معرفی شبکه‌های فرصت‌طلبانه

کوثر نقره‌ای، کیارش میزانیان
۱- دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات
گرایش شبکه‌های کامپیوتری دانشگاه یزد
۲- استادیار عضو هیئت علمی گروه کامپیوتر دانشگاه یزد

kowsar.noghrei@stu.yazd.ac.ir
نام ارائه دهنده: کوثر نقره‌ای
کد مقاله: Com-0775

خلاصه

شبکه‌های فرصت‌طلبانه یکی از موضوعاتی است که در دهه‌ی اخیر از سوی جامعه‌ی علمی بسیار مورد توجه قرار گرفته است. در این شبکه‌ها گره‌های متحرک قادر به برقراری ارتباط به صورت غیر همزمان بوده و بیش‌تر مواقع یک مسیر انتها به انتها میان مبدأ و مقصد وجود ندارد. در این مقاله ابتدا تعریف کاملی از ویژگی‌های این شبکه‌ها ارائه شده و سپس معماری و عملکرد این شبکه‌ها تشریح شده است. سپس کاربردهای آن به طور خلاصه مورد بحث قرار گرفته و در آخر مثال‌هایی از این کاربردها آمده است.

کلمات کلیدی: شبکه‌های فرصت‌طلبانه، الگوریتم حمل – ذخیره – ارسال، شبکه‌های سیار موردی.

۱. مقدمه

در سال‌های اخیر استفاده از تلفن‌های همراه، رایانه‌های جیبی[1] و دیگر دستگاه‌های سیار با رشد فزاینده‌ای روبه‌رو بوده است. برای برقراری ارتباط میان این دستگاه‌ها از دو روش استفاده می‌شود. در یک روش فناوری‌های بی‌سیم و در روش دیگر جابه‌جایی کاربران به عنوان رسانه‌ی انتقال داده به کار می‌رود. در روش اول به علت هزینه‌ی زیاد و سختی ایجاد زیرساخت‌های لازم، سرعت گسترش شبکه‌ها کاهش پیدا می‌کند. در حالی که در روش دوم، انتقال داده وابسته به فرصت‌های برخوردی[2] است که به وسیله‌ی جابه‌جایی گره‌ها به وجود می‌آید. استفاده از این روش برای برقراری ارتباط در شبکه‌های کامپیوتری، نوع جدیدی از شبکه‌ها به نام شبکه‌های فرصت‌طلبانه[3] را ایجاد می‌کند (۱).

می‌توان شبکه‌های فرصت‌طلبانه را یکی از تکامل‌های به وجود آمده در شبکه‌های سیار موردی[4] و یک زیر کلاس از شبکه‌های متحمل تأخیر یا قطعی[5] دانست. البته در شبکه‌های سیار موردی، میان دو یا چند گره ارتباط همزمان بی‌سیم برقرار بوده و مسیریابی در آن ها به صورت بلادرنگ[6] صورت می‌گیرد، در حالی که گره‌های شبکه‌های فرصت‌طلبانه، دستگاه‌های قابل حمل سیاری هستند که ارتباط میان آن‌ها از طریق فناوری بی‌سیم و معمولاً به صورت غیر همزمان می‌باشد و حتی ممکن است هرگز یک مسیر ارتباطی پایدار بین فرستنده و گیرنده‌ی پیام به وجود نیاید. در نتیجه ارتباط میان گره‌ها از نظر زمانی بسیار متغیر بوده و ارسال پیام در آن‌ها با تأخیر زیادی مواجه است. در این شبکه‌ها برای تحویل پیام از الگوریتم ذخیره - حمل – ارسال[7] استفاده می‌شود؛ یعنی

[1] Personal Digital Assistant (PDA)
[2] Contact opportunity
[3] Opportunistic Networks (OppNets)
[4] Mobile Ad hoc Networks (MANET)
[5] Delay/Disruption Tolerance Networks(DTN)
[6] Real time
[7] Store-carry-forward algorithm

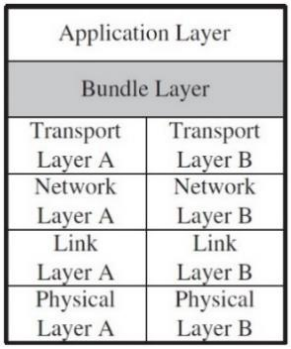
داده‌ها در بافر گره‌های متحرک ذخیره شده و همراه با آن‌ها حمل می‌شوند و هنگامی که فرصتی برای ارتباط با گره دیگری به وجود بیاید که بتواند پیام را به مقصد نهایی نزدیک‌تر کند، به آن گره ارسال شده و آن گره به عنوان گام بعدی[1] تعیین می‌گردد (۲).

پروتکل‌های TCP/IP در این محیط‌ها به آسانی نقض می‌شوند، زیرا ممکن است یک مسیر انتها به انتها بین مبدأ و مقصد فقط برای یک بازه‌ی زمانی کوتاه و غیر قابل پیش‌بینی وجود داشته باشد و چون این پروتکل‌ها برای شرایط ارسال داده و بازگشت سریع تصدیق آن طراحی شده‌اند و باید ابتدا یک مسیر کامل میان مبدأ و مقصد پیام به وجود بیاید تا ارسال داده امکان پذیر شود، نمی‌توانند در شبکه‌های فرصت‌طلبانه استفاده شوند (۱).

در بخش دوم این مقاله به معماری شبکه‌های فرصت‌طلبانه و تشریح پشته‌ی پروتکلی آن‌ها پرداخته شده است. در بخش سوم عملکرد شبکه‌های فرصت‌طلبانه و نحوه‌ی گسترش آن‌ها بیان می‌شود. در بخش چهارم به موارد کاربرد این شبکه‌ها و انواع آن‌ها از لحاظ نوع استفاده اشاره شده است. در بخش آخر نیز مثال‌هایی از این کاربردها آورده شده است.

۲. معماری شبکه‌های فرصت‌طلبانه

یک شبکه‌ی فرصت‌طلبانه معمولاً به بخش‌هایی تقسیم می‌شود که هر یک از این بخش‌ها یک ناحیه[2] نامیده می‌شود. شبکه‌های فرصت‌طلبانه، ارتباط گره‌های موجود در ناحیه‌های مختلف را از طریق تبادل پیام با استفاده از الگوریتم ذخیره - حمل - ارسال مقدور می‌سازند. گره‌های میانی[3] با گذاشتن یک لایه‌ی پروتکل جدید به نام لایه‌ی بسته[4] بر روی بقیه‌ی لایه‌ها این مکانیزم انجام می‌دهند. (شکل ۱)



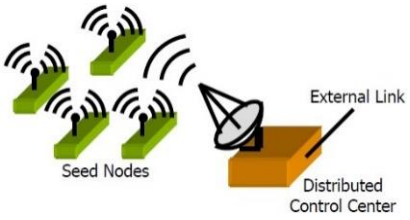
شکل ۱- پشته‌ی پروتکلی شبکه‌های فرصت‌طلبانه

در شبکه‌های فرصت‌طلبانه هر گره، یک موجودیت[5] با یک لایه‌ی بسته است که می‌تواند به عنوان یک میزبان[6] یا یک مسیریاب[7] و یا یک دروازه[8] عمل کند. وقتی گرهی به عنوان مسیریاب عمل می‌کند، لایه‌ی بسته می‌تواند کل یا تعدادی از بسته‌ها را بین گره‌های داخل یک ناحیه‌ی یکسان ذخیره، حمل و ارسال نماید. لایه‌ی بسته‌ی گرهی که به عنوان یک دروازه انجام وظیفه می‌نماید، برای انتقال پیام‌ها میان ناحیه‌های مختلف کاربرد دارد. یک دروازه می‌تواند بسته‌ها را میان دو یا حتی چندین ناحیه ارسال نماید و در صورت نیاز می‌تواند یک میزبان باشد که در این صورت بایستی حافظه‌ای ماندگار داشته باشد و از امنیت انتقالات پشتیبانی نماید تا بتواند پیام ها درون خود تا زمان مناسب حفظ نماید (۱).

[1] Next hop
[2] Region
[3] Intermediate nodes
[4] Bundle layer
[5] Entity
[6] Host
[7] Router
[8] Gateway

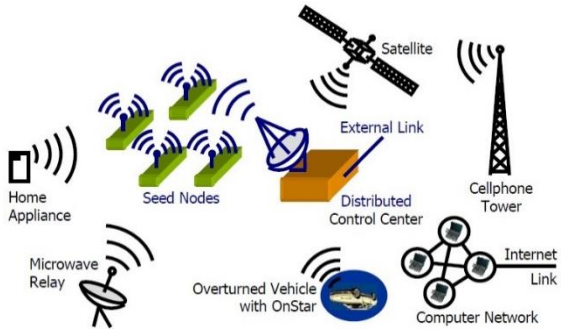
۳. عملکرد شبکه‌های فرصت‌طلبانه

هر شبکه‌ی فرصت‌طلبانه از یک بذر[1] تشکیل شده که این بذر یک مجموعه از گره‌های به کار گرفته شده در زمان گسترش ابتدایی شبکه است. به این بذر در جای خود می‌توان به عنوان یک شبکه نگاه شود، ولی می‌تواند تنها شامل یک گره نیز باشد. (شکل ۲)



شکل ۲- بذرهای شبکه‌های فرصت‌طلبانه

این بذر بایستی رشد کرده و به یک شبکه‌ی بزرگ‌تر تبدیل شود. برای این منظور بایستی دعوت نامه‌هایی به دستگاه‌های خارجی[2]، خوشه‌های گره[3]، شبکه‌ها و دیگر سیستم‌های دارای قابلیت اتصال فرستاده شود. هر گره جدید که عضو شبکه‌های فرصت‌طلبانه می‌شود، امدادگر[4] نامیده می‌شود و خود می‌تواند گره‌های خارجی را به شبکه دعوت کند. با دعوت گره‌های آزاد، شبکه‌های فرصت‌طلبانه می‌توانند از نظر اقتصادی بسیار مقرون به صرفه باشند. (شکل ۳)



شکل ۳- شبکه‌ی فرصت‌طلبانه‌ی گسترش یافته

مجموعه‌ی امدادگران شبکه‌های فرصت‌طلبانه موجودیت‌هایی هستندکه ممکن است به عنوان یک گره شبکه نیز در نظر گرفته نشوند. موجودیت‌های با سیم یا بی‌سیم، مستقل یا وابسته و حتی گره‌های فاقد هر گونه قابلیت حسی، مانند پردازنده‌های مرکزی[5] شبکه‌ای LANها یا پردازشگرهای بی‌سیم درون خودروها، نیز می‌توانند به طور مؤثری در عملیات ارتباطی و پردازشی شبکه‌های فرصت‌طلبانه شرکت کنند. برای مثال می‌توان اطلاعات مربوط به حضور و غیاب، عادت‌های کاری و نحوه‌ی دسترسی به اینترنت کاربران را به وسیله‌ی رایانه‌ی شخصی یا رایانه‌ی جیبی و مکان آن‌ها را به وسیله‌ی تلفن همراه (حتی تلفن‌های همراه بدون قابلیت GPS) جمع‌آوری نمود.

با ادامه‌ی دعوت از گره‌های دیگر توسط امدادگران، حجم شبکه افزایش می‌یابد، تا آن جا که شبکه از لحاظ اندازه، مکان گره‌ها و توانایی آن‌ها به یک میزان آستانه می‌رسد. در این زمان شبکه‌های فرصت‌طلبانه قادر به برقراری ارتباط، انجام محاسبات و حس ویژگی‌های موجودیت‌های محیط با جزئیات

[1] Seed
[2] Foreign device
[3] Node clusters
[4] Helper
[5] Mainframe

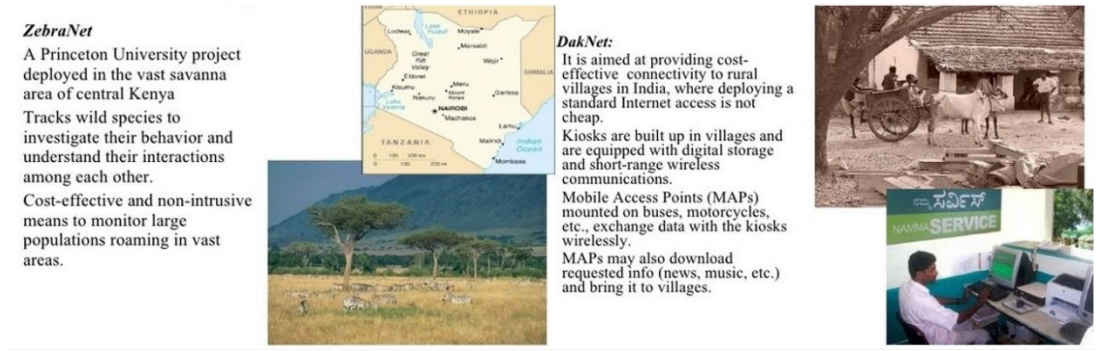
قابل توجهی هستند و هنگامی که از آن‌ها در یک مورد اضطراری مانند موقعیت ترمیم سوانح[1] استفاده شود، می‌توانند داده‌هایی را برای تخمین خسارت[2] جمع‌آوری نمایند.

وقتی تعداد کافی از امدادگران برای ایجاد امکان برقراری ارتباط، انجام محاسبات و حس محیط فراهم شد، گسترش شبکه‌های فرصت‌طلبانه متوقف می‌گردد. گاهی برای تشخیص این تعداد، برای دعوت گره‌های بیش‌تر از تحلیل سود – زیان استفاده می‌شود. شبکه‌های فرصت‌طلبانه بایستی از به کار گرفتن گره‌های زائد که کارایی آن‌ها را با مصرف غیر ضروری منابع کاهش می‌دهند، خودداری نماید. البته پیکربندی شبکه به صورت ایستا و منجمد نیست و با تغییر منطقه‌ی در حال نظارت (با حوادثی مانند زمین لرزه) و تغییر سطح نظارت مورد نیاز در مکان‌های مختلف (با توجه به میزان خسارت) شبکه دوباره خود را به صورت پویا پیکربندی کرده و حوزه‌ی عملیاتی و توانایی‌های خود را با نیازهای جدید وفق می‌دهد.

به طور کلی بایستی توجه داشت که کار کردن در هنگام سوانح نیاز به عملکرد خاص و جدیدی از سوی امدادگران ندارد و لزومی ندارد که هنگام وقوع سانحه، یک امدادگر عمل بسیار متفاوتی با کارهای روزانه‌ی خود انجام دهد. برای مثال در نظارت بر آتش سوزی، شبکه‌ی حسگر آب و هوا یک امدادگر است که در حالت عادی به جمع‌آوری داده‌های مربوط به بارش و ... می‌پردازد، ولی در زمان وقوع یک آتش سوزی می‌توان این شبکه‌ی حسگر را از عملیات عادی خود بازداشت و از منابع آزاد شده‌ی آن برای افزایش نرخ نمونه‌گیری دما و جهت باد استفاده نمود. هم‌چنین می‌توان شبکه‌های فرصت‌طلبانه‌ای را برای برقراری ارتباط، انجام محاسبات، ذخیره‌سازی اطلاعات، حس محیط و بقیه‌ی امکانات مورد نیاز در موارد اضطراری پیش‌بینی نشده ایجاد نمود و برای این کار باید از قطعات پیش‌رفته‌تری استفاده کرد. برای مثال برای افزایش قابلیت حس محیط اطراف می‌توان از دستگاه‌های دارای چندین حسگر بهره برد. البته هزینه‌ی این قطعات نیز با پیش‌رفت فناوری و تولید حسگرهای جدیدتر روز به روز ارزان‌تر می‌شود (۳).

۴. کاربردهای شبکه‌های فرصت‌طلبانه

کاربرد شبکه‌های فرصت‌طلبانه در محیط هایی است که در برابر تأخیر و خطا قابلیت تحمل بالایی داشته باشند. برای مثال در پروژه‌ی شبکه‌ی ارتباطی ساکنان لاپ لند[3] (نام منطقه‌ای در اروپای شمالی در نزدیکی مدار قطبی شمالی) برای برقراری ارتباط اینترنتی اقوام لاپ ساکن در مناطق دور افتاده یا در پروژه‌ای به نام ZebraNet برای ردگیری گورخرهای وحشی و در پروژه‌ای به نام DakNet در کشور هند در روستاهای دور افتاده که ایجاد روش‌های دسترسی استاندارد به اینترنت در آن‌ها مشکل است، برای برقراری ارتباط اینترنتی از شبکه‌های فرصت‌طلبانه استفاده شد (۱). (شکل ۴)



شکل ٤- پروژه‌ی شرکت ZebraNet برای ردگیری گورخرهای وحشی (سمت راست)
و پروژه‌ی شرکت DakNet برای ارتباط اینترنتی روستاهای هند (سمت چپ)

[1] Disaster recovery
[2] Damage assessment
[3] Sami network connectivity (SNC) project

می‌توان کاربردهای مهمی برای این شبکه‌ها در شرایط حساسی مانند ترمیم سوانح یا تأمین امنیت یک منطقه در یک موقعیت اضطراری مشاهده نمود. این شبکه‌ها توانایی بهبود کارایی عملیات امداد و نجات و ترمیم سوانح را تا حد بسیار زیادی دارا هستند. برای حوادثی مانند طوفان و آتش سوزی که امروزه مسیر آن‌ها را با دقت بسیار زیادی می‌توان پیش‌بینی کرد، امکان شروع به کار بذرهای شبکه‌های فرصت‌طلبانه و حتی تکمیل این مرحله، قبل از شروع سانحه وجود دارد. در این زمان، مکان یابی و دعوت بقیه‌ی گره‌ها و خوشه‌ها به شبکه‌های فرصت‌طلبانه بسیار ساده‌تر است. اولین امدادگران دعوت شده به وسیله‌ی بذرها می‌توانند شبکه‌های حسگر مورد نیاز برای نظارت و تخمین خسارت باشند که در ساختمان‌ها، جاده‌ها و پل‌ها قرار دارند.

مانند بسیاری از فناوری‌های دیگر شبکه‌های فرصت‌طلبانه نیز می‌توانند هم برای سودرسانی و هم برای زیان زدن به انسان‌ها استفاده شوند. گره‌های امدادگر دعوت شده به شبکه‌های فرصت‌طلبانه ممکن است از هدف اصلی شبکه‌ی میزبان خود آگاه نباشند و در نتیجه افراد خوب[1] می‌توانند توسط یک شبکه‌ی فرصت‌طلبانه‌ی بدخواه[2] فریب بخورند و فرض کنند که برای سودرسانی به کاربران مورد استفاده قرار گرفته‌اند. به طور مشابه، افراد بد[3] ممکن است توسط یک شبکه‌ی فرصت‌طلبانه‌ی خیراندیش[4] به کار گرفته شوند و فرض کنند که اهداف مضری برای کاربران را دنبال می‌کنند، در حالی که در اصل اهداف مثبتی را در پیش گرفته‌اند. در حالت منفی، شبکه‌های فرصت‌طلبانه‌ی خانگی می‌توانند بدترین متجاوزان به حریم شخصی باشند. زیرا می‌توانند رایانه‌های شخصی، گوشی‌های تلفن همراه، دوربین‌های امنیتی متصل به رایانه‌ها و پردازشگرهای وسایل برقی خانگی را به کار بگیرند.

برای خنثی نمودن تهدیدات شبکه‌های فرصت‌طلبانه‌ی بدخواه، می‌توان از شبکه‌های شکارگر[5] استفاده نمود که از همه‌ی انواع شبکه‌های بدخواه شامل شبکه‌های فرصت‌طلبانه‌ی بدخواه تغذیه[6] می‌کنند. روند کار این شبکه‌ها به این شکل است که آن‌ها ابتدا شبکه‌های بدخواه مشکوک را تشخیص می‌دهند، سپس جاسوس‌هایی[7] را در آن‌ها جاگذاری نموده و در نهایت از این جاسوس‌ها برای پی بردن به اهداف اصلی شبکه‌های مشکوک استفاده می‌کنند. البته بعضی از شبکه‌های مشکوک ممکن است در اصل از نوع خیراندیش باشند که قربانی اهداف اشتباه شده باشند. به طور معکوس، رقیبان هوشمند می‌توانند شبکه‌های شکارگر بدخواه ایجاد نمایند که از همه‌ی شبکه‌های خیراندیش شامل شبکه‌های فرصت‌طلبانه‌ی خیراندیش تغذیه می‌کنند.

۵. مثال‌هایی از کاربردهای شبکه‌های فرصت‌طلبانه

۱- مثال کاربرد شبکه‌های فرصت‌طلبانه‌ی خیراندیش: بذر شبکه‌ی فرصت‌طلبانه در ناحیه‌ای که زلزله رخ داده ایجاد می‌شود که این بذر یک شبکه‌ی بی‌سیم موردی با گره‌های قوی‌تر از یک شبکه‌ی موردی معمولی از لحاظ انرژی، منابع محاسباتی و ارتباطی است. وقتی شبکه‌ی فرصت‌طلبانه فعال می‌شود، بذر تلاش می‌کند تا هر گره مفید در عملیات تخمین خسارت و ترمیم سوانح را کشف نماید و در این راه از هر روش موجود برای شناسایی شبکه‌های دیگر، مانند تشخیص با استفاده امواج رادیویی (شامل امواج تلفن همراه) یا جستجوی گره‌های موجود در منطقه‌ی مورد نظر با استفاده از آدرس IP و حتی تشخیص مبتنی بر هوش مصنوعی با استفاده از وسایل برقی و رایانه‌های شخصی، بهره می‌برد.

شبکه‌های فرصت‌طلبانه زیرمجموعه‌ی بهینه‌ای از گره‌های تشخیص داده شده و مرتبط با شبکه را فراخوانی می‌کنند تا دستگاه‌ها، خوشه‌ها و همه‌ی شبکه‌هایی که قادر به برقراری ارتباط، انجام محاسبات و حس محیط و ... هستند را دعوت نمایند. در موقعیت‌های اضطراری هر موجودیتی با هر گونه قابلیت حسی، شامل تلفن‌های همراه با قابلیت GPS یا رایانه‌های مجهز به دوربین‌های نظارتی، می‌توانند برای شبکه‌های فرصت‌طلبانه با ارزش باشند.

فرض کنید شبکه‌ی فرصت‌طلبانه قادر باشد سه شبکه‌ی حسگر مستقل را در ناحیه‌ی سانحه با هم مرتبط سازد که این سه شبکه شامل شبکه‌ی نظارت بر آب و هوا، شبکه‌ی کنترل زیرساخت‌های آبی و شبکه‌ی مراقبت مکان‌های عمومی باشد. این شبکه‌ها نامزدهایی برای امدادگر شدن هستند و طوری تنظیم شده‌اند که در هنگام بروز سانحه بلافاصله عملیات عادی و روزانه‌ی خود را رها کرده و شروع به همکاری در وظایف ترمیم سوانح می‌نمایند. برای مثال

[1] Good guy
[2] Malevolent OppNet
[3] Bad guy
[4] Benevolent OppNet
[5] Predator network
[6] Feed
[7] Spy

شبکه‌ی حسگر نظارت بر آب و هوا را می‌توان برای حس کردن آتش و سیل، شبکه‌ی حسگر کنترل زیرساخت‌های آبی را برای حس کردن جابه‌جایی وسایل نقلیه و تشخیص سنگینی ترافیک و شبکه‌ی حسگر مراقبت مکان‌های عمومی را برای جستجوی خودکار برای یافتن تصاویر قربانیان به کار برد.

۲- مثال کاربرد شبکه‌های فرصت‌طلبانه‌ی بدخواه:فرض کنید سربازان دشمن می‌خواهند با استفاده از مردم عادی که از اهداف آن‌ها بی‌اطلاع هستند، در ظاهر یک شبکه‌ی حسگر نظارت بر آب و هوا ایجاد نمایند. ولی در اصل شبکه‌ی حسگر اصلی هنگام شروع به فعالیت تبدیل به یک بذر از یک شبکه‌ی فرصت‌طلبانه بدخواه می‌شود. شبکه‌ی حسگر شروع به جذب امدادگر می‌کند، ولی برای هیچ یک از امدادگران اهداف اصلی خود را آشکار نمی‌سازد و اعلام می‌دارد که نظارت بر آب و هوای منطقه را برای یک برنامه‌ی تحقیقاتی سودمند دنبال می‌کند. اما در حقیقت هدف این شبکه‌ی حسگر تحلیل الگوهای بادی منطقه است تا بتواند برای پخش سریع‌تر مواد شیمیایی سمی در محیط از این اطلاعات بهره ببرد. زمانی که در جذب امدادگران از نظر سطح جغرافیایی و مهارت‌های حسی به آستانه مورد نظر برسد، از داده‌های جمع‌آوری شده استفاده کرده و زمان و مکان شروع حمله‌ی شیمیایی را تعیین می‌نماید (۳).

۶. نتیجه‌گیری

در این مقاله ابتدا مفهوم شبکه‌های فرصت‌طلبانه به صورت مفصل مورد بحث قرار گرفته و سپس برای درک بهتر، به تشریح معماری مورد استفاده در این شبکه‌ها پرداخته شده است. در مبحث عملکرد شبکه‌های فرصت‌طلبانه، به نحوه‌ی تشکیل و گسترش این شبکه‌ها در محیط اشاره شده و در بخش بعد موارد کاربرد این شبکه‌ها آورده شده است و شبکه‌های فرصت‌طلبانه با توجه به اهداف استفاده از آن‌ها طبقه بندی شده‌اند. در پایان نیز به مثال‌هایی از این کاربردها در زندگی روزمره اشاره شده است.

۷. مراجع

[1]. Huang. C.M, Lan. K.C and Tsai. C.Z, A survey of opportunistic networks, 22nd International Conference on Advanced Information Networking and Applications, IEEE, 2008.

[2]. Poonguzharselvi. B and Vetriselvi. V, Survey on routing algorithms in opportunistic networks, International Conference on Computer Communication and Informatics (ICCCI), IEEE, 2013.

[3]. Lilien. L, Kamal. Z.H, Bhuse. V and Gupta. A, The concept of opportunistic networks and their research challenges in privacy and security, Mobile and Wireless Network Security and Privacy, 85-117, Springer, 2007.