بررسی چالش‌ها و راهکارهای امنیتی در شبکه‌های بی‌سیم

فاطمه سیاحی[1]، فرزانه دستجردی[2]

[1] موسسه آموزش عالی امام جواد یزد، s.rezaee.1990@gmail.com
[2] دانشگاه یزد، dastjerdi_it@yahoo.com

چکیده

یک شبکه بی سیم، از سیگنال‌های رادیویی برای تبادل داده‌ها بین دو یا چند دستگاه فیزیکی استفاده می‌کند که معمولا "گره‌های" شبکه نامیده می‌شوند. هنگامی که گره‌ها به هیچ یک از زیر ساخت-های از پیش موجود وابسته نیستند، شبکه‌های بی‌سیم، شبکه‌های ادهاک بی‌سیم نام می‌گیرند. در این مورد، ارتباطات، به توانایی گره‌ها برای تشکیل یک شبکه رادیویی چند منظوره وابسته است.

امنیت یک نگرانی عمده برای ارتباطات بین گره‌های سیار ومتحرک در یک محیط خصمانه است. در حضور گره‌های مخرب، یکی از چالش های مهم، طراحی راه‌حل‌های امنیتی قوی است که می‌تواند شبکه را از حملات مختلف مسیریابی محافظت کند. شبکه-های ادهاک بیسیم می‌تواند در انزوا و یا در هماهنگی با زیرساخت-های سیمی کار کند.

در این مقاله قصد داریم بر چالش‌های امنیتی وحملات امنیتی اساسی که در پنج مجموعه مختلف از شبکه‌های بیسیم ادهاک ایجاد می‌شوند تمرکز کنیم: شبکه‌های ادهاک متحرک یا MANET، شبکه‌های حسگر بیسیم یا WSN، شبکه‌های حسگر بیسیم بدون نظارت یا UWSN، شبکه‌های بیسیم توری یا WMN و شبکه‌های تحمل‌کننده تاخیر یا DTN. از آنجاییکه این شبکه‌ها ویژگی‌های زیادی را به اشتراک می‌گذارند، به منظور وضوح و کامل بودن، ابتدا چالش‌های امنیتی اصلی مشترک همه شبکه‌های ادهاک بی‌سیم را معرفی می‌کنیم. سپس، برای هر یک از این فن‌آوری‌های شبکه، مسائل امنیتی خاص را معرفی و جزئیات راه‌حل‌های پیشنهادی که تاکنون در ادبیات ارائه شده است را مشخص خواهیم کرد و در پایان ویژگی‌های متمایز این پنج شبکه را بیان می‌کنیم.

واژه های کلیدی

شبکه‌های ادهاک، شبکه‌های ادهاک متحرک، شبکه‌های توری بیسیم، شبکه‌های تحمل کننده تاخیر، شبکه‌های حسگر بیسیم.

۱- مقدمه

یک شبکه ادهاک[1] متشکل از تعداد زیادی گره‌های حسگر است که در یک محیط به طور گسترده پخش شده و به جمع‌آوری اطلاعات از محیط می‌پردازند. لزوماً مکان قرار گرفتن گره‌های حسگر، از قبل‌تعیین‌شده و مشخص نیست. چنین خصوصیتی این امکان را فراهم می‌آورد که بتوانیم آنها را در مکان‌های خطرناک و یا غیرقابل دسترس رها کنیم.

امنیت یک نگرانی عمده برای ارتباطات بین گره‌های سیار ومتحرک در یک محیط خصمانه است. در حضور گره‌های مخرب، یکی از چالش‌های مهم، طراحی راه‌حل‌های امنیتی قوی است که می‌تواند شبکه را از حملات مختلف مسیریابی محافظت کند. شبکه-های ادهاک بیسیم می‌تواند در انزوا و یا در هماهنگی با زیرساخت-های سیمی کار کند.[1]. بنابراین امنیت در تمامی مسائل شبکه‌های ادهاک بیسیم مورد توجه قرار گیرند.

حملات علیه شبکه‌های بی‌سیم می‌توانند بر اساس وضعیت مهاجم، رفتار وی و هدف حمله طبقه‌بندی شوند.

وضعیت: آیا مهاجم بیگانه است یا خودی(مهاجم بجای دیگری است یا نه). مهاجمان خارج نهادهایی هستند که به شبکه تعلق ندارند بلکه می‌خواهند خدمات ارائه شده را مختل کنند. مهاجمان خودی، گره‌های مجازی هستند که به شیوه‌ای مخرب رفتار می‌کنند.

رفتار: تمایز بین حملات منفعل و فعال است. اولی سوءاستفاده از ارتباطات و نظارت و تجزیه و تحلیل رفتار شبکه، بدون دخالت در آن است. دومی دسترسی فیزیکی به یک بخش از شبکه و تلاش برای اصلاح رفتار عادی شبکه است.

هدف: حمله برای دسترسی به شبکه و یکپارچگی خدمات، هدف در اختلال خدمات ارائه شده توسط شبکه است. بسیاری از عدم سرویس دهی‌ها، مسیریابی و حملات فیزیکی در این دسته قرار دارند. حملات علیه حریم خصوصی و محرمانه بودن حملاتی هستند که سعی دارند بینشی راجع به اطلاعات ظاهرا محرمانه بدست آورند. به طور خاص، اهداف چنین حملات، اطلاعاتی هستند که در شبکه مورد استفاده قرار می‌گیرند اطلاعات در مورد توپولوژی شبکه و عملکرد و اطلاعات متنی(مانند موقعیت و زمان رویداد). لذا ما در این مقاله شبکه‌های ادهاک متحرک، شبکه حسگر بیسیم، شبکه حسگر بیسیم بدون نظارت، شبکه بیسیم توری و شبکه تحمل‌کننده تاخیر را بررسی و درباره مسائل امنیتی آنها بحث خواهیم کرد و در پایان بصورت جدول مقایسه‌ای بین این چهار شبکه خواهیم داشت[1] و[2].

[1] -Ad-hoc