دانشگاه اراک

دانشکده فنی و مهندسی

کارشناسی ارشد مهندسی کامپیوتر

ارائه پروتکلی برای مقابله با حمله لانه‌کرمی در شبکه‌های اقتضایی سیار

پژوهشگر

ایرج اصولی

استاد راهنما

دکتر فاخته سلطانی

استاد مشاور

دکتر وحید رافع

دی ماه ۱۳۹۲

بسم ا... الرحمن الرحیم

عنوان پایان نامه

ارائه پروتکلی برای مقابله با حمله لانه‌کرمی در شبکه‌های اقتضایی سیار

توسط:

ابرج اصولی

پایان نامه

ارائه شده به مدیریت تحصیلات تکمیلی به عنوان بخشی از فعالیت های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته مهندسی کامپیوتر

از

دانشگاه اراک

اراک-ایران

ارزیابی و تصویب شده توسط کمیته پایان نامه با درجه: ....

دکتر فاخته سلطانی (استاد راهنما) ....

دکتر وحید رافع (استاد مشاور) ....

دکتر رضا رافع (استاد داور) ....

تاریخ: ....

ت

تقدیم به آنها که سبزی وجودشان امید بودن من است.

با سپاس فراوان از اساتید گرامی سرکار خانم دکتر فاخته سلطانی و جناب آقای دکتر وحید رافع که پیمودن این راه بدون یاری و راهنمایی‌های بیدریغشان ممکن نبود.

چکیده

شبکه‌های اقتضایی سیار، شبکه‌هایی هستند که گره‌های شبکه متحرک می‌باشند و زیر ساخت ثابتی ندارند. برخلاف شبکه‌های بی‌سیم معمول که از طریق یک ایستگاه پایه با یکدیگر ارتباط برقرار می‌کنند، در شبکه‌های اقتضایی چنین زیر ساختی وجود ندارد و گره‌ها در این شبکه برای برقراری ارتباط متکی به همکاری یکدیگر هستند. از طرف دیگر سادگی در برپایی چنین شبکه‌هایی مستقل از هر مکان و زمانی، روز به روز به محبوبیت این شبکه‌ها می‌افزاید. هرچند، اطمینان از عملکرد درست و تامین امنیت و ... از جمله مسائلی هستند که در خصوص این شبکه‌ها باید مد نظر قرار بگیرند.

حمله لانه‌کرمی یکی از شدیدترین حملاتی است که امنیت شبکه را تهدید می‌کند. این پایان نامه بر روی حمله لانه‌کرمی متمرکز می‌شود و یک پروتکل مسیریابی امن مبتنی بر پروتکل مسیریابی AODV، به نام WBRP (پروتکل مسیریابی دورزنی حمله لانه‌کرمی) را ارائه می‌دهد. WBRP از مقدار آستانه استفاده نمی‌کند و یک مسیر امن برای دور زدن گره‌های بداندیش فراهم می‌کند. بر اساس ویژگی‌هایی که یک حمله لانه‌کرمی دارد، پروتکل پیشنهادی هر گره موجود در شبکه را قادر به تصمیم‌گیری در تبادل بسته‌های مسیریابی در میان همسایه‌های خود می‌سازد. هر گره می‌تواند با محاسبه ضریب تغییرات زمان رفت و برگشت بسته Hello در میان همسایه‌های خود گره مظنون را تشخیص بدهد و آن را از شرکت در مسیریابی از جانب خود محروم کند، در نهایت مسیر امنی بدست آید. نتایج شبیه-سازی توسط شبیه‌ساز NS2 نحوه کارکرد این پروتکل را نشان می‌دهد، این پروتکل در برابر حمله لانه‌کرمی از مقاومت لازم و خوبی برخوردار است و نرخ بسته‌های حذف شده توسط گره‌های بداندیش را کاهش می‌دهد.

کلمات کلیدی : شبکه‌های اقتضایی سیار، پروتکل مسیریابی بنا به اقتضای AODV، حملات لانه‌کرمی، ضریب تغییرات

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

فصل

۱- مقدمه

مقدمه

شبکه‌های کامپیوتری از نظر دیدگاه اجتماعی یک پدیده‌ی فرهنگی و از دیدگاه مهندسی کامپیوتر یک تخصص و علم تلقی می‌شود. پیشرفت و توسعه در مرزهای دانش، گواه این است که شبکه‌های کامپیوتری به بخش جدایی ناپذیری از زندگی تبدیل شده‌اند. سرمایه گذاری گسترده‌ی دولت‌ها در زمینه شبکه‌های کامپیوتری برای ایجاد یک بستر ارتباطی، باعث پدید آمدن شبکه‌های گسترده (WAN یا Wide-Area-Network) شد. به طوریکه دیگر محدودیت مکانی و جغرافیایی، ... مفهومی نداشت و شرایط برای اتصال همگانی و ارتباط با همدیگر فراهم شده بود.

در این راستا شبکه‌های بی‌سیم، خواه سلولی و یا شبکه‌های بی‌سیم محلی، به سرعت نقش بسزایی در برقراری ارتباط در بین افراد پیدا کردند. ارتباط بی‌سیم دیجیتال یک ایده‌ی جدیدی نیست. در اوایل ۱۹۰۱، یک فیزیکدان ایتالیایی گوگلیمو مارکونی یک تلگراف بی‌سیم ship-to-shore که از مورس بهره می‌برد را ارائه داد. استفاده گسترده از این شبکه‌ها در ادارات، منازل، مراکز علمی، نقاط نظامی، هتل‌ها و همچنین فرودگاه‌ها و غیره گواه اهمیت این شبکه‌ها می‌باشد. از طرفی رشد تکنولوژی سخت افزار و ادوات لازم برای ارتباطات باعث دسترسی گسترده به دستگاه‌های بی‌سیم همچون تلفن‌های سیار، حسگرها و رایانه‌های جیبی (Pocket PC) شده است، که به نوبه‌ی خود افزایش تقاضا را برای ارتباطات بی‌سیم با نرخ ارسال اطلاعات بالا، مثلا ارسال جریان‌های داده‌ای چند رسانه‌ای روی تلفن‌های همراه یا اتصال کامپیوترهای دستی به اینترنت، را در پی دارد.

با وجود فعالیت‌های گسترده در زمینه شبکه‌های کامپیوتری، ارتباطات بی‌سیم بیشترین توجه را به خود جلب کرده‌اند، ولی آنچه که اخیرا توجه محققین را به خود معطوف کرده است شبکه‌های بی‌سیمی است که بدون زیرساخت ثابت و از قبل تعریف شده‌ای ایجاد می‌شوند. در این پایان نامه این نوع از شبکه‌ها مورد بحث واقع شده‌اند. شبکه‌های اقتضایی سیار به خاطر عدم نیاز به زیرساختار ثابت و بستر پرهزینه، امروزه بیشتر مورد توجه قرار گرفته‌اند. در شبکه‌های اقتضایی یک گره به محض ورود به فضای تحت پوشش به صورت پویا به شبکه اضافه می‌شود. مثالی از این مورد Bluetooth است.

تفاوت میان شبکه‌های اقتضایی و شبکه‌های محلی بی‌سیم (WLAN) در ساختار مجازی آن‌ها است. به عبارت دیگر، ساختار مجازی شبکه‌های محلی بی‌سیم بر پایه‌ی طرحی ایستا است، در حالی که شبکه‌های اقتضایی از هر نظر پویا هستند. در کنار مزایایی که این پویایی برای استفاده‌کنندگان فراهم می‌کند، حفظ امنیت را نیز با چالش‌های بسیاری همراه می‌کند.

همچون WLANها، شبکه‌های اقتضایی برای برقراری ارتباط بی‌سیم در یک حیطه جغرافیایی محدود منظور شده‌اند. بیشتر شبکه‌های اقتضایی یک حیطه‌ی کوچکتر از WLANها را پوشش می‌دهند اما این آنچه که شبکه‌های اقتضایی را از WLANها متمایز می‌کند، نیست. بیشتر خصیصه‌های برجسته‌ی MANET[1] برخلاف WLAN می‌باشند، آن‌ها به هیچ زیرساختار ثابتی برای برقراری ارتباط متکی نیستند.

در شبکه‌های اقتضایی معمولا نقطه دسترسی، تقویت‌کننده و یا اداره مرکزی وجود ندارد. حال آنکه شبکه‌های بی‌سیم محلی که تا هم اکنون کاربرد وفوری دارند همیشه دارای زیرساختار سیمی ایستاتیک می‌باشند، که عمدتا در این شبکه‌ها تعدادی مسیریاب به تعدادی گره مشتری سرویس می‌دهند. که در مقابل، گره‌های موجود در شبکه اقتضایی قابلیت عمل کردن به عنوان مسیریاب را دارند.

با توجه به محدودیت‌ها در این نوع شبکه، عدم وجود زیرساختار قابل دسترس، تغییر سریع و غیر قابل پیش‌بینی بودن توپولوژی، پروتکل‌های مسیریابی در این نوع از شبکه‌ها با چالش‌هایی روبرو هستند. بدون هیچ زیرساختار مسیریابی گره‌های تشکیل‌دهنده شبکه اقتضایی خودشان به عنوان مسیریاب عمل می‌کنند. با وجود اهمیت مسلم مسیریابی، شگفت‌آور نخواهد بود که مسیریابی مبنایی برای طبقه‌بندی شبکه‌های اقتضایی در دو گروه باشد [1]: تک‌پرشی (single-hop) و چندپرشی (multi-hop).

در شبکه‌های اقتضایی تک‌پرشی، گره‌ها به عنوان مسیریاب عمل نمی‌کنند و بنابراین ارتباط فقط ما بین گره‌هایی ممکن است که در بازه‌ی فرکانس رادیویی یکدیگر باشند همچون بلوتوث. از طرف دیگر شبکه‌های چندپرشی شبکه‌هایی هستند که گره‌ها مایل به فعالیت به عنوان مسیریاب هستند و ترافیک دیگر گره‌ها را به جلو می‌رانند یا مسیریابی می‌کنند [1].

پروتکل‌های مسیریابی فراوانی برای شبکه‌های اقتضایی پیشنهاد شده است. هر پروتکل روش خاص خود را دارد که این مبانی طراحی در پروتکل بر اساس یک فرض ساده یا روش‌های پیچیده و محاسباتی می‌باشد. به عنوان مثال در بسیاری از این پروتکل‌های طرح شده، فرض بر این است که شرایط خاصی حاکم می‌باشد و قابلیت‌های یکسانی را می‌توان در نظر گرفت.

علاوه بر عدم وجود زیرساختار قابل دسترس و همچنین تغییر سریع و غیرقابل پیش بینی توپولوژی، کمبود توان باتری، پهنای باند محدود، میزان خطای زیاد، ازدحام داده از مسائل اساسی شبکه‌های اقتضایی است. با توجه به محدودیت‌های مذکور، پروتکل‌های مسیریابی که برای این گونه از شبکه‌ها طراحی می‌شوند، باید به گونه‌ای باشند که این مسائل را در خود جای بدهند. یعنی مبنای طراحی برخی از پروتکل‌ها می تواند در صرفه جویی توان باتری گره‌ها یا کمینه کردن میزان سربارهای پردازشی باشد و همچنین می‌توان عوامل اجتناب از حشو همچون بسته‌های سیل‌آسا (که خود عامل کاهش پهنای باند است) را در طراحی مد نظر قرار داد.

[1] Mobile Ad hoc NETwork

شبکه‌های اقتضایی همچون سایر شبکه‌های بی‌سیم و سیمی برای بقای حیات خود و ارائه سرویس به کاربران باید بتوانند در مقابل حملات مقاوم باشند. از آنجایی که پروتکل‌های مسیریابی معمولا با هدف صرفا مسیریابی و یافتن کوتاهترین مسیر طراحی می‌شوند، اهداف امنیتی را در خود جای نمی‌دهند و در برابر گره‌های بداندیش به شدت آسیب‌پذیرند. این آسیب‌پذیری در شبکه‌های اقتضایی بیشتر به چشم می‌آید، از آنجایی که پروتکل‌های مسیریابی در شبکه‌های اقتضایی بیشتر به قصد کمینه کردن سربار بسته‌ها طراحی شده‌اند و گره‌های موجود در شبکه را گره خوب فرض کرده‌اند. یک پروتکل مسیریابی بدون در نظر گرفتن اهداف امنیتی با وجود کارایی بالاتر در نوع خود، آسیب پذیری بیشتری را دارد و یک گره می‌تواند تهدیدی برای امنیت سیستم محسوب شود و تاثیر قابل توجهی بر عملکرد سیستم داشته باشد.

همانطور که ذکر شد، مسیریابی یک چالش بزرگ برای شبکه‌های چندپرشی اقتضایی می‌باشد که این بدلیل تکیه بر گره‌های موجود در شبکه برای مسیریابی و ویژگی‌های خود این شبکه می‌باشد. حیرت آور نخواهد بود که تضمین امنیت مسیریابی حتی یک چالش بزرگتری محسوب شود.

امنیت، سرویس حیاتی برای ارتباطات شبکه سیمی و بی‌سیمی است. موفقیت و عملکرد درست شبکه در وجود امنیت است و بدون آن تضمینی برای عملکرد صحیح و ارائه سرویس‌های مورد نظر شبکه وجود ندارد. مسیریابی، جلورانی بسته‌های داده، نگهداری مسیر و بروز رسانی اطلاعات مسیر از جمله توابع مهم شبکه‌های اقتضایی می‌باشند که می‌توانند مورد حمله واقع شوند و شبکه را تحت تاثیر قرار بدهند.

شبکه‌های بی‌سیم اقتضایی سیار بدلیل ماهیتی که دارند نسبت به شبکه‌های سیمی بیشتر مورد حملات قرار می‌گیرند. اول اینکه از لینک‌های ارتباطی بی‌سیم استفاده می‌کنند و این خود باعث می‌شود که شبکه در معرض بدرفتاری‌های گسترده‌ای قرار بگیرد. بدلیل باز بودن محیط بی‌سیم، کنترلی روی حضور گره‌ها وجود ندارد. از این رو شبکه می‌تواند از هر سویی مورد حمله قرار بگیرد. حملات و آسیب‌ها می‌توانند شنود غیر فعال، نشت اطلاعات محرمانه، جعل هویت گره‌ها، مصالحه‌ی یک گره خوب جهت دسترسی به کلیدهای احراز هویتی باشند. علاوه بر ماهیت ذاتی شبکه که بدلیل بی‌سیمی بودن دارا است می‌توان به خصوصیات دیگر این شبکه اشاره کرد که به نوبه‌ی خود بر چالش‌های امنیتی دامن می‌زنند.

حرکت خود مختارانه گره‌ها در شبکه اقتضایی این مفهوم را می‌رساند که شبکه و گره‌ها فاقد حفاظت فیزیکی مناسب هستند و براحتی می‌توانند مورد حملات خارجی قرار بگیرند، مگر اینکه قواعد خاص برای حرکت گره‌ها در نظر گرفت که در برخی موارد غیرعملی می‌باشد. از طرف دیگر در شبکه‌های اقتضایی هیچ گره مرکزی وجود ندارد، در واقع شبکه ماهیت غیرمتمرکزی را دارد که این باعث می‌شود برای عملکرد شبکه به همکاری گره‌ها متکی باشیم. فرض اینکه هر گره به خوبی عمل خود را انجام خواهد داد و همکاری مورد نظر را برآورد خواهد کرد از مواردی می‌باشد که یقین صد درصدی را نمی‌تواند داشته باشد. هر حمله‌ای می تواند به این مشارکت آسیب برساند و کارکرد شبکه را مختل کند.

از آنجا که در شبکه‌های اقتضایی گره‌ها با محدودیت منابعی همچون پهنای باند و توان محاسباتی و مصرفی مواجهند، رفتار خود خواهانه اجتناب ناپذیر می‌باشد. گره‌های خودخواه، گره‌هایی هستند که در عملیات شبکه همچون

مسیریابی و جلورانی بسته‌های داده شرکت نمی‌کنند و منابع خود را در جهت اهداف خودشان بکار می‌برند. این گره‌ها از مشارکت در توابع شبکه خودداری می‌کنند اما از منابع شبکه برای رسیدن به اهداف خود استفاده می‌کنند. خودخواهی گره‌ها می‌تواند اثر مخربی روی شبکه داشته باشد. از جمله آثار مخرب می‌توان به کاهش کارآیی شبکه، اعمال مصرف توان بیشتر به گره‌های خوش‌رفتار، چند تکه شدن شبکه، عدم شناسایی موفقیت آمیز مسیرهای موجود، از دست رفتن داده‌ها با این فرض که مسیر وجود دارد، اشاره کرد. خودخواهی باعث می‌شود بر روی گره‌های خوش رفتار فشار کاری بالایی اعمال شود و این خود باعث می شود که عدالت در شبکه از بین برود.

حمله لانه‌کرمی از پیچیده‌ترین و ماهرانه‌ترین حملات فعال در شبکه می‌باشد. در این نوع حمله دو گره بدخواه در شبکه با تبانی یکدیگر ایجاد تونلی به نام لانه‌کرمی می‌کنند. این نوع حمله با انتشار اخبار دروغین مسیریابی، که شامل نزدیکترین مسیر به مقصد می‌باشند، ترافیک شبکه را به سمت خود می‌کشاند. گره‌های بدخواه با جذب ترافیک به سمت خود می‌توانند حملاتی از قبیل دور ریختن بسته‌های داده، دستکاری، آنالیز و شنود را انجام دهند. این حمله سبب می شود که ارتباط در شبکه به شدت مختل شود. شناسایی حمله لانه‌کرمی بدلیل پیچیده بودن و پنهانی بودن دشوار است.

وجود یک ساختار اعتماد یا زیرساخت مدیریتی و یک شخص ثالث در شبکه‌های بی‌سیم و سیمی، این امکان را مهیا می‌کنند که بر رفتار گره‌ها نظارت شود. وجود زیرساختارهای رمزنگاری مانند تولید، پخش کلید مشترک و احراز هویت، شناسایی و مقابله با بدرفتاری را آسان ساخته است. حال آنکه در شبکه‌های اقتضایی سیار توپولوژی متغیر و نبود زیرساخت پشتیبانی دسترسی به بسیاری از مکانیزم‌های رمزنگاری را بی‌ثمر می‌سازد، آنچه که ذکر شد گواه بر این است که مساله‌ی پیاده سازی امنیت درچنین شبکه‌ای چالش برانگیز است. طبیعت شبکه از جمله: توپولوژی متغیر و غیرقابل پیش‌بینی بودن، عدم وجود زیرساخت مود اطمینان از پیش تعریف شده، برابری و یکسان بودن گره‌ها نسبت به همدیگر و عدم برتری یک گره نسبت به سایرین (فقدان مرکز مدیریتی، بازرسی) باعث شده‌اند که روش‌های پیشنهادی مبتنی بر رمزنگاری برای این شبکه مناسب نباشند.

در این پایان‌نامه به بررسی حملات و تهدیدات امنیتی شبکه‌های اقتضایی پرداخته شده است و با استفاده از راهکار آماری به ارائه راه‌حلی پرداخته می‌شود که گره‌ها را در تمام نقاط شبکه قادر به تصمیم‌گیری در مورد شرکت کردن همسایه خود در مسیریابی از جانب خود می‌کند. در فصل دوم پایان‌نامه مبانی و خصوصیات شبکه‌های اقتضایی سیار، اهمیت، پیشینه و ویژگی‌های شبکه، چالش‌ها و محدودیت‌های طراحی بررسی می‌شوند. فصل سوم به مسیریابی و امنیت شبکه‌های اقتضایی می‌پردازد. پس از بررسی چالش‌های امنیتی به معرفی پروتکل‌های مسیریابی و حملات در شبکه‌های اقتضایی پرداخته می‌شود. فصل چهارم به اقدامات متقابل امنیتی ارائه شده برای مقابله با حملات امنیتی متمرکز می‌شود. پس از بررسی طرح‌های مسیریابی امن، در فصل پنجم به کنکاش راهکارهای ارائه شده در مقابله با حمله لانه‌کرمی مبتنی بر روش‌های سخت‌افزاری یا دیده‌بانی و دیگر موارد پرداخته می‌شود.

فصل ششم راهکار WBRP را به عنوان یک پروتکل مسیریابی امن در مقابله با حمله لانه‌کرمی ارائه می‌دهد با بررسی نتایج آزمایش‌ها ایمن بودن پروتکل پیشنهادی در مقابل حمله لانه‌کرمی به اثبات می‌رسد که نسبت به دیگر

راهکارهای مقدار آستانه‌ای یا سخت افزاری برتری دارد. در پایان، در فصل هفتم پس از نتیجه‌گیری کلی پیشنهادی برای ادامه پژوهش ارائه داده شده است.

فصل

۲- مبانی و خصوصیات شبکه های اقتضایی سیار

۲-۱- مقدمه

با توسعه و رشد در زمینه‌ی تجهیزات ارتباطی و مخابراتی بی‌سیم، دنیا دچار تحولی شگرف در زمینه‌ی ارتباطات شد. توجه دولت‌ها در ایجاد یک زیرساختار ارتباطی، باعث پدید آمدن شبکه‌های گسترده‌ای شد. رشد و توجه در این زمینه شرایط را برای ایجاد شبکه‌ی جهانی اینترنت را فراهم کرد. دیگر مفهومی به نام مسافت، دوری از هم، عدم دسترسی به منابع و غیره معنایی نداشت. بدون هیچ انحصار طلبی، هر کسی می‌توانست در رشد و گسترش این شبکه به نوبه‌ی خود سهیم باشد. اگر چه استفاده از رسانه‌ی انتقال کابلی همچون سیمی و فیبر نوری همچنان رایج ترین رسانه‌ی انتقال در دسترسی به اینترنت هستند ولی امروزه با رایج و فراگیر شدن تجهیزات ارتباطی سیار همچون کامپیوترهای دیجیتالی دستی، تلفن همراه، لپ‌تاپ و غیره کاربران مشتاق به دسترسی اینترنت بی‌سیم و سیار، بطوریکه قابل دسترس در هر مکان و زمانی می‌باشد، هستند. از میان شبکه‌های بی‌سیم سیار، شبکه‌های اقتضایی بدلیل سهولت در نصب و راه اندازی، عدم نیاز به زیرساختار از پیش تعریف شده و تجهیزاتی همچون ایستگاه پایه، هزینه‌ی برقراری ارتباط را با دلایل توجیه کننده‌ای برای برخی کاربردها پایین آورده است که مورد توجه بسیاری قرار گرفته است. عدم وجود زیر ساخت ثابت، کنترل مرکزی و همچنین وابستگی به همکاری تک تک گره‌ها برای عملکرد شبکه، محدودیت و چالش‌هایی را در زمینه‌ی طراحی و برقراری امنیت نسبت به دیگر شبکه‌ها مواجه کرده‌اند.

در این فصل ابتدا مفهوم شبکه‌های اقتضایی، خصوصیات و کاربردهای این شبکه معرفی می‌شوند. و در نهایت به نتیجه‌گیری مطالب فصل پرداخته می‌شود.

۲-۲- مروری بر شبکه‌های بی‌سیم اقتضایی

شبکه اقتضایی بی‌سیم یک شبکه بدون زیرساختار است که می‌تواند بر اساس یک سبک پویا و با گره‌های متحرک بنا شده باشد. بر خلاف یک شبکه‌ی بی‌سیم زیرساخت‌دار، شبکه‌ی اقتضایی فاقد زیر ساخت ثابت برای پشتیبانی می‌باشد و برای برقراری ارتباط با استفاده از مسیرهای چند پرشی اقدام می‌کند.

یک شبکه اقتضایی همچنین به عنوان شبکه خود- سازمان یافته نیز نام برده می‌شود زیرا به طور معمول هیچ مدیریت مرکزی در میان گره‌های سیار اقتضایی وجود ندارد، بنابراین با مشارکت همه گره‌های اقتضایی، شبکه قادر به فعالیت و برقراری ارتباط می‌باشد. هر گره باید توابع رایجی از قبیل آدرس دهی، مسیریابی، کنترل انرژی، و غیره را پیاده‌سازی کند. ویژگی مهم دیگر یک شبکه اقتضایی قابلیت یک گره سیار برای جابه‌جایی مستقلانه (آزادانه) است در حالیکه همچنان می‌تواند با گره‌های دیگر سیار در داخل همان شبکه در یک سبک اقتضایی ارتباط برقرار کند. به طور

ویژه، یک گره سیار می‌تواند در هر جهتی حرکت کند و همچنان قادر به مشارکت در برقراری هر ارتباطی باشد. در شبکه‌ی اقتضایی امکان دارد که گره‌ها سیار باشند و یا نباشند، از طرف دیگر ممکن است که ترکیبی از گره‌های سیار و گره‌های ثابت وجود داشته باشد. از آنجایی که هر وسیله‌ی تجهیز شده با امکانات ارتباطی بی‌سیم می‌تواند در شبکه‌ی اقتضایی وجود داشته باشد، یک ناهمگونی وسیعی در میان وسیله‌ها پدید می‌آید. این ناهمگونی وسیع در میان وسیله‌ها حاکی از این است که ارتباطات، ذخیره سازی، محاسبات و مصرف توان این وسیله‌ها به طور وحشتناکی با هم تفاوت دارند [2].

در ارتباط با مصرف توان، یک گره سیار معمولا با توان باتری محدودی و قابلیت محاسباتی کاهش یافته‌ای عمل می‌کند. اگر یک وسیله سیار توان محاسباتی بالایی یا برقراری ارتباطات زیادی را استفاده کند باتری به طور چشمگیری تخلیه خواهد شد. بنابراین، یک تعادل مابین قابلیت محاسباتی و مصرف توان در شبکه اقتضایی همیشه مورد توجه است. یک فرستنده و یک گیرنده در یک شبکه اقتضایی می‌توانند در هر جایی باشند. هر چند برقراری ارتباط مستقیم برای یک فرستنده با هر گیرنده ممکن نمی‌باشد(یعنی، روی یک پرش) و این به دلیل پوشش رادیویی محدود است. بنابراین، یک بسته‌ی ارسال شده ممکن است که چندین پرش را برای رسیدن به مقصد مورد نظر بپیماید. هر گره میانی باید بسته‌هایی را که دریافت می‌کند برای برقراری ارتباط ما بین یک فرستنده و گیرنده به همسایه‌ی خودش جلورانی کند [3].

عضویت شبکه به خاطر پویا بودن شبکه به طور مداوم تغییر می‌کند. شبکه‌های اقتضایی نه فقط می‌توانند شبکه‌های زیرساخت‌دار را با متصل‌کردن دیگر گره‌های خارج از بازه و یا با اتصال وسیله‌ها به سرویس‌های زیرساختاری بسط بدهند، آن‌ها همچنین می‌توانند شبکه‌هایی ایجاد کنند که هیچ زیرساختاری وجود ندارد. این قابلیت به شدت برای کاربرد نظامی بدلیل سیاریت و سرعت پیکربندی و همچنین پیکربندی مجدد مورد توجه است [4].

برای تشکیل یک محیط مشارکتی خود- سازمان یافته، هر میزبان سیار به یک گره خودی[2] فرض شده است که حاضر به رله کردن پیام‌های دیگری به سمت مقصد نهایی‌اشان است. قابلیت اطمینان سراسری در همه گره‌های شبکه یک فرض اساسی امنیتی در شبکه‌های اقتضایی می‌باشد [5]. هر چند این فرض همیشه در واقعیت تحقق نمی‌یابد. ماهیت شبکه‌های اقتضایی، آن‌ها را برای برای حملات بداندیشانه[3] اعم از استراق سمع غیرفعال و اختلال فعال بشدت آسیب پذیر ساخته است [1,5].

گره‌ها در شبکه‌های اقتضایی اطلاعات ارتباطی همسایگانشان را نگهداری می‌کنند و برای رله کردن داده از طرف یکدیگر استفاده می‌کنند. بنابراین، همکاری گره برای بقای شبکه‌های اقتضایی سیار الزامی می‌باشد از آنجایی که، آن به عنوان اساس برای بسیاری از فعالیت‌های کلیدی شبکه از قبیل دسترسی رسانه، مسیریابی و امنیت به خدمت گرفته می‌شود [6].

[2] friendly
[3] malicious

هر چند، ممکن است موقعیتی باشد که یک یا چند گره برای همکاری در شبکه امتناع کنند، از این‌رو تشخیص چنین گره‌هایی مهم است تا از آسیب‌های آتی جلوگیری شود و همچنین دیگر گره‌ها را به همکاری باید تشویق کرد.

شبکه‌های اقتضایی در گذشته در زمینه‌ی دفاعی (پدافندی) اغلب تحت عنوان شبکه‌های رادیویی بسته[۴] مطالعه شده بودند [7,8]، اخیرا جلب توجه مجددی در این زمینه به خاطر در دسترس پذیر بودن لپ‌تاپ‌ها و Palmtopهای ارزان با رابط رادیویی شده است و یک گروه کاری MANET در داخل Internet (IETF) Engineering Task Force برای توسعه یک قالب کاری برای شبکه‌های اقتضایی تشکیل شده است [7]. برخی از کاربردهای شبکه‌های اقتضایی شامل انجمنی از کاربران کامپیوترهای سیار برای یک کنفرانس، هماهنگی مابین پرسنل امداد رسانی اورژانس، شبکه‌ی شخصی[۵] با وسیله‌های بی‌سیم که در ارتباط نزدیکی با شخص هستند و تعامل ما بین چندین PANs وقتیکه افراد ملاقات می‌شوند، شبکه‌های حسگر بی‌سیم در حوزه‌ی پرخطر معین، رله کردن اطلاعات سربازان برای اطلاع از موقعیت در میدان نبرد می‌باشند [7]. در ادامه برخی دیگر از کاربردهای شبکه‌های اقتضایی بیان می‌شود. در سال‌های اخیر با مشخص شدن خصوصیات شبکه‌های اقتضایی، به امتیازات تجاری آن‌ها نیز در ابعاد صنعتی توجه شده است.

به طور کلی دو نوع شبکه اقتضایی سیار وجود دارد: بسته[۶] و باز[۷] [7,9]. در شبکه‌های اقتضایی بسته، همه گره‌های سیار با یکدیگر در راستای یک هدف مشترک همکاری می‌کنند که در این میان به شبکه هایی از قبیل نظامی، امداد رسانی و عملیات اجرای قوانین می‌توان اشاره کرد. در یک شبکه‌ی اقتضایی سیار باز، گره‌های سیار متفاوت با اهداف متفاوت منابع خودشان را برای تضمین اتصال (متصل بودن) به اشتراک می‌گذارند. حال در این میان مهم نیست که از کدام نوع شبکه اقتضایی استفاده می شود، فقط در صورت مشارکت گره‌ها در یک سبک صحیح یک شبکه‌ی اقتضایی می‌تواند بدرستی کار کند.

کاربردهای اولیه شبکه‌بندی اقتضایی را می‌توان در پروژه‌ی شبکه رادیویی بسته دارپا[۸] سال ۱۹۷۲ پیگیری کرد [10] که از تکنولوژی کلید زنی بسته از قبیل تسهیم پهنای باند و مسیریابی ذخیره و جلورانی در محیط بی‌سیم سیار بهره می‌گرفت. خصوصیات PRNet[۹] یک معماری توزیع شده شامل شبکه‌ای از رادیوهای پخش همگانی با کنترل مرکزی کمینه و یک ترکیبی از پروتکل‌های دسترسی کانال GSMA و Aloha که برای پشتیبانی از اشتراک پویای پخش همگانی کانال رادیویی استفاده شده‌اند، می‌باشد. همچنین با استفاده از تکنیک‌های مسیریابی چند پرشی ذخیره و جلورانی محدودیت پوشش رادیویی حذف شده است که به طور مؤثر کاربران متعددی را به برقراری ارتباط در یک حوزه‌ی جغرافیایی گسترده قادر می‌سازد [10].

---

[4] packet radio networks
[5] PAN
[6] Closed
[7] open
[8] DARPA
[9] Packet Radio Network (PRNet)

شبکه‌های رادیویی بقاپذیر[10] در سال ۱۹۸۳ توسط دارپا برای بررسی مسائل عمده‌ی PRNet در حوزه مدیریت انرژی، قابلیت پردازش، امنیت و مقیاس‌پذیری شبکه توسعه داده شد. اهداف اصلی در توسعه الگوریتم‌های شبکه پشتیبانی شبکه‌ای بود که بتواند به گره‌های زیادی مقیاس‌پذیر باشد و در مقابل حملات امنیتی ایستادگی کند و همچنین فرکانس‌های رادیویی با حداقل توان و هزینه را برای پشتیبانی پروتکل‌های پیچیده رادیویی بسته استفاده کند [10].

اینترنت تاکتیکی توسط ارتش آمریکا در سال ۱۹۹۷ در بزرگترین مقیاس از شبکه‌ی رادیویی بسته‌ای چند پرشی بی‌سیم سیار[11] پیاده سازی شد. دنباله‌ی مستقیم[12]، طیف گسترده[13]، دسترسی چند گانه تسهیم زمانی[14] رادیویی با نرخ داده ده‌ها کیلو بیت در هر ثانیه در این شبکه مورد بهره قرار گرفتند، همچنین از پرو تکل‌های تجاری اینترنت اصلاح یافته برای ارتباط ما بین گره‌ها استفاده کردند [10]. در دهه‌ی ۸۰ و اوایل ۹۰ رشد در زمینه‌ی زیرساخت اینترنت و میکرو کامپیوتر انقلابی در امکان‌پذیری و قابلیت کاربرد ایده‌های اولیه شبکه رادیویی بسته ایجاد کرد [10].

در حالیکه کاربردهای اولیه شبکه‌های اقتضایی بیشتر مصارف نظامی بود، کاربردهای غیر نظامی همچنین به طور قابل توجهی رشد پیدا کردند. به طور ویژه در چند سال گذشته با رشد سریع در تحقیقات ارتباطات اقتضایی سیار شبکه‌های اقتضایی سیار در میان مؤسسات تجاری و انجمن‌های استاندارد مورد توجه قرار گرفتند. تکنولوژی‌های جدیدی از قبیل [11] IEEE802.11، Bluetooth [1,12,11,13,14] و HyperLan [10] پیاده‌سازی تکنولوژی اقتضایی را در خارج از حوزه‌ی نظامی را تسهیل می‌کنند و کاربردهای جدید شبکه‌ی اقتضایی را در حوزه‌های متفاوت پدیدار می‌کنند.

دسته‌بندی‌های متفاوتی از کاربردهای شبکه اقتضایی ارائه شده است. با وجود اینکه نحوه‌ی طبقه‌بندی فرق می‌کند ولی در اصل یکی هستند [2,15,1,14]. در جدول ۲-۱ جامع‌ترین دسته‌بندی که شامل می‌شود ارائه شده است.

[10] Survivable Radio Network - SURAN
[11] Mobile Wireless Multihop Packet Radio Network
[12] Direct – Sequence
[13] Spread – Spectrum
[14] Time Division Multiple Access