بِسْمِ اللّهِ الرّحْمَنِ الرّحِيمِ

دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی کامپیوتر گرایش نرم‌افزار

مسیریابی بی‌نشان در شبکه‌های اقتضایی متحرک جغرافیایی

استادان راهنما:
دکتر بهروز ترک لادانی
دکتر احمد براآنی

پژوهشگر:
محمد ذوالفقاری

شهریورماه ۱۳۹۱

دانشگاه اصفهان
دانشکده فنی و مهندسی
گروه مهندسی کامپیوتر

پایان‌نامه کارشناسی ارشد رشته مهندسی کامپیوتر گرایش نرم‌افزار آقای محمد ذوالفقاری
تحت عنوان

مسیریابی بی‌نشان در شبکه‌های اقتضایی متحرک جغرافیایی

در تاریخ ۹۱/۷/۲۵ توسط هیأت داوران زیر بررسی و با درجه عالی به تصویب نهایی رسید.

۱- استاد راهنمای پایان‌نامه	دکتر بهروز ترک لادانی	با مرتبه ی علمی	دانشیار	امضا
۲- استاد راهنمای پایان‌نامه	دکتر احمد براآنی	با مرتبه ی علمی	دانشیار	امضا
۳- استاد داور داخل گروه	دکتر حمید ملا	با مرتبه ی علمی	استادیار	امضا
۴- استاد داور خارج از گروه	دکتر مجتبی مهدوی	با مرتبه ی علمی	استادیار	امضا

امضای مدیر گروه

چکیده

ماهیت باز شبکه‌های اقتضایی، که از انتشار آزاد سیگنال‌های داده در هوا نشأت می‌گیرد، به همراه نیاز به دریافت کمک از سایر گره‌ها جهت ایجاد ارتباط، تأمین حریم خصوصی را برای گره‌های این نوع شبکه با چالش‌های زیادی مواجه می‌سازد. در این بین پروتکل‌های مسیریابی نیز می‌توانند منجر به افشای بخشی از حریم خصوصی گره‌ها مانند هویت مبدأ و مقصد و مکان آن‌ها شود. ویژگی‌ها و محدودیت‌های موجود در گره‌های این شبکه‌ها نیز مسئله تأمین حریم خصوصی آن‌ها را دشوارتر می‌نماید. از جمله این ویژگی‌ها می‌توان به تحرک، توان پردازشی محدود، عمر محدود باتری و امکان تسخیر توسط دشمن اشاره نمود. از این رو مسیریابی بی نشان که می‌تواند حریم خصوصی گره‌ها را در برابر سایرین محفوظ نگاه دارد نقش ویژه‌ای در امنیت این شبکه‌ها خواهد داشت.

تاکنون روش‌های متنوعی در مورد ایجاد بی‌نشانی در فرآیند مسیریابی شبکه‌های اقتضایی ارائه شده است. برخی از پروتکل‌های موجود، بی‌نشانی قابل قبولی در سیستم ایجاد می‌نمایند ولی از کارایی لازم در شبکه برخوردار نیستند. در مقابل عده‌ای دیگر از پروتکل‌ها اقدام به کاهش میزان بی‌نشانی به منظور افزایش کارایی پرداخته‌اند. پیدایش مسیریابی‌های جغرافیایی که کارایی و توسعه‌پذیری لازم در شبکه‌های اقتضایی را دارا هستند موجب شد تا ایده ارائه مسیریابی‌های جغرافیایی بی‌نشان که به اندازه کافی بی‌نشان و نیز کارا باشند شکل گیرد. بنابراین در این پایان‌نامه به ارائه یک گونه بی‌نشان از مسیریابی جغرافیایی GPSR پرداخته‌ایم که بتواند بی‌نشانی قابل قبول را با کارایی مطلوب تأمین نماید.

جهت تحلیل طرح پیشنهادی، کارایی آن با پروتکل مسیریابی جغرافیایی GPSR توسط شبیه‌سازی آن‌ها در محیط NS2 مقایسه شده است. همچنین، با تخمین هزینه عملیات رمزنگارانه، کارایی آن با پروتکل‌های مسیریابی بی‌نشان ANODR- به عنوان پروتکلی مبنا در این زمینه- و نیز یکی از پروتکل‌های ارائه شده برای مسیریابی جغرافیایی بی نشان مورد مقایسه قرار گرفته است. به علاوه، به تحلیل مقاومت پروتکل طراحی شده در برابر انواع حملات مطرح در مسیریابی‌های بی‌نشان پرداخته شده است. از جمله این حمله‌ها می‌توان به شنود سراسری شبکه، حملات مبتنی بر طول، حملات مبتنی بر زمان، تسخیر گره‌ها و تبانی گره‌های تسخیر شده اشاره کرد.

نتیجه حاصل از شبیه‌سازی نشان داد که با افزودن ویژگی بی‌نشانی به مسیریابی GPSR، کارایی پروتکل پیشنهادی هم چنان با پروتکل GPSR قابل مقایسه است. هم‌چنین نشان داده شده است که هزینه عملیات رمزنگارانه انجام شده در پروتکل پیشنهادی نسبت به پروتکل ANODR بسیار کمتر است که حکایت از کارایی بیشتر آن دارد. البته مقایسه هزینه‌های رمزنگاری پروتکل پیشنهادی و پروتکل دیگر مسیریابی جغرافیایی بی‌نشان مشخص نمود که هزینه رمزنگاری در پروتکل پیشنهادی بیشتر است که در مقایسه با تأمین بی‌نشانی مقصد، این هزینه توجیه‌پذیر است. تحلیل پروتکل پیشنهادی در برابر حملات رایج در مسیریابی‌های بی‌نشان مشخص نمود که این پروتکل می‌تواند در

برابر بسیاری از حملات مطرح شده مقاومت نماید. پروتکل پیشنهادی تنها در برابر حمله جلوگیری از سرویس نمی‌تواند مقاوم باشد.

واژگان کلیدی: شبکه‌های اقتضایی متحرک، بی‌نشانی، مسیریابی بی‌نشان، مسیریابی بی‌نشان جغرافیایی

فهرست مطالب

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

فهرست شکل‌ها

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فصل اول– کلیات

۱-۱ مقدمه

فناوری بی‌سیم در سال‌های اخیر توانسته انقلابی در زمینه سیستم‌های کامپیوتری به وجود آورد. امروزه نسل جدید دستگاه‌های محاسباتی متحرک[۱] مانند رایانه‌های قابل حمل[۲]، رایانه‌های جیبی[۳] و تلفن‌های همراه که از فناوری‌های بی‌سیم استفاده می‌نمایند توانسته‌اند توجه مصرف کنندگان بسیار زیادی را معطوف به خود نمایند.

شبکه‌های اقتضائی متحرک[۴] گونه‌ای از شبکه‌های بی‌سیم هستند که به دلیل کاربردهای بالقوه در فضای تجاری، نظامی، اجتماعی و غیره بسیار مورد توجه قرار گرفته‌اند. امکان فراهم آوردن سریع ارتباط در کاربردهای حساس از قبیل حوادث غیر مترقبه و یا مأموریت‌های نظامی از دیگر عوامل توجه به این نوع شبکه‌هاست. این شبکه‌ها از دستگاه‌های متحرک خودمختار بی‌سیمی تشکیل شده‌اند که به آنها گره گفته می‌شود. گره‌ها می‌توانند در هم‌بندی‌های تصادفی و به صورت کاملا پویا سازماندهی شوند. عدم نیاز به وجود زیرساخت، جهت ایجاد ارتباطات بین گره‌ها، از خصوصیات و ویژگی‌های اصلی این نوع شبکه‌ها است که یکی از دلایل محبوبیت آنها نیز به شمار می‌رود. گره‌های موجود در این شبکه‌ها می‌توانند با سایر گره‌هایی که در محدوده امواج رادیویی آن‌ها هستند به صورت مستقیم و با سایر گره‌ها به صورت غیر مستقیم ارتباط برقرار نمایند. البته جهت برقراری

---

[1] Mobile
[2] Laptops
[3] Personal Digital Assistance (PDA)
[4] Mobile ad hoc networks

ارتباط‌های غیر مستقیم نیاز به همکاری گره‌های موجود در مسیر دارند. برخی از ویژگی‌های شبکه‌های اقتضایی متحرک عبارتند از:

- عدم وجود زیرساخت، منابع و مدیریت‌های متمرکز
- همکاری گره‌ها جهت ایجاد ارتباطات
- محدودیت منابع گره‌های سیار
- هم‌بندی پویا و قابل گسترش
- وجود تحرک در گره‌ها
- عدم وجود اطمینان در مسیرهای دسترسی به گره‌ها
- عدم امکان محافظت فیزیکی از گره‌ها

بنا بر آنچه ذکر شد می‌توان گفت مسیریابی در این شبکه‌ها نیازمندی‌های کاملا متفاوتی با شبکه‌های سیمی دارند. گره‌ها در این شبکه‌ها، علاوه بر وظایف اصلی خود، باید در مسیریابی بسته‌های سایرین، مشارکت نمایند. هم‌بندی پویا در این شبکه‌ها و نیز انجام فرآیند مسیریابی در گره‌ها با توان پردازشی محدود، پروتکل‌های مسیریابی را با محدودیت‌های زیادی مواجه می‌سازد. امروزه پروتکل‌ها و استانداردهای متنوعی جهت مسیریابی در شبکه‌های اقتضایی مطرح شده‌اند. پروتکل‌های مسیریابی DSDV [۱۸]، OLSR [۱۹]، AODV [۲۰]، DSR [۲۱]، ZRP[۲۲] ، CBRP [۲۳] و GPSR [۱] از جمله مهم‌ترین و پرکاربردترین مسیریابی‌های موجود در شبکه‌های اقتضایی هستند که هر یک سعی می‌کنند مسیر بهینه را از مبدأ به مقصد انتخاب نمایند.

از طرف دیگر ماهیت باز شبکه‌های بی‌سیم موجب می‌شود که این شبکه‌ها در برابر حملات، آسیب‌پذیری بیشتری داشته باشند به گونه‌ای که تأمین حریم خصوصی برای گره‌ها را با چالشی جدی مواجه می‌سازد [۱۲]. در این شبکه‌ها سیگنال‌ها در فضا انتشار می‌یابند که برای همگان قابل دسترس است. این در حالیست که مسیریابی‌های امروزی در شبکه‌های بی‌سیم از جمله AODV و DSR به امنیت گره‌ها توجهی ندارند. برخلاف شبکه‌های بی‌سیم، شبکه‌های سیمی توسط چندین لایه مانند زیر ساختار سخت‌افزاری، مدیریت و دیواره‌های آتش محافظت می‌شوند.

تا کنون تعدادی پروتکل به منظور تأمین امنیت در فرآیند مسیریابی ارائه شده‌اند. این پروتکل‌ها در زمره پروتکل‌های مسیریابی امن طبقه‌بندی شده و شامل دو دسته، یکی بر مبنای پروتکل پایه AODV و دیگری بر

مبنای پروتکل پایه DSR یا DSDV ارائه شده‌اند [۲۵]. مراجع [۲۶]، [۲۷]، [۲۸] و [۲۹] تعدادی از مسیریابی‌های امن در شبکه‌های اقتضایی که مبتنی بر پروتکل پایه DSR مطرح گشته‌اند را نمایش می‌دهد [۳۰]. هم‌چنین مراجع [۳۱]، [۳۲]، [۳۳] و [۳۴] نیز تعدادی از مسیریابی‌های امن در شبکه‌های اقتضایی که مبتنی بر مسیریابی پایه AODV شکل گرفته‌اند را نمایش می‌دهد. اگرچه مسیریابی‌های امن با استفاده از رمزنگاری، درهم‌سازی و مکانیزم‌های احراز اصالت پیام[5] سعی می‌نمایند تا محرمانگی، صحت و انکارناپذیری پیام را تأمین نمایند اما هم چنان در برابر حملات تحلیل ترافیک آسیب‌پذیر هستند [۲۵]. با رمزنگاری سطح کاربرد می‌توان محتوای بسته‌های مبادله شده را از دید مشاهده کنندگان بیرونی محافظت کرد، اما همچنان اطلاعاتی حیاتی از حریم خصوصی گره‌ها در معرض افشا هستند. از جمله این اطلاعات می‌توان به مکان جغرافیایی، سرعت و جهت حرکت گره‌ها و ارتباطات آن‌ها با یکدیگر اشاره نمود که به سادگی از طریق تحلیل ترافیک قابل استنتاج است [۲۴]. در این میان پروتکل‌های مسیریابی نیز می‌توانند منجر به افشای حریم خصوصی گره‌ها شوند. به عنوان مثال، به سادگی می‌توان سرآیند بسته‌ها را که در هوا منتشر شده‌اند مشاهده نمود و مبدأ و مقصد ارتباط و احتمالا موقعیت آنها را استنتاج نمود.

بنابراین پروتکل‌های مسیریابی در حفاظت از حریم خصوصی گره‌ها در این شبکه‌ها جایگاه ویژه‌ای پیدا می‌نمایند. این اطلاعات برای تمامی گره‌های میانی موجود در مسیر نیز قابل استنتاج است. از طرف دیگر به دلیل آنکه امکان محافظت فیزیکی از گره‌ها نیز در این نوع شبکه‌ها وجود ندارد دشمن می‌تواند گره‌ای را در شبکه تسخیر نموده و در داخل آن گره اقدام به شنود شبکه و استنتاج اطلاعات بنماید. امکان افشای اطلاعاتی از حریم خصوصی مبدأ و مقصد برای ناظرین بیرونی و نیز گره‌های میانی مشارکت کننده در آن ارتباط، نیاز به انجام مسیریابی، به نحوی که این اطلاعات را بتواند محرمانه نگاه دارد لازم می‌سازد. به این گونه از مسیریابی که در آن جلوگیری از افشای اطلاعات محرمانه مبدأ و مقصد ارتباط، مهم و حیاتی باشد مسیریابی بی‌نشان[6] گفته می‌شود.

به طور مثال فرض کنید که یک میدان جنگ با این نوع شبکه‌ها پیاده‌سازی شده باشد. هم‌چنین فرض نمایید که یک عملیات در حال برگزاری باشد که شامل تعدادی نیروی شناسایی جهت شناسایی منطقه، نیروی رزمی و فرماندهی باشد. شبکه اقتضایی باید ارتباطات میان مرکز فرماندهی عملیات با نیروها و نیز ارتباطات میان نیروهای رزمی را فراهم آورد. بی‌نشانی ارتباطات جهت اجرای عملیات بسیار مهم می‌باشد. در غیر این صورت

[5] HMAC
[6] Anonymous routing

می‌تواند به افشای عملیات منجر شود. دشمن نیز می‌تواند نیروی شناسایی خود را داشته باشد و آنها را در شبکه اقتضایی منتشر کند. برای مثال ادوات سخت‌افزاری سیار با آنتن‌های خاص استفاده نماید که با دریافت یک موج رادیویی بتواند موقعیت گره منتشر کننده را نشان دهد. بنابراین دشمن نیز با فراهم آوردن شبکه خود می‌تواند موقعیت، حرکت و تعداد گره‌های موجود در شبکه اقتضایی را شناسایی کند. چنانچه دشمن مشاهده نماید که بیشتر گره‌ها در حال حرکت به سمت موقعیت خاصی از آنها هستند می‌تواند وجود عملیات و نیز موقعیت احتمالی حمله را نتیجه‌گیری نمایند. این مثال در شرایطی ارائه شد که فرض شده است دشمن به محتوای هیچ یک از پیام‌ها نتواند دسترسی داشته باشد و تنها از شنود شبکه اقتضایی توانسته اطلاعات بسیار مهمی را نتیجه‌گیری نماید. بنابراین محافظت از حریم خصوصی گره‌ها در این شبکه‌ها می‌تواند بسیار مهم و حیاتی باشد.

در این پایان نامه به ارائه پروتکلی برای انجام مسیریابی بی‌نشان در شبکه‌های اقتضائی متحرک می‌پردازیم. این پروتکل با محرمانه نگه‌داشتن هویت مبدأ، مقصد و گره‌های میانی در حین مسیریابی، به حفظ حریم خصوصی آن‌ها کمک می‌کند. پروتکل پیشنهادی، بر مبنای پروتکل مسیریابی جغرافیایی GPSR [۱] ارائه شده است. در حقیقت در این پایان نامه به بی‌نشان نمودن پروتکل مسیریابی جغرافیایی GPSR پرداخته شده است. بهره‌گیری از مسیریابی جغرافیایی GPSR منجر به کاهش هزینه عملیات رمزنگارانه[۷] در فرآیند مسیریابی بی‌نشان شده است. البته در مسیریابی جغرافیایی GPSR فرض می‌شود که مبدأ، از موقعیت دقیق جغرافیایی مقصد مطلع است. در طرح پیشنهادی تنها فرض بر اطلاع مبدأ از محدوده جغرافیایی بی‌نشان مقصد، و بالعکس می‌باشد. بدین ترتیب، مبدأ و مقصد با اطلاع از موقعیت جغرافیایی بی‌نشان یکدیگر به تبادل اطلاعات محرمانه می‌پردازند. این اطلاعات در هر مسیر تا موقعیت بی‌نشان مقصد به صورت مستقیم و با کمک مسیریابی جغرافیایی ارسال شده و در آن محدوده همه پخشی خواهد شد. بدین ترتیب بی‌نشانی مبدأ در مقابل همه گره‌ها، حتی مقصد ارتباط و بی‌نشانی مقصد در برابر ناظرین شبکه حفظ خواهد شد.

۱-۲ انگیزه

امروزه با گسترش علم رمزنگاری محافظت از محتوای پیام‌های خصوصی تقریبا به صورت کامل تأمین می‌شود. اما چنانچه ذکر شد تنها محتوای پیام‌ها شامل اطلاعات مهم و حیاتی نیستند. سایر اطلاعاتی که با شنود

[7] Cryptographic operations

ارتباطات و از نحوه ارسال پیام‌ها می‌توان نتیجه‌گیری کرد اطلاعات مهمی هستند که با وجود گسترش زیادی که در علم رمزنگاری حاصل شده است هم چنان قابل افشا هستند. این مشکل به خصوص در مورد شبکه‌های اقتضایی و در کاربردهای نظامی چالشی جدی به حساب می‌آید. از این رو فرآیند مسیریابی به نحوی که بتواند اطلاعات حریم خصوصی گره‌ها را محرمانه نگاه دارد بسیار مورد توجه قرار گرفته است.

روش‌های اولیه تأمین بی‌نشانی در شبکه‌های اقتضایی، با تطبیق مفاهیم بی‌نشانی که در مورد شبکه‌های سیمی مطرح بودند آغاز شدند. امروزه روش‌های متنوعی برای بی‌نشانی ارائه شده است. پروتکل SDAR [۶] یکی از پروتکل‌های اولیه در مسیریابی بی‌نشان شبکه‌های اقتضایی است که البته فارغ از مشکل نیز نیست. محاسبات بسیار سنگین پردازشی در آن، عملا آن را ناکارآمد ساخته است. از این رو پروتکل دیگری با نام ANODR [۹] ارائه شد که توانست میزان محاسبات پردازشی را کم‌تر نماید. اگرچه پروتکل ANODR توانست محاسبات پردازشی کمتری نسبت SDAR استفاده نماید اما هم چنان محاسبات پردازشی زیادی داشت که آن را عملا ناکارآمد ساخت.

ورود مسیریابی‌های جغرافیایی که کارایی و توسعه‌پذیری بالایی برای شبکه‌های اقتضایی به همراه داشتند ایده ارائه مسیریابی جغرافیایی بی‌نشان را از ذهن گذراند. پروتکل‌هایی که بتوانند کارایی و توسعه‌پذیری خود را از مسیریابی جغرافیایی استفاده نمایند و بی‌نشانی خود را از ANODR تأمین نمایند. یکی از اولین پروتکل‌های مسیریابی جغرافیایی بی‌نشان توسط Zhou و همکاران وی ارائه شد [۱۰]. از آنجا که ماهیت مسیریابی جغرافیایی با مفاهیم بی‌نشانی تناقضی آشکار دارد این پروتکل نیز نتوانست به خوبی بی‌نشانی حاصل را تأمین نماید.

از این رو رفع تناقض‌های ذاتی بی‌نشانی و مسیریابی جغرافیایی انگیزه‌ای شد تا بتوان پروتکلی ارائه نمود که به اندازه کافی، کارا و بی‌نشان باشد. این مهمی است که در این پایان نامه برآنیم تا آنرا ارائه نماییم.

۱-۳ مروری بر ساختار پایان نامه

مطالب ارائه شده در این پایان نامه با شروع از مفاهیم بی‌نشانی و ارائه ادبیات موضوع که در فصل دوم به طور مفصلی به آن پرداخته شده است شروع می‌شود. سپس در فصل سوم با انگیزه ارائه پروتکل مسیریابی

جغرافیایی بی‌نشان که به اندازه کافی کارا باشد پروتکل پیشنهادی ارائه شده است. در همین فصل به بررسی حملات و مقاومت پروتکل پیشنهادی در برابر آنها نیز پرداخته می‌شود.

تحلیل میزان کارایی و امنیت پروتکل پیشنهادی در فصل چهارم مورد بررسی قرار گرفته است. در این فصل توسط مقایسه پروتکل ارائه شده با سه روش دیگر، امنیت و کارایی آن ارزیابی می‌شود.

در نهایت در فصل پنجم نیز جمع‌بندی و نتیجه‌گیری این پایان نامه ارائه می‌شود.

فصل دوم- مفاهیم و ادبیات موضوع

۲-۱ مقدمه

مفهوم بی‌نشانی ابتدا در قالب شبکه‌های سیمی مطرح شد. امروزه این مفهوم توانسته جایگاه بسیار پرارزشی در ارتباطات شبکه‌های سیمی پیدا نماید. شبکه‌های عمومی از قبیل اینترنت، که از هر دو نوع ارتباطات سیمی و بی‌سیم در زیر ساختار خود استفاده می‌نمایند، با پشتیبانی از مفهوم بی‌نشانی به دنبال کسب مقبولیت و محبوبیت بیشتر نزد استفاده کنندگان هستند. هم‌چنین کاربردهای بسیار زیادی که قبلا تمایلی به استفاده از آنها وجود نداشت امروزه به صورت گسترده‌ای در معرض توجه هستند. برای مثال انتخابات الکترونیکی مقوله‌ای است که پیش از ارائه بی‌نشانی موضوعیتی نداشت. اما امروزه اکثر کشورها تمایل به اجرای انتخابات الکترونیکی که بی‌نشانی رأی شخص در آن تأمین شده باشد دارند.

در شبکه‌های اقتضایی نیز که به دلایلی از جمله ماهیت باز شبکه‌های بی‌سیم، نیاز به مشارکت در فرآیند مسیریابی و عدم وجود زیر ساختار آسیب‌پذیری بیشتری دارند تأمین بی‌نشانی بسیار مورد نیاز قرار گرفته است. فرآیند مسیریابی در شبکه‌های اقتضایی به دلیل نیاز به مشارکت و همکاری سایر گره‌ها چالشی عمده در بی‌نشانی گره‌ها ایجاد می‌نماید. به عنوان مثال چنانچه گره‌ای بخواهد ارتباط خود با مقصدی خاص را از نگاه سایر گره‌ها و نیز مقصد خود مخفی نگاه دارد در مسیریابی‌های معمول شبکه‌های اقتضایی میسر نخواهد شد. ضرورت تأمین

بی‌نشانی در فرآیند مسیریابی شبکه‌های اقتضایی، که در کاربردهای حساس نظامی بسیار مورد توجه است، موجب شده است تا پروتکل‌های زیادی در این موضوع ارائه شوند.

در ادامه ابتدا به تعریف مفهوم علمی بی‌نشانی پرداخته می‌شود. سپس خصیصه‌های مطلوب و مورد نیاز در پروتکل‌های بی‌نشانی ارائه می‌گردند. از این خصیصه‌ها جهت ارزیابی امنیت پروتکل‌ها نیز می‌توان استفاده نمود. در ادامه به بررسی سیر تاریخی پروتکل‌های بی‌نشان پرداخته می‌شود. جزئیات پروتکل‌های عنوان شده در هنگام بررسی سیر تاریخی در بخش‌های جداگانه این فصل در ادامه بیان شده‌اند. فصل جاری با مقایسه پروتکلی‌های بی‌نشانی ادامه می‌یابد و در نهایت با جمع‌بندی و نتیجه‌گیری پایان می‌پذیرد.

۲-۲ تعریف بی‌نشانی

از بی‌نشانی به صورت کلی به پنهان نمودن یک موجودیت در میان سایر موجودیت‌های هم‌سان تعبیر می‌کنند به‌گونه‌ای که تمامی آنها دارای صفت یکسانی باشند [۱۱]. به مجموعه موجودیت‌های هم‌سان، مجموعه بی‌نشانی مرتبط با صفت مشترک اطلاق می‌شود. به این ترتیب چنانچه تنها بدانیم صفت مشترک اتفاق افتاده است به صورت قطعی نمی‌توان گفت صفت مذکور توسط کدامیک از اعضای مجموعه بی‌نشانی اتفاق افتاده است. هر چه تعداد اعضای مجموعه بی‌نشانی بزرگتر باشد میزان بی‌نشانی حاصل بیشتر می‌شود. تعداد اعضای مجموعه بی‌نشانی، درجه بی‌نشانی موجودیت را نشان می‌دهد. به عنوان مثال از بی‌نشانی مقصد در یک شبکه اقتضایی به مخفی نمودن مقصد در میان مجموعه‌ای از گره‌ها در شبکه اطلاق می‌شود [۱۱].

بی‌نشانی در موارد متعدد می‌تواند موضوعیت پیدا کند. بی‌نشانی اطلاعات، بی‌نشانی مقصد، بی‌نشانی مسیر و یا بی‌نشانی مکان نمونه‌ای از آنهاست که در مورد شبکه‌های اقتضایی مطرح است. به عنوان مثال بی‌نشانی مقصد در این شبکه‌ها به معنی پنهان نمودن هویت گره مقصد در بین تعدادی گره در شبکه است به نحوی که نتوان ادعا کرد دقیقا کدامیک از آنها مقصد واقعی ارتباط بوده است.

چنانچه بتوان تضمین نمود که تعداد اعضای مجموعه بی‌نشانی یک موجودیت از حداقل k کمتر نشود از آن تعبیر به بی‌نشانی مرتبه $k^{۸}$ می‌شود [۴۵].

[8] K-Anonymity

۲-۳ خصیصه‌های بی‌نشانی

مرجع [۲۵] خصیصه‌های بی‌نشانی را به صورت زیر تعریف می‌نماید:

- **محرمانگی شناسه:** هیچ کس به غیر از مبدأ و مقصد نباید از شناسه یکتای آنها آگاه شود. هم‌چنین مبدأ و مقصد نباید هیچ گونه اطلاعی از گره‌های میانی موجود در مسیر داشته باشند.
- **محرمانگی مکان:** هیچ کس نباید از موقعیت مکانی مبدأ و مقصد اطلاع یابد. هم‌چنین گره‌ها نباید بتوانند از فاصله و یا تعداد گام خود از مبدأ و یا مقصد آگاهی یابند.
- **محرمانگی مسیر:** اول اینکه دشمن در داخل مسیر و یا خارج از آن نباید بتواند بسته را تا مبدأ و یا مقصد ره‌گیری نماید. دوم اینکه دشمن نتواند به الگوی حرکتی مبدأ و یا مقصد ارتباط دسترسی داشته باشد.

از آنجا که هر خصیصه بی‌نشانی عنوان شده در مرجع [۲۵] دارای بخش‌های مختلف است لذا مقایسه راهکارهای تأمین بی‌نشانی را مشکل می‌نماید. زیرا یک پروتکل ممکن است با بخشی از تعریف فوق هماهنگی داشته باشد اما با بخش دیگری از تعریف هماهنگی نداشته باشد. از این رو در ادامه خصیصه‌های عنوان شده در مرجع فوق با تفکیک بیشتری ارائه شده‌اند که از آنها به عنوان مبنای مقایسه راهکارهای تأمین بی‌نشانی استفاده خواهد شد.

- **محرمانگی شناسه مبدأ،** شناسه یکتای مبدأ ارتباط باید از نگاه گره مقصد و نیز از نگاه تمام گره‌های موجود در شبکه پنهان بماند.
- **محرمانگی شناسه مقصد،** شناسه یکتای مقصد ارتباط باید از نگاه تمام گره‌های موجود در شبکه پنهان بماند. شناسه یکتای مقصد نمی‌تواند از نگاه مبدأ پنهان نگه داشته شود. زیرا مبدأ ارتباط باید از هویت دقیق شخص مورد نظر خود اطلاع داشته باشد.
- **محرمانگی شناسه یکتای گره‌های میانی،** مبدأ و مقصد از شناسه یکتای گره‌های میانی مشارکت کننده در فرآیند مسیریابی، نباید اطلاعی داشته باشند. هم‌چنین شناسه یکتای گره‌های میانی از دید ناظرین بیرونی و درونی نیز باید محافظت شود.