ارائه یک الگوریتم کارا جهت کشف حمله wormhole در شبکه‌های حسگر بی‌سیم

فرزاد تشتریان، دانشگاه آزاد اسلامی، واحد مشهد، گروه فناوری اطلاعات، مشهد، ایران – f.tashtarian@mshdiau.ac.ir
حسن شاکری، دانشگاه آزاد اسلامی، واحد مشهد، گروه فناوری اطلاعات، مشهد، ایران - shakeri@mshdiau.ac.ir
محمد حسین یغمائی مقدم، دانشگاه فردوسی مشهد - گروه کامپیوتر - yaghmae@um.ac.ir
عباس قائمی بافقی، دانشگاه فردوسی مشهد - گروه کامپیوتر - yaghmae@um.ac.ir

چکیده: حمله wormhole یکی از خطرناک‌ترین حمله‌ها در شبکه‌های حسگر بی‌سیم است. در این نوع حمله یک گره مهاجم بسته‌ها را از یک نقطه از شبکه دریافت می‌کند و با استفاده از یک لینک پرسرعت (تونل) ، آنها را به گره همدست خود در یک نقطه دورتر در شبکه ارسال می‌کند. گره‌های مهاجم سپس از طریق این تونل به شکل‌های مختلف در شبکه اختلال ایجاد می‌کنند. در این مقاله یک راه‌حل جدید و کارامد برای کشف wormhole ارائه می‌شود که براساس اسکن‌کردن قطاعی و لایه‌ای شبکه توسط ایستگاه اصلی عمل می‌کند، راه‌حل پیشنهادی نیازی به به سخت‌افزارهای خاص اضافی یا مکانیزم همگام‌سازی ندارد و درعین حال نتایج شبیه‌سازی نشان می‌دهد که با احتمال بسیار بالا wormhole را تشخیص می‌دهد و محل دقیق wormhole را نیز تعیین می‌کند.

کلمات کلیدی: حمله wormhole، شبکه‌های حسگر بی‌سیم، امنیت، مسیریابی

۱- مقدمه

استفاده از شبکه‌های حسگر بی‌سیم به‌ویژه در محیط‌هایی ازقبیل حفاظت از محیط زیست، کاربردهای نظامی و ...که ایجاد زیرساخت‌های متداول شبکه غیرممکن، پرخطر یا پرهزینه است، مورد توجه قرار گرفته است. اما ماهیت کانال‌های ارتباطی بی‌سیم، فقدان زیرساخت و محیط ناامن این شبکه‌ها آنها را دربرابر حملات مختلف امنیتی آسیب‌پذیر می‌کند. یکی از خطرناک‌ترین حملات علیه این شبکه‌ها حمله wormhole[۱]، [۲]، [۳] است. در این نوع حمله یک گره مهاجم بسته‌ها را از یک نقطه از شبکه دریافت می‌کند و با استفاده از یک «تونل»، آنها را به گره همدست خود در یک نقطه دور در شبکه ارسال می‌کند. حالت‌های مختلف تونل‌زنی ازقبیل استفاده از یک کانال مخفی سیمی، کپسوله‌سازی بسته‌ها و یا ارسال با توان بالا در[۴] توضیح داده شده است. بسته‌ها ازطریق تونل سریع‌تر و با تعداد گام کمتر نسبت به مسیرهای عادی چندگامی به مقصد می‌رسند بنابراین تونل ذاتا می‌تواند حتی مفید باشد اما گره‌های مهاجم از آن سوءاستفاده می‌کنند به این ترتیب که به گره های دور از هم وانمود می‌کنند که همسایه نزدیک به یکدیگر هستند و بنابراین ترافیک بسته‌ها به سمت تونل جذب می‌شود. سپس گره های مهاجم براساس این فریبکاری می‌توانند حملات مختلفی را صورت دهند که مهم‌ترین آنها اختلال در پروتکل مسیریابی است. بسیاری از پروتکل‌های مسیریابی براساس شمارش گام‌ها عمل می‌کنند درحالی‌که wormhole تعداد گام‌های بین دو گره دور را به صورت غیرواقعی کم نشان می‌دهد. در [۱] نحوه تاثیر wormhole در اختلال در چندین پروتکل مسیریابی ازجمله DSR[۵]، AODV [۶]، DSDV [۷] و OLSR [۸] توصیف شده است. گره های مهاجم می‌توانند با دورریختن گزینشی بسته‌ها، حمله DoS را صورت دهند یا ترافیک شبکه را مورد تحلیل آماری قرار دهند. علاوه بر این برخی از پروتکل‌های خوشه‌بندی، جمع‌آوری داده‌ها و ... که بر اساس موقعیت گره ها و وضعیت همسایگی آنها عمل می‌کنند، در اثر حمله wormhole دچار اختلال می‌شوند.

متاسفانه انجام حمله wormhole نسبتا آسان و مقابله با آن دشوار است. مهاجم برای حمله wormhole نیازی به داشتن دانش درمورد جزئیات لایه MAC یا پروتکل‌های لایه‌های دیگر ندارد و حتی ممکن است در سطح بیت کار کند که توسط لایه‌های بالاتر قابل کشف نیست و به دلیل سریع بودن، تحلیل زمانی هم برای مقابله با آن کارآمد نیست. همچنین چون در

حملات wormhole بسته‌ها به همان شکلی که دریافت می‌شوند، ارسال می‌گردند، با مکانیزم‌های رمزنگاری نمی‌توان با حمله مقابله کرد. ازطرف دیگر wormhole نیاز به همکاری هیچ گره میزبانی ندارد.

راه‌حل‌های مختلفی برای کشف wormhole ارائه شده است. برخی از ویژگی‌های یک راه حل خوب عبارتند از نرخ بالای تشخیص wormhole و نرخ پایین اعلام اشتباهی wormhole، مصرف کم انرژی با توجه به محدودیت منابع در شبکه‌های حسگر بی‌سیم، عدم نیاز به سخت‌افزارهای خاص از قبیل ساعت دقیق یا GPS، عدم نیاز به همگام‌سازی زمانی بین گره های شبکه، سازگاری با پروتکل‌های لایه‌های مختلف.

در این مقاله یک راه حل جدید برای مقابله با حملات wormhole ارائه می‌کنیم. مکانیزم پیشنهادی که براساس اسکن‌کردن قطاعی و لایه‌ای شبکه توسط ایستگاه اصلی عمل می‌کند، نه تنها با احتمال بسیار بالا wormhole را تشخیص می‌دهد، بلکه با استفاده از این ایده ابتکاری محل دقیق wormhole را تعیین می‌کند. راه‌حل پیشنهادی بدون نیاز به سخت‌افزار اضافی خاص یا همگام‌سازی، با احتمال بالا wormhole را کشف و موقعیت آن را تعیین می‌کند. ساختار ادامه این مقاله به صورت زیر است: در بخش ۲ کارهای تحقیقاتی انجام‌شده در این زمینه را مرور خواهیم کرد. در بخش ۳ تعریف مساله و فرضیات درنظرگرفته‌شده را ارائه می‌کنیم. در بخش ۴ راه حل پیشنهادی را معرفی و تشریح می‌کنیم. بخش ۵ به ارائه نتایج شبیه‌سازی و بالاخره بخش ۶ به نتیجه‌گیری اختصاص دارد.

۲- کارهای مرتبط

حمله wormhole ابتدا به صورت مستقل در[۱]، [۲] و [۳] معرفی شد. از آن پس راه‌حل‌های مختلفی برای مقابله با wormhole ارائه شده است که اغلب براساس محدودکردن زمانی یا مکانی انتقال بسته و یا براساس شناسایی همسایه‌ها با استفاده از نظریه گراف و مختصات هندسی عمل می‌کنند. برخی از راه‌حل‌ها از سخت‌افزارهای اضافی خاص مانند آنتن‌های جهت‌دار [۹] یا گره های نگهبان [۱۰]، [۱۱] استفاده می‌کنند و برخی دیگر مانند [۱]، [۱۲] براساس تحلیل زمانی یا همگام-سازی دقیق عمل می‌کنند.

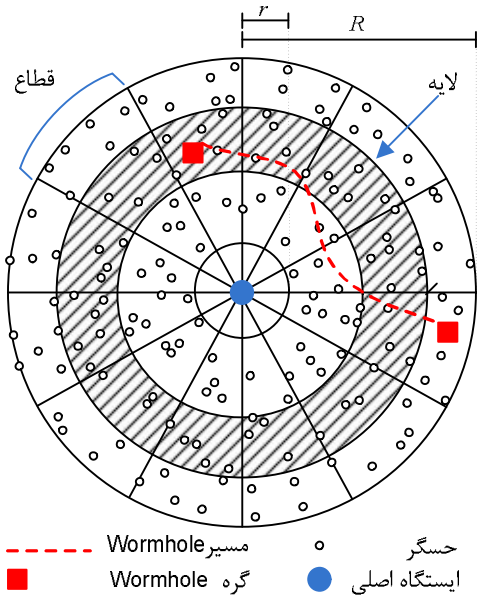
در [۱۰] با استفاده از مفهوم گراف‌های هندسی تصادفی برای مدل‌سازی wormhole، شرط لازم و کافی برای تشخیص ورم هول توسط هر راه حلی ارائه شده است. همچنین یک مکانیزم رمزنگاری با استفاده از کلیدهای محلی موسوم به LBK برای مقابله با wormhole معرفی شده است. در این راه حل تعدادی از گره ها موسوم به نگهبان با برد ارتباطاتی بیشتر و قابلیت تشخیص موقعیت خود به کشف wormhole کمک می‌کنند.

در [۱۳] افزایش تعداد همسایه‌های حسگرها و کاهش طول کوتاه‌ترین مسیرها بین هر دو زوج حسگر به عنوان شواهدی بر وجود wormhole مورد بررسی قرار می‌گیرد. در [۱۴] کارایی مسیریابی چندگامی تحت حمله ورم هول مورد بررسی قرار گرفته و طرحی به نام تحلیل آماری چندگذره (SAM) باز هم براساس ردیابی تغییرات غیرعادی در برخی آماره‌ها ارائه شده است. پروتکل LiteWorp [۴] برمبنای نظارت هر گره بر ترافیک ورودی و خروجی همسایه‌هایش عمل می‌کند. در [۱۵] یک مکانیزم به نام مهار بسته برای ردیابی و مقابله با حملات ورم هول و نیز یک پروتکل خاص به نام TIK برای پیاده‌سازی مهارها معرفی شده است. مهار عبارت است از اطلاعاتی که به بسته ضمیمه می‌شود تا بسته نتواند بیش از فاصله معینی از ارسال-کننده آن دور شود. در [۱۶] یک مکانیزم انتها به انتها و در [۱۷] یک روش مبتنی بر زیرساخت‌های ممنوع در گراف همبندی ارائه شده است. TrueLink [۱۸] یک راه حل مقابله با ورم هول است که با استفاده از ترکیب راهکار زمانی و تایید اعتبار، وجود لینک واقعی را بین دو گره که همسایه وانمود می‌شوند، بررسی می‌کند. در [۱۹] یک پروتکل به نام MobiWorp برای مقابله با حمله ورم هول در شبکه‌های سیار ارائه شده است که از نظارت محلی بر ارتباطات همسایه‌ها توسط هر گره و یک نهاد امنیتی مرکزی برای ردیابی موقعیت گره های سیار و کشف رفتارهای سوء گره های مهاجم استفاده می‌کند. در [۲۲] با استفاده از آنتن‌های جهت‌دار که در تمامی حسگرها تعبیه شده است، با یک الگوریتم ساده جهت تشخیص لینک‌های سالم، wormhole تشخیص داده می‌شود.

۳- بیان مسأله و فرضیات

۳-۱ مدل شبکه

ما فرض می‌کنیم گستره شبکه حسگر بی‌سیم یک ناحیه دایره‌ای شکل به شعاع R است و یک ایستگاه اصلی با شعاع r از شبکه، در مرکز دایره اصلی واقع است. چیدمان گره ها می‌تواند به صورت تصادفی یا معین باشد. ایستگاه اصلی دارای آنتن جهت‌دار است ولی گره ها از آنتن‌های معمولی (غیرجهت‌دار) استفاده می‌کنند. دایره اصلی را به چند قطاع و چند لایه تقسیم می‌کنیم (شکل ۱). تعداد قطاع‌ها و لایه‌ها جزء مشخصه های مسأله است. تعداد قطاع‌ها به زاویه قطاع بستگی دارد و تعداد لایه ها نیز به عرض هر لایه بستگی دارد. ما مقادیر مختلف را از حداقل ۵ درجه تا حداکثر ۹۰ درجه برای زاویه مذکور و عرض هر لایه را بین ۵ تا ۸۰ متر مورد بررسی قرار می‌دهیم که به ترتیب معادل تعداد ۷۲ تا ۴ قطاع و ۱۶ تا ۱ لایه می باشد. ما برای سادگی کار، زاویه قطاع ها را با عرض هر لایه، برابر در نظر گرفته ایم. به عنوان مثال در شکل(۱) زاویه قطاع برابر با ۳۰ درجه و عرض هر لایه برابر با ۳۰ متر در نظر گرفته شده است.



شکل ۱: مدل شبکه و نمایش قطاع و لایه

فرض می‌کنیم که هر گره در ابتدای راه‌اندازی شبکه شماره لایه و قطاعی که در آن واقع است را می‌داند[۹][۲۱][۲۲].

مدل انرژی ارسال و دریافت داده مطابق با مدل انرژی در LEACH [۲۰] در نظر گرفته شده است، بدین‌گونه که اگر فاصله فرستنده تا گیرنده (d) بیشتر از d0 باشد T از مدل چند مسیری (اتلاف توان d4) و درغیراین‌صورت از مدل فضای آزاد (اتلاف توان d2) برای ارسال (l) بیت داده استفاده می شود.

$$E_{Tx}(l,d) = E_{Tx-elec}(l) + E_{Tx-amp}(l,d) = \begin{cases} lE_{elec} + l\varepsilon_{fs}d^2 & d < d_0 \\ lE_{elec} + l\varepsilon_{mp}d^4 & d \geq d_0 \end{cases} \quad (۱)$$

$$E_{Rx}(l) = E_{Rx-elec}(l) = lE_{elec} \quad (۲)$$

Eelec : مقدار انرژی مصرفی برای راه‌اندازی مدار فرستنده یا گیرنده و ε_{amp}: انرژی مورد نیاز تقویت‌کننده انتقالی برای دستیابی به E_b/N_0 مورد قبول، می‌باشد.

۳-۲ مدل حمله wormhole

حمله wormhole با برقراری یک لینک با تاخیر کم (تونل) بین دو نقطه شبکه آغاز می‌شود و سپس بسته‌ها در ابتدای تونل دریافت و از طریق این تونل منتقل می‌شوند و در انتهای تونل مجددا پخش می‌شود و به این ترتیب گره هایی که درواقع دور از هم هستند، تصور می‌کنند که همسایه یا نزدیک به هم هستند. در شکل ۱ یک نمونه wormhole در شبکه نشان داده شده است.

فرض می‌کنیم که در ابتدای راه‌اندازی شبکه، wormholeی وجود ندارد ولی بعدا ممکن است یک یا حتی چند حمله wormhole همزمان صورت گیرد.

۴- راه حل پیشنهادی

همانطور که اشاره شد، در الگوریتم پیشنهادی ایستگاه اصلی مجهز به آنتن جهتدار می‌باشد و با اسکن نمودن شبکه قادر به کشف و تعیین محل wormholeها می‌باشد. اسکن نمودن شبکه توسط ایستگاه اصلی از دو مرحله اسکن قطاعی و اسکن لایه‌ای تشکیل شده است. اسکن قطاعی با توجه به قابلیت آنتن‌های جهتدار[۹] امکانپذیر خواهد بود، بدین صورت که ایستگاه اصلی بسته‌ها را به قطاع‌هایی با زاویه مشخص ارسال می‌نماید و اسکن لایه‌ای نیز با تنظیم شعاع ارسال همه‌پخشی ایستگاه اصلی میسر می‌باشد (شکل۱) [۹][۲۱][۲۲]. در همان ابتدای کار با فرض عاری بودن شبکه از وجود wormhole، گره‌های حسگر با دریافت بسته HELLO از ایستگاه اصلی، شماره قطاع و لایه خود را تعیین می‌نمایند. در ادامه جزئیات الگوریتم ارائه‌شده را در این دو مرحله به طور کامل شرح خواهیم داد.

مرحله ۱: اسکن قطاعی

در این مرحله ایستگاه اصلی، s قطاع شبکه را در جهت پادساعتگرد اسکن می‌نماید ($s=360/\theta$ و θ زوایه هر قطاع می‌باشد). برای انجام این کار، ایستگاه اصلی به قطاع iام بسته DWE را ارسال می‌نماید؛ این بسته شامل دو فیلد اصلی (s#,TS) است که s# شماره قطاع iام وTS مهرزمان، برای نشان دادن بسته های جدید می‌باشد. اگر گره حسگری این بسته را دریافت نماید و شماره قطاعش مخالف با s# باشد، بسته WNP را برای ایستگاه اصلی به صورت تک‌گامی ارسال می‌کند. فیلدهای این بسته عبارتند از: (myID, mySectoy#, rceRSSI)، که myID همان شناسه گره حسگر، mySector# شماره قطاع حسگر و rceRSSI شدت انرژی سیگنال دریافتی بسته DWE می‌باشد.

این امکان که حسگری در قطاع jام بسته‌ای با شماره قطاع i را دریافت نماید، تنها زمانی رخ می‌دهد که یک گره wormhole این بسته را در قطاع شماره i دریافت نماید و آنرا برای گره همدست خود به قطاع شماره j ارسال نماید و حسگر همدست، این پیام را در قطاع jام با شعاع مشخصی ارسال نماید. دراین‌صورت برخی از حسگرهای قطاع jام بسته WNP را برای ایستگاه اصلی ارسال می‌کنند و ایستگاه اصلی شماره قطاع حسگری را که بسته DWE را با بیشترین مقدار rceRSSI دریافت کرده است، به عنوان موقعیت سر دیگر wormhole شناسایی می‌نماید. پس در این مرحله، ایستگاه اصلی با اسکن قطاعی خواهد توانست شماره قطاع‌های دو سر wormhole را شناسایی نماید. اما برای مشخص نمودن دقیق‌تر موقعیت گره-های wormhole می‌بایست اسکن لایه‌ای مرحله دوم را نیز انجام دهد. تنها در مواقعی که دو سر گره wormhole در یک قطاع باشند، ایستگاه اصلی در این مرحله قادر به کشف wormhole نمی‌باشد. اما با توجه به موقعیت‌های گره‌های wormhole، شانس این وجود دارد که با اسکن لایه‌ای بتواند تنها وجود آنها را در شبکه کشف نماید.

مرحله ۲: اسکن لایه‌ای

این اسکن به دو دلیل توسط ایستگاه اصلی انجام می‌پذیرد: ۱) جهت مشخص شدن دقیق‌تر موقعیت گره‌های wormhole ای که شماره قطاع آنها در مرحله قبل بدست آمده است.۲) جهت کشف wormhole هایی که در مرحله قبل به دلیل قرار گیری در یک قطاع کشف نشده‌اند.

در این اسکن، ایستگاه اصلی مجددا بسته DWE را با شعاع‌های متفاوت ارسال می‌نماید، با این تفاوت که شماره لایه(l#) را جایگزین شماره قطاع(s#) بسته DWE خواهد کرد. حسگری که بسته DWE را با شماره لایه‌ای متمایز با شماره لایه‌ای که

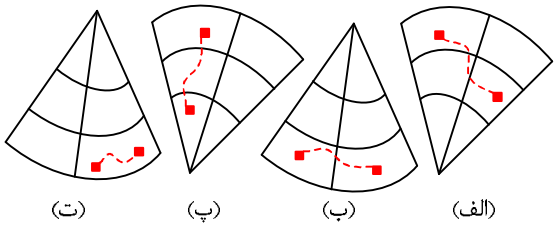
در آن مستقر است، دریافت نماید، بسته WNP را با همان ساختار بالا به همراه شماره لایه خود (mylayer#) به صورت تک‌گامی به ایستگاه اصلی ارسال می‌نماید. با فرض این‌که ایستگاه اصلی بسته DWE را به لایه l1 ارسال نماید و بسته WNP را از گره حسگری در لایه l2 و قطاع s2 دریافت کند (شماره قطاع‌های s1و s2 از مرحله قبل بدست آمده است) می‌تواند محل دقیق گره wormhole را به صورت (s1, l1) و (s2, l2) مشخص نماید. در صورتی که دو گره wormhole در یک لایه قرار گرفته باشند، ایستگاه اصلی فقط می‌تواند به اطلاعات بدست آمده از مرحله قبل اکتفا نماید. با توجه به دو مرحله‌ی الگوریتم پیشنهادی چهارحالت ذیل را خواهیم داشت:

۱- گره‌های wormhole در قطاع‌ها و لایه‌های متفاوتی قرار گرفته اند: الگوریتم پیشنهادی قادر به تعیین شماره لایه‌ها و قطاع‌ها می‌باشد.(شکل۲- قسمت الف)

۲-گره‌های wormhole در یک لایه و قطاع‌های مجزا قرار گرفته‌اند: الگوریتم پیشنهادی فقط قادر به تعیین شماره قطاع‌ها می‌باشد. (شکل۲- قسمت ب)

۳-گره‌های wormhole در یک قطاع و لایه‌های مجزا قرار گرفته‌اند: الگوریتم پیشنهادی فقط قادر به تعیین شماره لایه‌ها می‌باشد. (شکل۲- قسمت پ)

۴- گره های wormhole در یک قطاع ویک لایه قرار گرفته‌اند: الگوریتم پیشنهادی قادر به کشف wormhole نمی-باشد(شکل۲- قسمت ت). در این حالت گره های wormhole به دلیل نزدیک بودن به یکدیگر قادر به مختل نمودن عملکرد شبکه به صورت سراسری نمی‌باشند بلکه همان قطاع و لایه ای را که در آن قرار گرفته اند، مورد حمله قرار خواهند داد.



شکل ۲: حالت‌های مختلف قرارگرفتن wormhole

۵- نتایج شبیه سازی

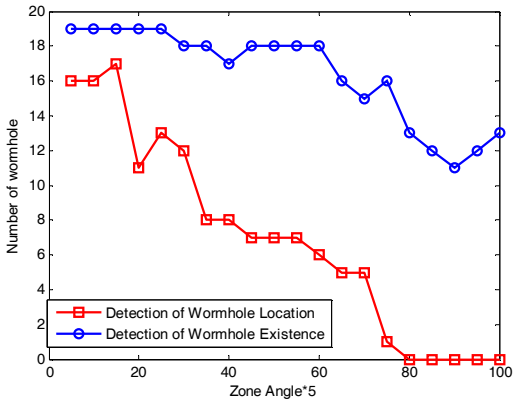
برای ارزیابی راه‌حل پیشنهادی شبیه‌سازی به کمک نرم افزار Matlab انجام شد. مشخصه های شبیه‌سازی در جدول ۱ ارائه شده‌اند.

جدول شماره ۱: پارامتر های شبیه سازی

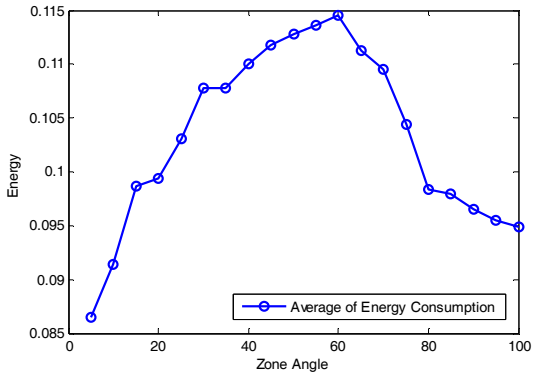
عنوان	مقدار
R	100m
r	20m
تعداد حسگر(N)	100 ~ 1000
شعاع پوشش	20m
انرژی اولیه	0.1 J
$\mathbf{E_{elect}}$	50 nJ/bit
$\boldsymbol{\varepsilon_{fs}}$	10 pJ/bit/m^2
اندازه بسته‌ها	128 byte

تعداد Wormhole	20

نتایج شبیه‌سازی در شکل‌های ۳ تا ۵ ارائه شده است. در شکل ۳ تعداد wormholeهای کشف‌شده و تعداد wormholeهایی که موقعیت آنها تعیین شده است، برحسب زاویه قطاع نشان داده شده است. مطابق این شکل هرچه زاویه قطاع کمتر باشد، احتمال کشف wormhole بیشتر است که این مسأله با توجه به دقت بیشتر در حالت قطاع‌های کوچک‌تر قابل توجیه می‌باشد. شکل ۱ همچنین نشان می‌دهد که بیشترین احتمال تشخیص موقعیت wormhole مربوط به زاویه قطاع ۱۵ درجه است. علت این است که با قطاع‌های کوچک‌تر احتمال این که در دو قطاعی که سرهای wormhole را دربردارند، گره ی وجود نداشته باشد و بنابراین wormhole به ایستگاه اصلی گزارش نشود، زیاد است. از طرف دیگر با قطاع‌های خیلی بزرگ احتمال این که دو سر wormhole در یک قطاع باشد و بنابراین گره ها حالت غیرعادی را احساس نکنند، افزایش می‌یابد.

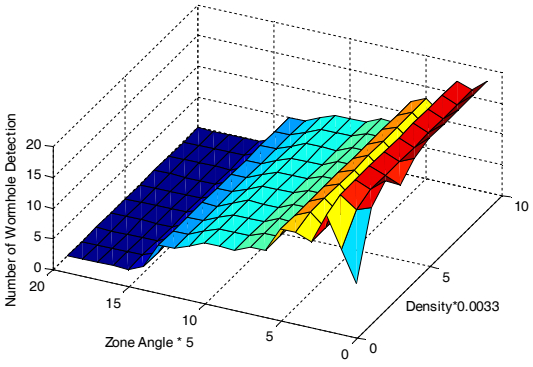


شکل ۳: نرخ کشف wormhole و تعیین موقعیت آن برحسب زاویه قطاع



شکل ۴: میانگین مصرف انرژی برحسب زاویه قطاع

شکل ۴ میانگین مصرف انرژی مصرفی کل شبکه را برحسب زاویه قطاع نشان می‌دهد. این مقدار به ازاء زاویه قطاع ۶۰ درجه به حداکثر مقدار خود می‌رسد. علت این است که تعداد حسگر های بیشتری ایستگاه اصلی را از وجود گره wormhole آگاه می سازند. اما با قطاع‌های کوچک‌تر تعداد گره هایی کمتری در صورت تشخیص وجود wormhole پیام WNP را به ایستگاه گزارش می‌کنند. ازطرف دیگر با قطاع‌های خیلی بزرگ احتمال کشف نشدن wormhole توسط گره ها افزایش می‌یابد زیرا دو سر Wormhole با احتمال زیادی در یک قطاع و یک لایه قرار خواهند گرفت. در این شرایط گره ها هیچ بسته‌ای به ایستگاه اصلی گزارش نمی‌کنند و سطح میانگین انرژی مصرفی شبکه کاهش می یابد.



شکل ۵: نرخ کشف wormhole برحسب زاویه قطاع و چگالی گره ها

شکل ۵ نرخ کشف wormhole و تعیین موقعیت آنرا برحسب زاویه قطاع و چگالی گره های شبکه نشان می‌دهد. همانطور که در این شکل مشاهده می گردد، این نرخ با افزایش زاویه قطاعها کاهش یافته و به صفر می رسد، که دلیل آن بالارفتن احتمال قرارگیری دو سرwormhole در یک قطاع و یک لایه می باشد. با افزایش چگالی حسگر ها نیز نرخ کشف wormhole و تعیین موقعیت آن بالا می رود. همانطور که مشاهد می شود در چگالی و زاویه قطاع پایین، این نرخ به دلیل کاهش احتمال وجود حسگری که بتواند، ایستگاه اصلی را از حضور wormhole با خبر سازد، پایین است و این احتمال با افزایش چگالی افزایش پیدا خواهد کرد.

۶- نتیجه گیری

در این مقاله یک راه‌حل جدید و ابتکاری برای کشف wormhole در شبکه‌های حسگر بی‌سیم ارائه کردیم. این راه‌حل براساس اسکن فضای شبکه توسط ایستگاه اصلی به دو صورت قطاعی و لایه‌ای عمل می‌کند. ارزیابی‌ها نشان می‌دهد که با انتخاب مناسب زاویه قطاع و لایه، نرخ کشف wormhole درحدود ۹۵درصد و نرخ تعیین موقعیت wormhole درحدود ۸۵درصد به‌دست خواهد آمد.

مراجع

[۲۲] فرزاد تشتریان، عباس قائمی بافقی و محمدحسین یغمائی مقدم، **"ارائه یک الگوریتم کشف wormhole کارا و مبتنی بر آنتن‌های جهت-دار در شبکه‌های حسگر بی‌سیم"**، هفتمین کنفرانس انجمن رمز ایران، دانشگاه خواجه نصیر طوسی، ۱۳۸۹.

[1] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks.," in INFOCOM, 2003.

[2] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in Proc. SCS Communication Networks and Distributed Systems Modeling and Simulation, 2002.

[3] K. Sanzgiri, B. Dahill, B. Levine, C Shields, and E. Belding-Royer, "A secure routing protocol for ad hoc networks," in ICNP, 2002, pp. 78–89.

[4] Issa Khalil, Saurabh Bagchi, and Ness B. Shroff, "Liteworp: A lightweight countermeasure for the wormhole attack in multihop wireless networks.," in DSN, 2005, pp. 612–621.

[5] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad-hoc wireless networks," in Mobile Computing. Kluwer Academic, 1996.

[6] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in Proc. IEEE Workshop on Mobile Computing Systems, 1999.

[7] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance vector routing (dsdv) for mobile computeres," in Proc. ACM SIGCOMM, Sep. 1994.

[8] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in IEEE INMIC, 2001.

[9] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in Network and Distributed System Security Symposium (NDSS), 2004.

[10] *L. Lazos, R. Poovendran, C. Meadows, P. Syverson, and L. W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach," in the IEEE Wireless Communications and Networking Conference (WCNC05), Volume 2, 13-17, pp. 1193 – 1199, 2005.*

[11] Farid Naït-Abdesselam,˝ *Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks*˝ SECURITY IN MOBILE AD HOC AND SENSOR NETWORKS IEEE Communications Magazine • April 2008

[12] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan," *Detecting and Locating Wormhole Attacks in Wireless Sensor Networks Using Beacon Nodes*",World Academy of Science, Engineering and Technology 55 2009

[13] *Levente Butty´an, L´aszl´o D´ora, and Istv´an Vajda. Statistical wormhole detection in sensor networks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, ESAS, volume 3813 of Lecture Notes in Computer Science, pages 128–141. Springer, 2005.*

[14] *L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path," In Proc. IEEE Wireless Communications & Netwoking Conference (IEEE WCNC), New Orleans, USA, Mar. 2005.*

[15] *Y. C. Hu, A.Perrig, and D. B. Johnson," Wormhole Attacks in Wireless Networks," IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.*

[16] *Weichao Wang, Bharat Bhargava, Yi Lu, and Xiaoxin Wu. Defending against wormhole attacks in mobile ad hoc networks. In Wiley Journal Wireless Communications and Mobile Computing (WCMC), volume 6, pages 483 –503.Wiley, 2006.*

[17] *Radha Poovendran and Loukas Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," ACM Journal on Wireless Networks (WINET), 2005.*

[18] *J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "Truelink: A practical countermeasure to the wormhole attack in wireless networks," in Proc. of ICNP '06, 2006.*

[19] *I. Khalil, S. Bagchi, and N. B. Shroff, MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks, IEEE/CreateNet conference on Security and Privacy in Communication networks (SecureComm 2006), Baltimore, MD, August 28th – September 1st 2006, 12 pages.*

[20] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", (MobiCom'99), Seattle, WA, August 1999

[21] F. Tashtarian, A. T. Haghighat, M. T. Honary and H. Shokrzadeh, "A New Energy-Efficient Clustering Algorithm for Wireless Sensor Networks", to be appear in Proc. of the International Conference on Software, Telecommunications and Computer Networks SoftCOM September 27 - 29, 2007.