۷-۵ واریسی سهام دریافتی
- ۷۴..... ۸-۵ مقایسه پروتکل پیشنهادی با سایر پروتکل‌های به روز رسانی
- ۷۴..... ۱-۸-۵ مقایسه ویژگی‌های کارآمدی
- ۷۵..... ۲-۸-۵ مقایسه حجم محاسبات و ارتباطات روش پیشنهادی با سایر روش‌ها

۷۷..... ۳-۸-۵ مقایسه ویژگی های امنیتی

۷۸..... ۹-۵ نتیجه گیری

#### فصل ششم: ارائه یک مدل اعتماد توزیع شده مقاوم

۸۱..... ۱-۶ مقدمه

۸۲..... ۲-۶ مدل سیستم

۸۲..... ۱-۲-۶ مدل شبکه

۸۴..... ۲-۲-۶ مدل دشمن

۸۴..... ۳-۶ تسهیم راز

۸۶..... ۴-۶ روند دریافت گواهینامه در مدل پیشنهادی

۸۸..... ۵-۶ اضافه شدن سرویس دهنده جدید به گروه

۸۹..... ۶-۶ برقراری یک دسته جدید از گره های سرویس دهنده کمکی توسط سرویس دهنده های اصلی

۹۰..... ۷-۶ به روز رسانی سهام

۹۱..... ۸-۶ ارزیابی مدل اعتماد پیشنهادی

۹۱..... ۱-۸-۶ دسترس پذیری

۹۲..... ۲-۸-۶ سازگاری با توپولوژی متغیر شبکه

۹۲..... ۳-۸-۶ امنیت

۹۳..... ۴-۸-۶ حجم محاسبات و ارتباطات

۹۵..... ۹-۶ مقایسه مدل پیشنهادی با مدل های پایه

۹۷..... ۱۰-۶ نتیجه گیری

#### فصل هفتم: نتیجه گیری

۹۹..... ۱-۷ مقدمه

۹۹..... ۲-۷ مرور مطالب

۱۰۱..... ۳-۷ نوآوری ها

۱۰۲..... ۴-۷ پیشنهادات ادامه کار

۱۰۳..... پیوست: فهرست الفبایی واژگان و اصطلاحات تخصصی

۱۰۶..... فهرست مراجع

## فهرست اشکال

صفحه	عنوان
۳	شکل ۱-۱: مثالی از یک شبکه دارای زیرساخت
۴	شکل ۲-۱: مثالی از یک شبکه اقتضایی متحرک
۶	شکل ۳-۱: کاربرد نظامی شبکه‌های اقتضایی متحرک
۷	شکل ۴-۱: کاربرد شبکه‌های اقتضایی متحرک در عملیات‌های امداد و نجات
۲۱	شکل ۱-۲: الگوریتم استخراج گواهینامه از روی گواهینامه نامزد
۲۶	شکل ۲-۲: پنجره آسیب‌پذیری، هر جعبه سیاه نمایانگر انجام عملیات به روز رسانی سهام است
۳۷	شکل ۱-۳: طبقه‌بندی انواع مدل‌های اعتماد بر اساس مفهوم اعتماد
۳۸	شکل ۲-۳: انواع مدل‌های اعتماد بر اساس ساختار شبکه
۴۵	شکل ۳-۳: طبقه‌بندی انواع روش‌های برقراری مرجع صدور گواهینامه توزیع شده
۴۷	شکل ۴-۳: روند دریافت گواهینامه در روش ژو و همکاران ( $t=4, n=6$ )
۴۹	شکل ۵-۳: روند دریافت سرویس گواهینامه به کمک $t-1$ گره همسایه
۵۶	شکل ۱-۴: ناسازگاری شمای به روز رسانی مرسوم با تفکیک شبکه‌های اقتضایی
۶۳	شکل ۱-۵: تقسیم طول عمر شبکه به چند بازه زمانی مساوی
	شکل ۲-۵: نمایی کلی از شبکه اقتضایی، راز سیستم با یک شمای تسهیم راز آستانهای (۱۰،۳) بین گره‌های سرویس‌دهنده تسهیم شده است
۶۶	
۶۹	شکل ۳-۵: تفکیک شبکه به دو زیر شبکه مجزا
۸۱	شکل ۱-۶: شبکه اقتضایی با کاربرد نظامی در مقیاس وسیع
	شکل ۲-۶: توزیع یک سهم از راز سیستم با استفاده از یک شمای تسهیم راز $(k, m)$ بین هر دسته از گره‌های سرویس‌دهنده کمکی
۸۳	

## فهرست جداول

<u>صفحه</u>	<u>عنوان</u>
۱۵	جدول ۱-۲: نمادهای بکار گرفته شده در رمزنگاری آستانهای.....
۳۳	جدول ۲-۲: مقایسه مکانیسم‌های رمزنگاری بکار گرفته شده در TTP توزیع شده.....
۳۴	جدول ۳-۲: ویژگی‌های رمزنگاری در برخی از روش‌های برقراری DCA.....
۳۹	جدول ۱-۳: مقایسه مراجع صدور گواهینامه متمرکز و توزیع شده.....
۴۳	جدول ۲-۳: مقایسه بین PDCA و FDCA.....
۶۳	جدول ۱-۵: نمادهای بکاررفته در پروتکل پیشنهادی.....
۷۵	جدول ۲-۵: مقایسه ویژگی‌های کارآمدی پروتکل پیشنهادی با سایر پروتکل‌ها.....
۷۶	جدول ۳-۵: مقایسه حجم محاسبات و ارتباطات روش پیشنهادی با سایر روش‌ها.....
۷۸	جدول ۴-۵: مقایسه ویژگی‌های امنیتی پروتکل پیشنهادی با سایر پروتکل‌های به روز رسانی.....
۹۳	جدول ۱-۶: تعداد نمارسانی‌های هر گره برای عملیات‌های موجود در مدل اعتماد پیشنهادی.....
۹۵	جدول ۳-۶: تعداد پیام‌های ارسالی برای عملیات‌های موجود در مدل اعتماد پیشنهادی.....
۹۶	جدول ۳-۶: مقایسه مدل پیشنهادی با مدل‌های پایه.....

## چکیده

شبکه اقتضایی متحرک یک شبکه بی سیم متشکل از گره‌های متحرک است که برخلاف شبکه‌های مرسوم به هیچ گونه زیرساخت از قبل معین و مدیریت متمرکز 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، معمولاً 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 گره‌های شبکه که سرویس دهنده نامیده می‌شوند، تسهیم می‌شود. تسهیم کلید خصوصی به گونه‌ای انجام می‌گیرد که برای بازیابی راز باید حداقل تعداد آستانه‌ای از سرویس دهنده با هم همکاری داشته باشند. تسهیم راز به تنهایی برای مقابله با دشمن متحرک که قصد تسخیر آستانه‌ای از سرویس دهنده‌ها 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 گونه‌ای است که سرویس دهنده‌ها در دسته‌های مستقل متشکل از آستانه‌ای از سرویس دهنده‌ها 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<sup>۱</sup>، عدم انکار<sup>۲</sup>، احراز اصالت<sup>۳</sup>، تمامیت<sup>۴</sup> 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، معمولاً 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<sup>۵</sup> می‌شود. بنابراین باید به دنبال راه‌حل مناسبی جهت برقراری یک مدل اعتماد مقاوم در این شبکه‌ها بود.

---

<sup>1</sup> Confidentiality

<sup>2</sup> Non repudiation

<sup>3</sup> Authentication

<sup>4</sup> Integrity

<sup>5</sup> Single point of failure

## ۲-۱ 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 زیر ساخت. هر شبکه با زیر ساخت دارای یک دروازه ثابت سیمی یا یک ایستگاه پایه<sup>۱</sup> 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<sup>۲</sup> و تلفن موبایل اشاره کرد. در شکل ۱-۱ نمونه‌ای از شبکه‌های دارای زیر ساخت نشان داده شده است.



شکل ۱-۱: مثالی از یک شبکه دارای زیر ساخت.

نوع دیگر شبکه‌های بی‌سیم که فاقد زیر ساخت هستند با نام شبکه‌های اقتضایی متحرک<sup>۳</sup> (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 معمولاً شبکه چندگامی<sup>۴</sup> یا ذخیره‌و-ارسال<sup>۵</sup> 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 کشتی‌ها، هواپیماها، ماشین‌ها و بر روی افراد و یا حتی ادوات<sup>۶</sup> خیلی کوچک قرار گرفته باشند. در شکل ۲-۱ نمونه‌ای از شبکه اقتضایی نشان داده شده است.

<sup>1</sup> Base Station

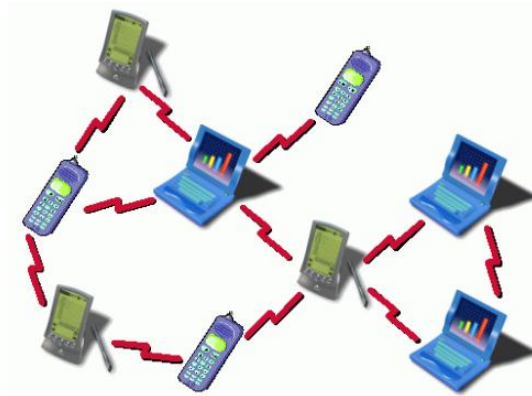
<sup>2</sup> Local area network

<sup>3</sup> Mobile Ad hoc Networks

<sup>4</sup> Multi-hop

<sup>5</sup> Store-and-forward

<sup>6</sup> Devices



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

### ۱-۲-۱ ویژگی های شبکه های اقتضایی

درک ویژگی های شبکه های اقتضایی امری مهم به شمار می رود زیرا این ویژگی ها تاثیر زیادی بر طراحی پروتکل-های امنیتی در این شبکه ها می گذارند.

#### زیرساخت شبکه

در این شبکه ها هیچ زیر ساخت از قبل معینی در نظر گرفته نشده است. همه وظایف مربوط به شبکه مانند مسیریابی، مدیریت شبکه و... توسط خود گره های حاضر در شبکه انجام می گیرد. به علت کم بودن محدوده انتقال اطلاعات<sup>۱</sup>، انتقال اطلاعات به صورت چند گامی صورت می گیرد. بنابراین هر گره را می توان به صورت یک ماشین میزبان یا یک مسیریاب در نظر گرفت. شبکه های اقتضایی ممکن است به صورت خود به خود و بدون دانش قبلی نسبت به مکان فیزیکی و محیطی که در آن شبکه بر پا می شود، تشکیل گردند. ویژگی بدون زیر ساخت بودن شبکه های اقتضایی این شبکه ها را قادر می سازد تا سرویس های خاصی را که شبکه های معمولی قادر به انجام آن نیستند، ارائه کنند.

#### توپولوژی شبکه

گره ها در شبکه های اقتضایی به صورت آزادانه جابجا می شوند که حاصل آن توپولوژی با اتصال ضعیف است. به علت جابجایی آزادانه و غیر قابل پیش بینی گره ها توپولوژی شبکه نیز غیر قابل پیش بینی است. این اتصال ضعیف توپولوژی شبکه حاصل اتصال بی سیم گذرا است که باعث می شود تا گره ها عدم دسترسی به برخی از سرویس های حیاتی را تجربه کنند. جابجایی گره ها و اتصال بی سیم این اجازه را به گره ها می دهد تا به صورت خود به خود شبکه را ترک کنند و یا به شبکه بپیوندند و این باعث بی نظمی در شبکه می شود. سرویس های امنیتی باید با این تغییرات سریع و مکرر که در شبکه اتفاق می افتد سازگار باشند.

<sup>۱</sup> Transmission range



### خود-سازماندهی ۱

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 معمولاً در این وسایل از CPU کوچک و حافظه کوچک استفاده می‌شود. محدودیت منابع ممکن است باعث از کارافتادن گره‌ها به علت اتمام باتری 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 انتقالی بیشتری احتیاج دارد، و توان انتقالی بیشتر باعث مصرف بیشتر باتری می‌شود. بنابراین پروتکل‌های امنیتی در شبکه‌های اقتضایی باید به نحو مناسبی جهت مواجهه 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 مؤید این هستند که 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<sup>۲</sup> گفته می‌شود. حال اگر تعداد زیادی از گره‌های

<sup>۱</sup> Self-organizing

<sup>۲</sup> Selfish

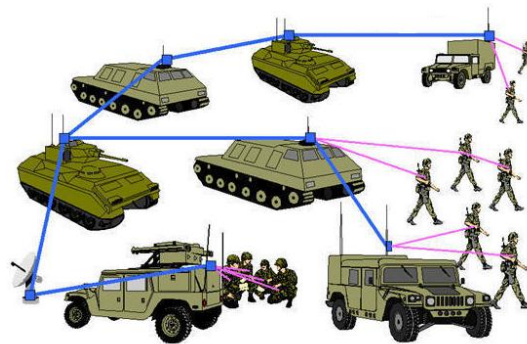
شبکه از خود رفتار خود خواهانه بروز دهند کیفیت سرویس به شدت کاهش خواهد یافت. بنابراین در این شبکه‌ها باید سازو کاری جهت مقابله با رفتار خود خواهانه گره‌ها وجود داشته باشد.

### ۲-۲-۱ کاربردهای شبکه‌های اقتضایی

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

#### کاربردهای نظامی

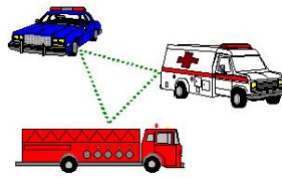
خاستگاه شبکه‌هایی که به زیرساخت‌های از قبل معین متکی نیستند به اوایل دهه هفتاد میلادی و پروژه‌های DARPA [۱] و PRENET [۲] که تمرکز آنها بر اهداف نظامی بود، برمی‌گردد. علت بکارگیری شبکه‌های اقتضایی و جذابیت آن در محیط‌های نظامی عدم نیاز به زیرساخت از قبل معین و خود سازنده بودن این شبکه‌هاست. شبکه متداولی را در نظر بگیرید که به زیرساختی مانند ایستگاه پایه متکی است. این زیرساخت نقطه آسیب‌پذیری 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 می‌توانند به کار خود ادامه دهند. نمونه‌ای از کاربرد نظامی این شبکه‌ها در شکل ۳-۱ نشان داده شده است.



شکل ۳-۱: کاربرد نظامی شبکه‌های اقتضایی متحرک.

#### عملیات امداد و نجات

در هنگام حوادث غیر مترقبه ممکن است زیرساخت‌های شبکه از بین بروند، بنابراین باید بتوان شبکه‌ای را جهت عملیات امداد و نجات در سریعترین زمان ممکن برپا کرد. شکل ۴-۱ عملیات امداد و نجات را نشان می‌دهد. در این شکل سه اتوموبیل پلیس، آتش‌نشانی و اورژانس جهت همکاری در عملیات امداد و نجات یک شبکه اقتضایی را بوجود آورده‌اند.



شکل ۱-۴: 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 نشدنی اند یا اینکه نمی‌توانند پوشش مناسب را بدهند، شامل می‌شود. شبکه‌های خصوصی یا شبکه‌های شخصی برای هدف‌هایی مانند ویدئو کنفرانس، ارتباط راه‌دور و... کاربردهای احتمالی از شبکه‌های اقتضایی می‌باشند.

### ۳-۱ 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.

### ۲-۳-۱ سرویس‌های امنیتی

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

### ۳-۳-۱ رمزنگاری

محرمانگی یک سرویس امنیتی است که باعث عدم افشای اطلاعات ارسالی برای افراد نامحرم می‌شود. سرویس محرمانگی با بکارگیری یک مکانیزم 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 کار گرفته شود تا بتوان عملیات رمزگذاری یا رمزگشایی را انجام داد. همانند محرمانگی بسیاری دیگر از سرویس‌های امنیتی متکی بر مکانیزم‌های رمزنگاری هستند. کلیدهای رمزنگاری دارای دو نوع متفاوت است که باعث به وجود آمدن دو سیستم کاملاً متفاوت رمزنگاری شده است:

سیستم رمزنگاری کلید متقارن<sup>۱</sup>: 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<sup>۲</sup>: در این 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<sup>۳</sup> و مبتنی بر گواهینامه<sup>۴</sup> 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<sup>۵</sup> (CA)) است که معتبر بودن

<sup>1</sup> Symmetric

<sup>2</sup> Asymmetric

<sup>3</sup> Identity based

<sup>4</sup> Certificate based

<sup>5</sup> Certificate Authority