ارائه یک الگوریتم شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم به کمک انتشارات محلی و کانال‌های کرم‌چاله قانونی

رضا رافع[۱]، استادیار، فرشته خدادادی[۲]، دانشجوی کارشناسی ارشد

۱- گروه مهندسی کامپیوتر - دانشکده فنی و مهندسی - دانشگاه اراک - اراک - ایران - r-rafeh@araku.ac.ir
۲- گروه مهندسی کامپیوتر - دانشگاه آزاد اسلامی واحد ملایر - ملایر - ایران - f-khodadadi@yahoo.com

چکیده: یکی از حمله‌های خطرناک شناخته شده علیه شبکه‌های حسگر بی‌سیم، حمله تکرار گره است. در این حمله، دشمن یک یا چند گره نرمال درون شبکه را ضبط کرده، کپی‌هایی (گره‌های تکراری) از آن‌ها تولید و در شبکه منتشر می‌کند. این گره‌های کپی تحت کنترل دشمن می‌باشند که می‌توانند به راحتی با دیگر گره‌های شبکه کلید مشترک برپا کرده و به تبادل داده بپردازند. در این مقاله یک الگوریتم جدید، مبتنی بر اطلاعات محلی و استفاده از لینک‌های کرم‌چاله قانونی جهت شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم متحرک پیشنهاد می‌گردد. الگوریتم پیشنهادی از دو فاز تشخیص محلی و تشخیص غیرمحلی تشکیل شده است. در فاز تشخیص محلی، هر گره به‌طور مستقل با توجه به پیغام‌های "Hello" منتشر شده، گره‌های کپی موجود در همسایگی خود را شناسایی می‌کند. در فاز تشخیص غیرمحلی، گره‌های برپا کننده لینک‌های کرم‌چاله قانونی با توجه به انتشار پیغام‌های "Hello" اقدام به شناسایی گره‌های کپی می‌کنند. نتایج شبیه‌سازی نشان می‌دهد که الگوریتم پیشنهادی از نظر معیارهای نرخ تشخیص و سرعت تشخیص نسبت به الگوریتم‌های موجود عملکرد بهتری دارد.

واژه‌های کلیدی: شبکه‌های حسگر، حمله گره‌های کپی، کانال کرم‌چاله قانونی، تشخیص محلی، تشخیص سراسری.

Proposing a New Algorithm for Detecting Node Replication Attack in Wireless Sensor Networks based on the Local Propagations and Legal Wormhole Channels

R. Rafeh[1], F. Khodadai[2]

1- Department of Computer Engineering, Faculty of Engineering, Arak University, Arak, Iran,
2- Department of Computer Engineering, Islamic Azad University, Malayer Branch, Malayer, Iran,

Abstract: A common attack in wireless sensor networks is the node replication attack. In this attack, attackers capture a number of nodes and spread copies of them in the network. Replicated nodes, which are controlled by the attackers, start communicating with other nodes to corrupt network protocols. In this paper we propose a new algorithm for detecting replica nodes in wireless sensor networks with mobile nodes using the legal wormhole channels. The proposed algorithm consists of two phases: local detection and global detection. In the first phase, each node detects replica nodes in its neighborhood by disseminating "Hello" messages. In the second phase few nodes in the network establish legal wormhole channels pairwise and exchange the information of their neighbors. When there is a common node in these neighbors, that node is known as a replica node. The experimental results show that the proposed algorithm outperforms similar algorithms in terms of detection rate and detection time.

Keywords: Wireless Sensor Network, Node Replication Attack, Legal Wormhole Channel, Local Detection, Global Detection.

تاریخ ارسال مقاله: ۱۳۹۳/۱/۱۸
تاریخ اصلاح مقاله: ۱۳۹۳/۲/۸
تاریخ پذیرش مقاله: ۱۳۹۳/۲/۳۰
نام نویسنده مسئول: رضا رافع
نشانی نویسنده مسئول: ایران - اراک – میدان سردشت - دانشگاه اراک - گروه مهندسی کامپیوتر

۱- مقدمه

امروزه شبکه‌های حسگر بی‌سیم در بسیاری از کاربردها، نظیر محیط‌زیست، عملیات نظامی و اکتشافات استفاده می‌شوند. از آنجا که گره‌های حسگر قابلیت‌های محاسباتی، حافظه‌ای و رادیویی پایینی دارند و با توجه به کاربرد این‌گونه شبکه‌ها در محیط‌های بحرانی و خصوصاً نظامی، برقراری امنیت در این شبکه‌ها امری بسیار مهم بوده و مورد توجه بسیاری از محققان قرارگرفته است [۱ و ۲].

یکی از حمله‌های خطرناک در شبکه‌های حسگر بی‌سیم حمله تکرار گره[۱] است. دشمن می‌تواند یک گره را ضبط کند و اطلاعات مهم از جمله اطلاعات کلید[۲] داخل آن را استخراج و با استفاده از این اطلاعات گره‌های تکراری (یا گره‌های کپی) ایجاد کند. گره‌های کپی قابلیت برپایی کلید با گره‌های قانونی را دارند. دشمن می‌تواند این گره‌های کپی را در شبکه پخش کرده و حمله‌های مختلفی را راه‌اندازی کند. گره‌های کپی توسط دشمن کنترل می‌شوند، ولی دارای اطلاعات قفل‌گذاری می‌باشند که به آن‌ها اجازه می‌دهد شبیه گره‌های مجاز در شبکه به نظر آیند. پروتکل‌هایی که برای ارتباطات ایمن شبکه‌های حسگر استفاده می‌شوند، این اجازه را به گره‌های تکراری می‌دهند تا کلیدهای جفتی با دیگر گره‌ها و ایستگاه پایه برقرار کنند. بنابراین گره‌های تکراری قادر به رمزگذاری، رمزگشایی و تصدیق همه مخابره‌هایشان هستند. دشمن می‌تواند از این موقعیت درون‌شبکه‌ای به روش‌های مختلف بهره‌برداری کند. برای مثال، دشمن می‌تواند به‌سادگی بخش اعظمی از ترافیک شبکه که از طریق گره‌های کپی عبور می‌کند را نظارت کند، با تزریق داده‌های تحریف‌شده عملیات نظارتی حسگرها را خراب کند و پروتکل‌های رایج شبکه‌های حسگر از جمله خوشه‌بندی و تجمع داده‌ها را مختل کند[۳، ۴ و ۵]. تاکنون الگوریتم‌هایی جهت مقابله با حمله تکرار گره در شبکه‌های حسگر ثابت توسط محققان در [۱۳-۶] ارائه شده است که در شبکه‌های حسگر متحرک قابل به‌کارگیری نیستند. در [۲۳-۱۴] نیز الگوریتم‌هایی جهت مقابله با حمله تکرار گره در شبکه‌های حسگر متحرک ارائه شده است.

ایده اصلی الگوریتم ارائه‌شده در [14] برگرفته از این واقعیت است که برای شبکه‌های بدون گره‌های تکراری، اگر یک گره حسگر u در زمان T1 گره دیگری نظیر v را ملاقات کرده باشد و گره u در همان زمان (T1) یک عدد تصادفی r را برای v ارسال کرده باشد، هنگامی‌که گره‌های u و v مجدداً همدیگر را در زمان T2 ملاقات کنند، اگر گره u از v درخواست ارسال عدد تصادفی کند، گره u همان عدد تصادفی r‌ای را دریافت خواهد کرد که در زمان T1 برای v فرستاده بود. در غیر این صورت شبکه حاوی گره‌های تکراری v است. بنابراین گره u می‌تواند با درخواست عدد تصادفی r از گره v مطمئن شود آیا این همان گره v است که قبلاً آن را ملاقات کرده بود یا خیر. معایب این الگوریتم عبارت‌اند از: سربار بالای ارتباطاتی، کند بودن فرآیند تشخیص گره‌های تکراری و مسائل امنیتی. البته در صورت همکاری گره‌های تکراری، کارایی الگوریتم پایین می‌آید. اگر هر گره تکراری اعداد تصادفی موجود در حافظه خود را در اختیار سایر گره‌های کپی قرار دهد، فرآیند شناسایی این گره‌های کپی می‌توانند با شکست مواجه شود.

در [۱۵] یک الگوریتم دیگر جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک بر اساس تست ترتیبی نرخ احتمال (SPRT[۳]) مطرح شده است. در این مقاله ادعا شده است که الگوریتم ارائه شده اولین الگوریتم مطرح‌شده جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک است. ایده اصلی این الگوریتم برگرفته از این حقیقت است که یک گره متحرک ضبط نشده نباید هرگز در سرعتی بیش از حداکثر سرعت سیستم پیکربندی‌شده حرکت کند. گره‌های کپی همزمان در دو یا چند مکان مختلف شبکه قرار دارند که باعث چنین برداشتی می‌شود که گره‌های تکراری سرعت خیلی بیش‌تری نسبت به گره‌های معمولی دارند و بنابراین سرعت محاسبه‌شده برای گره‌های تکراری اغلب بیش‌تر از حداکثر سرعت سیستم پیکربندی‌شده می‌شود. معایب این الگوریتم عبارت‌اند از: متمرکز بودن، نیاز به همگام‌سازی، استفاده از کلیدهای عمومی(که برای گره‌های حسگر پرهزینه می‌باشند) و وجود سخت‌افزار اضافی برای تعیین مکان گره‌ها و وارسی مکان اعلان‌شده همسایه‌های گره (به‌طورکلی تعیین مکان گره‌های حسگر در شبکه‌های حسگر متحرک عملاً پرهزینه و مشکلی است).

در این مقاله یک الگوریتم سبک‌وزن و کارا به کمک اطلاعات محلی گره‌ها و لینک‌های کرم‌چاله[۴] قانونی جهت شناسایی گره‌های کپی در شبکه‌های حسگر متحرک پیشنهاد می‌گردد، به‌طوری‌که معایب الگوریتم‌های موجود را برطرف کند. الگوریتم پیشنهادی نیاز به تعیین مکان گره‌ها، انتشار پیغام‌های اعلام مکان، کلیدهای عمومی (و امضای دیجیتال) و فرایندهای پیچیده تشخیص گره‌های کپی ندارد.

ادامه این مقاله بدین ترتیب سازمان‌دهی می‌شود: بخش۲ به مرور کارهای گذشته می‌پردازد. در بخش ۳ راجع به حمله کرم‌چاله توضیحاتی داده شده است. مدل سیستم و فرضیات در بخش ۴ آمده است. در بخش ۵ الگوریتم پیشنهادی شرح داده می‌شود. ارزیابی الگوریتم پیشنهادی و نتیجه‌گیری به ترتیب در بخش‌های ۶ و ۷ آمده است.

۲- کارهای گذشته

در این بخش به معرفی الگوریتم‌های موجود جهت شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم می‌پردازیم و آن‌ها را از نظر ثابت یا متحرک بودن گره‌ها به دو دسته تقسیم می‌کنیم.

۲-۱- الگوریتم‌های شناسایی گره‌های تکراری در شبکه‌های حسگر ثابت

در [۶] چهار الگوریتم احتمالاتی توزیع‌شده به نام‌های NNB[۵]، DM[۶]، RM[۷] و LSM[۸] جهت شناسایی گره‌های تکراری در شبکه‌های حسگر ثابت ارائه شده است که از رمزنگاری کلید عمومی استفاده می‌کنند. NNB از پروتکل ساده همه‌پخشی بهره می‌گیرد. در این روش هر گره یک پیغام حاوی اطلاعات مربوط به موقعیت مکانی خودش را در کل شبکه منتشر می‌کند تا به دست همه گره‌ها برسد. هر گره اطلاعات مکانی همسایه‌هایش را ذخیره می‌کند و اگر یک ادعای مکانی ناسازگار دریافت کند آن گره را به‌عنوان خاطی در نظر می‌گیرد. در این روش اگر همه پیغام‌ها (حاوی موقعیت مکانی گره‌ها) به دست همه گره‌ها در شبکه برسد، نرخ تشخیص حمله تکرار گره ۱۰۰٪ خواهد بود ولی هزینه ارتباطات $O(n^2)$ خواهد شد. به‌منظور بهبود هزینه ارتباطات این روش، الگوریتم DM مطرح‌شده که در آن فقط از یک زیرمجموعه محدود از گره‌ها با نام گره‌های شاهد[۹] جهت ارسال پیغام‌های ادعای موقعیت مکانی استفاده می‌شود. وقتی‌که یک گره موقعیت مکانی خود را منتشر می‌کند، همسایه‌هایش این پیغام را به گره‌های شاهد ارسال می‌کنند. گره‌های شاهد به‌طور قطعی و بر اساس یک تابع از شناسه گره انتخاب می‌شوند. اگر دشمن یک گره را تکرار کرده باشد، گره‌های شاهد دو مکان ادعاشده مختلف برای یک شناسه دریافت خواهند کرد. اگرچه این الگوریتم هزینه ارتباطات را کم می‌کند ولی ایمنی و توانایی بالایی ندارد. به‌منظور افزایش ایمنی، الگوریتم RM ارائه شده است. در RM هنگامی‌که یک گره پیغام مربوط به موقعیت مکانی خود را منتشر می‌کند، هر یک از همسایه‌هایش (با احتمال p) یک کپی امضاءشده از این موقعیت مکانی ادعاشده را به یک مجموعه از گره‌ها (تحت عنوان گره‌های شاهد که به‌صورت تصادفی انتخاب شده‌اند) ارسال می‌کنند. هر یک از این گره‌های شاهد اگر وجود یک گره در دو مکان مختلف، در یک برهه زمانی یکسان را تشخیص دهند، آن گره را به‌عنوان گره تکراری یا گره کپی علامت می‌زنند. الگوریتم LSM شبیه RM رفتار می‌کند ولی یک اصلاح کوچک دارد که موجب بهبود قابل ملاحظه‌ای در نرخ تشخیص می‌شود. هنگام ارسال پیغام‌های ادعای مکانی به‌سوی گره‌های شاهد، هر گره (میانی) که این پیغام را مسیردهی می‌کند، امضای آن را بررسی، پیغام را ذخیره و سازگاری آن را با دیگر موقعیت-های مکانی ادعاشده در همان مرحله از تکرار الگوریتم بررسی می‌کند. سرانجام گره‌های تکراری توسط گره شاهد واقع در تقاطع دو مسیر که از دو نقطه مختلف شبکه توسط گره‌های با شناسه یکسان آغاز شده‌اند شناسایی می‌شود.

در [۷] یک پروتکل دیگر به نام SET جهت تشخیص گره تکراری مطرح شده است. SET از عملیات مجموعه‌ایی (اجتماع و اشتراک) روی زیرمجموعه‌های انحصاری در شبکه جهت تشخیص گره‌های کپی استفاده کند. در [۸] دو الگوریتم دیگر به نام‌های SDC[۱۰] و P-MPC[۱۱] مبتنی بر رویکرد "چندپخشی محلی شده[۱۲]" یا LM برای تشخیص گره‌های تکراری مطرح شده است. این الگوریتم‌ها در شبکه‌های حسگر با توپولوژی گرید کار می‌کنند. در الگوریتم SDC از یک تابع درهم‌سازی جغرافیایی [24] جهت نگاشت یکتا و تصادفی شناسه گره L به یک سلول در گرید استفاده می‌شود. تفاوت الگوریتم P-MPC با SDC در نحوه انتخاب سلول مقصد جهت ارسال ادعاهای مکانی است. در SDC هر ادعای مکانی به یک سلول قطعی منفرد ارسال می‌شود ولی در P-MPC ادعای مکانی به چندین سلول قطعی با احتمال‌های مختلف نگاشت و ارسال می‌شود.

در [۹] یک الگوریتم متمرکز دیگر به نام RED ارائه گردیده که ایده اصلی این روش نیز ارسال ادعاهای مکانی (دارای امضاء دیجیتالی) به مکان‌هایی از شبکه است که برحسب یک مقدار تصادفی منتشرشده توسط یک نقطه مرکزی (به‌طور پریودیک) انتخاب می‌شود. در [10] نیز به بررسی بیشتر و دقیق‌تر الگوریتم RED پرداخته شده است.

در [۱۱] به‌منظور شناسایی گره‌های کپی در یک شبکه حسگر بی‌سیم، یک پروتکل توزیع‌شده، قطعی و ارتجاعی[۱۳] (DDR) بر اساس یک استراتژی مبتنی بر گره شاهد مطرح شده است. در DDR، هنگامی‌که یک پیغام ادعای مکانی از یک گره به‌سوی مکان مقصد تصدیق شده ارسال می‌شود، سازگاری پیغام‌ها در گره‌های میانی موجود در مسیر به سمت مقصد نهایی بررسی می‌شود. چون DDR فقط از رمزنگاری کلید متقارن استفاده می‌کند در مقایسه با پروتکل‌های قبلی کارایی بهتری از نظر ارتباطات و محاسبات دارد.

در [۱۲] نیز دو الگوریتم دیگر به نام‌های RAWL[۱۴] و TRAWL[۱۵] مطرح شده است. در RAWL، برای هر گره u چندین قدم به تصادف در شبکه برداشته می‌شود و گره‌هایی که مورد عبور واقع شده‌اند به‌عنوان شاهدان گره u انتخاب می‌شوند. تحلیل‌های انجام‌شده در [۱۲] نشان می‌دهد که مرحله قدم برداشتن برای شناسایی گره‌های تکراری با احتمال بالا دارای مرتبه $O(\sqrt{n}\ \log n)$ است. الگوریتم TRAWL مبتنی بر RAWL است و یک جدول ردیابی[۱۶] به هر گره اضافه می‌کند تا هزینه حافظه را کاهش دهد.

در [۱۳] یک الگوریتم مبتنی بر حس‌کردن فشرده[۱۷] به نام CSI[۱۸] جهت تشخیص گره‌های کپی مطرح شده است. بینش کلیدی در طراحی CSI این است که تعداد گره‌های کپی در یک شبکه معمولاً محدود است. نویسندگان این مقاله عقیده دارند که برای یک دشمن به‌صرفه نیست که برای گرفتن کنترل شبکه یا مختل کردن عملیات شبکه بخواهد تعداد زیادی از گره‌های کپی را بسازد (هزینه ساخت گره‌های کپی زیاد است). بنابراین راه معقول برای دشمن این است که با کپی‌های کم‌تری شبکه را موردحمله قرار دهد. ایده اساسی CSI این است که هر گره یک عدد ثابت a به همسایه‌های تک‌گامه خود منتشر می‌کند. این عدد ثابت a می‌تواند به‌عنوان داده‌های حس شده توسط هر گره حسگر پنداشته شود. گره‌های حسگر از طریق تکنیک‌های جمع‌آوری داده‌ها (مبتنی بر حس) اعداد دریافتی از گره‌های فرزند[۱۹] در طول درخت تجمیع را ارسال یا تجمیع می‌کنند. ایستگاه پایه به‌عنوان ریشه درخت تجمیع، داده‌های تجمیع شده را دریافت و داده‌های حس

شده شبکه را بازیابی می‌کند. ایستگاه پایه با توجه به این داده‌های بازیابی شده اقدام به شناسایی گره‌های کپی می‌کند.

۲-۲- الگوریتم‌های شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک

در [۱۴] و [۱۵] الگوریتم‌هایی جهت مقابله با حمله تکرار گره در شبکه‌های حسگر متحرک مطرح شده است. همان‌طور که در بخش ۱ توضیح داده شد، الگوریتم [۱۴] مبتنی بر تولید و مبادله اعداد تصادفی بین گره‌ها است و الگوریتم [۱۵] نیز بر اساس سرعت حرکت گره‌ها در محیط شبکه اقدام به شناسایی گره‌های کپی می‌کند. در [۲۰] این روش بهبود داده شده است.

در [۱۶] یک الگوریتم دیگر به نام EDD[۲۰] برای مقابله با حمله تکرار گره در شبکه‌های حسگر متحرک مطرح شده است. ایده اصلی این الگوریتم برگرفته از این مطلب است که برای یک شبکه بدون گره تکراری، در یک دوره زمانی مشخص با طول T، تعداد دفعات (μ_1) رویارویی گره u با یک گره خاص v به احتمال زیاد باید محدود باشد. برای یک شبکه با دو گره تکراری v، تعداد دفعات (μ_2) رویارویی گره u با گره v در یک دوره زمانی با طول T باید بزرگ‌تر از یک آستانه باشد.

در [۱۷] یک الگوریتم ترکیبی جهت مقابله با حمله تکرار گره ارائه شده است. این الگوریتم در واقع از ترکیب الگوریتم‌های متمرکز و توزیع‌شده استفاده می‌کند. محیط شبکه به سکتورهایی مجزا تقسیم می‌شود و هر سکتور یک گره مرکزی دارد که گره‌ها می‌توانند شناسه‌هایشان را جهت بررسی به آن ارسال کنند. گره مرکزی می‌تواند هم به‌عنوان یک گره حس‌کننده محیط عمل کند و هم حمله‌های تکرار گره را تشخیص دهد. هر گره مرکزی واقع در هر سکتور، لیست شناسه و مکان گره‌های موجود در آن سکتور را نگه‌داری می‌کند.

در [۱۸] نیز با استفاده از کلید جفتی[۲۱] و فیلتر بلوم یک الگوریتم متمرکز جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک ارائه شده است که نیازمند اطلاعات مکانی گره‌ها نیست.

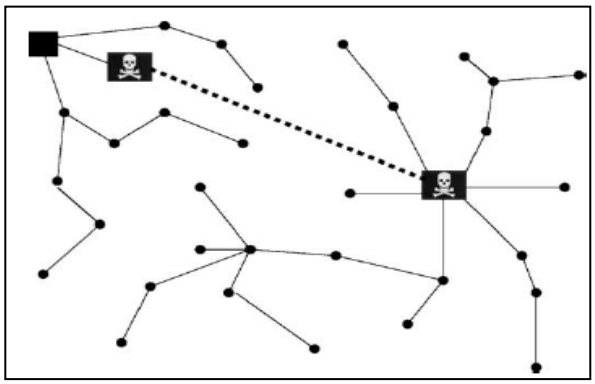
در [19] با توسعه مسئله مسیریابی به کمک تحرک، یک الگوریتم تشخیص نفوذ (SHD[۲۲]) برای شبکه‌های حسگر متحرک مطرح شده است. با توجه به این‌که دسترسی به اطلاعات مکانی گره‌ها مشکل است و مدل‌های تحرک متفاوت هستند، الگوریتم SHD این دو ضابطه را کنار می‌زند. الگوریتم SHD از مبادله لیست همسایه‌ها میان گره‌های متحرک و انتخاب گره‌های شاهد برای عمل تشخیص استفاده می‌کند. این الگوریتم در برابر تبانی گره‌های مهاجم در امان است. به‌طورکلی فرآیند تشخیص در SHD مبتنی بر ارسال پیغام $< ID, neighbor\_list >$ به گره‌ها در محدوده رادیویی خود در زمان شروع اجرای پروتکل و سپس استفاده از متدهای پرسش و پاسخ است.

در [۲۱] یک الگوریتم دیگر جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک مطرح شده است که از یک تصدیق هویت مبتنی بر نشانه جهت تشخیص گره‌های کپی استفاده می‌کند.

در [۲۲] نیز یک الگوریتم دیگر ارائه شده است که فقط از ارتباطات تک‌گامه و تحرک گره جهت شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک استفاده می‌کند.

۳- حمله کرم‌چاله

در حمله کرم‌چاله، دشمن دو گره در شبکه مستقر کرده و بین آن دو گره یک کانال اختصاصی و پرسرعت، تحت عنوان کانال کرم‌چاله راه‌اندازی می‌کند. به‌طوری‌که این دو گره می‌توانند به‌راحتی از طریق این کانال برای یکدیگر داده ارسال کنند. دو گره برپاکننده حمله کرم‌چاله معمولاً خیلی از هم دور می‌باشند و درواقع از یک نقطه شبکه به یک نقطه دیگر تونل می‌زنند. عملکرد این حمله به‌طور خلاصه بدین‌صورت است که گره‌های برپاکننده کانال کرم‌چاله، بسته‌های منتشرشده توسط گره‌های قانونی در یک ناحیه از شبکه (یک سر کانال) را به یک ناحیه دیگر از شبکه (سر دیگر کانال) ارسال کرده، در آنجا منتشر می‌کنند. این حمله تاثیر زیادی بر درخت‌های مسیریابی می‌گذارد. اگر دشمن در نزدیک یک ایستگاه پایه واقع شده باشد ممکن است با ایجاد یک "کرم‌چاله با مکان مطلوب"، قادر به تخریب کامل مسیریابی شود. شکل (۱)، نمونه‌ای از برپایی این حمله را نشان می‌دهد. به‌صورت کلی‌تر، کرم‌چاله‌ها می‌توانند جهت استخراج شرایط رقابتی مسیریابی استفاده شوند. شرایط رقابتی معمولاً زمانی رخ می‌دهد که یک گره به‌محض دریافت اولین نمونه از یک نوع پیغام خاص، یکسری عملیات را انجام می‌دهد و نمونه‌های بعدی آن را نادیده می‌گیرد. کرم‌چاله‌ها هم‌چنین می‌توانند با بازسازی بسته‌ها بین دو گره غیرهمسایه که فاصله زیادی از هم دارند آن‌ها را متقاعد کنند که با هم همسایه هستند تا با هم دیگر داده مخابره کنند. کرم‌چاله‌ها معمولاً در ترکیب با ارسال انتخابی یا استراق سمع[۲۳] استفاده می‌شوند.



شکل (۱): یک مثال از برپایی حمله کرم‌چاله[3]

۴- فرضیات سیستم و مدل حمله

فرض می‌شود شبکه حسگر حاوی n گره حسگر است که به‌طور تصادفی در یک ناحیه دوبعدی توزیع شده است. پس از فاز گسترش، گره‌های حسگر می‌توانند مطابق مدل‌های تحرک، نظیر مدل تصادفی، در محیط عملیاتی حرکت کنند. گره‌ها از موقعیت مکانی خودآگاه نیستند. هر گره یک شناسه یکتا دارد. فرض می‌شود که گره‌ها با یکدیگر از طریق کانال رادیویی بی‌سیم ارتباط برقرار کرده و از انتشار[۲۴] به شیوه همه-جهته[۲۵] استفاده می‌کنند. هر گره در حافظه خود یک کلید خصوصی دارد که ازآن‌جهت رمزگذاری داده‌ها و ارسال به ایستگاه استفاده می‌کند. هم‌چنین فرض می‌شود به تعداد W کانال کرم‌چاله قانونی در محیط شبکه وجود دارد. کانال کرم‌چاله قانونی درواقع کانالی است که توسط مدیر شبکه و به‌صورت قانونی در شبکه راه‌اندازی می‌شود. دو گره برپاکننده یک کانال کرم‌چاله قانونی ازنظر مکانی ثابت بوده و فاصله آن‌ها از هم بیش‌تر از 2r است. البته کانال‌های کرم‌چاله قانونی نیز می‌توانند متحرک باشند، به شرطی که فاصله دو گره برپاکننده یک کانال کرم‌چاله هیچ‌گاه کوچک‌تر یا مساوی 2r نشود. همه گره‌ها، به‌جز گره‌های برپاکننده کانال کرم‌چاله قانونی، امکانات سخت‌افزاری و نرم‌افزاری برابری (مثلاً ازنظر بُرد رادیویی، حافظه، انرژی) دارند. ولی گره‌های برپاکننده کانال‌های کرم‌چاله قانونی بُرد رادیویی بیش‌تری دارند، به‌طوری‌که دو گره دو سر یک کانال کرم‌چاله می‌توانند به‌طور مستقیم با یکدیگر مخابره کنند (دارای رادیو قوی‌تر هستند). هم‌چنین فرض می‌شود دو گره برپاکننده یک کانال کرم‌چاله قانونی پیغام‌های دریافتی از سوی همدیگر را در شبکه منتشر نمی‌کنند (عملی که گره‌های برپاکننده کانال کرم‌چاله غیرقانونی انجام می‌دهند). ازاین‌رو توسط الگوریتم‌های امنیتی مقابله با حمله کرم‌چاله (در صورت وجود این نوع الگوریتم در شبکه) شناسایی نمی‌شوند. هم‌چنین فرض می‌شود شبکه حسگر در یک محیط خصمانه گسترش می‌یابد، بنابراین شبکه ناامن بوده، دشمن می‌تواند گره‌هایی را ضبط کند و کپی‌هایی از این گره‌های ضبط‌شده را ایجاد و سپس در شبکه تزریق کند. هم‌چنین فرض می‌شود هر گره (نرمال و کپی) در هر دوره زمانی t، یک پیغام "Hello" منتشر می‌کند. نهایتاً فرض می‌شود گره‌های کپی همچون گره‌های نرمال در طول حیات شبکه، در محیط عملیاتی موردنظر متحرک می‌باشند.

۵- الگوریتم پیشنهادی

قبل از پرداختن به الگوریتم پیشنهادی باید اشاره شود که با توجه به تحرک گره‌های حسگر در محیط عملیاتی موردنظر، گره‌های حسگر باید به‌طور پریودیک (مثلاً بعد از هر t واحد زمانی) یک پیغام "Hello" منتشر کنند. این عمل درواقع یکی از نیازمندی‌های شبکه‌های حسگر متحرک است تا هر گره بتواند در هرلحظه همسایه-های جاری خود را شناسایی کرده، در صورت نیاز با آن‌ها کلیدهای اشتراکی برپا کند، داده مخابره کند و جدول مسیریابی خود را ایجاد کند. ازاین‌رو انتشار پریودیک پیغام "Hello" توسط گره‌ها در شبکه‌های حسگر متحرک یک فرض کاملاً منطقی است و ما نیز همین فرض را در الگوریتم پیشنهادی خود در نظر می‌گیریم. الگوریتم پیشنهادی که از دو فاز تشخیص محلی و تشخیص غیرمحلی تشکیل شده است، از این پیغام‌های "Hello" منتشر شده در جهت تشخیص گره‌های تکراری استفاده می‌کند. لذا الگوریتم پیشنهادی در طول حیات شبکه به‌طور پریودیک در فواصل زمانی t اجرا خواهد شد. در ادامه به شرح دو فاز الگوریتم پیشنهادی می‌پردازیم.

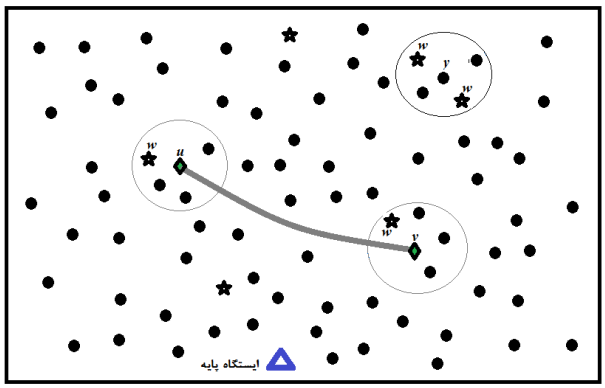
۵-۱- فاز اول: تشخیص محلی

در اولین فاز از الگوریتم پیشنهادی، هر گره قانونی به‌طور مستقل می‌تواند گره‌های تکراری را شناسایی کند. به‌این‌ترتیب که اگر یک گره در یک لحظه از زمان بیش از یک گره تکراری در همسایگی خودش داشته باشد می‌تواند تکراری بودن آن‌ها را تشخیص دهد. هر گره در حافظه خود لیستی (تحت عنوان لیست همسایگی) شامل شناسه‌های همسایه‌های ارسال‌کننده پیغام "Hello" در یک پریود زمانی را ذخیره می‌کند. هر گره u در پایان هر دوره زمانی t لیست همسایگی خود را بررسی کرده و اگر بیش از یک پیغام "Hello" از سوی یک گره با شناسه v دریافت کرده باشد، این گره را به‌عنوان گره تکراری شناسایی کرده و یک پیغام در شبکه منتشر می‌کند تا دیگر گره‌ها را نیز از این موضوع آگاه کند. گره‌های حسگر پس از هر دوره زمانی لیست همسایگی را از حافظه خود پاک می‌کنند. هرچه دشمن تعداد کپی‌های بیش‌تری از یک گره ضبط‌شده را در شبکه گسترش دهد، احتمال تشخیص گره‌های تکراری توسط فاز تشخیص محلی الگوریتم پیشنهادی بالاتر می‌رود.

۵-۲- فاز دوم: تشخیص غیرمحلی

در این بخش از الگوریتم پیشنهادی، با الگوبرداری از نحوه عملکرد حمله‌های کرم‌چاله اقدام به شناسایی گره‌های تکراری در شبکه‌های حسگر متحرک می‌کنیم. در حمله کرم‌چاله، دو گره در شبکه اگرچه همسایه تک‌گامه هم نیستند و در فاصله دوری از هم واقع شده‌اند ولی با راه‌اندازی یک تونل(لینک مستقیم) بین خودشان، داده‌های دریافتی از یک نقطه از شبکه را به نقطه‌ای دیگر از شبکه منتقل می‌کنند. در الگوریتم پیشنهادی از این ویژگی حمله کرم‌چاله جهت شناسایی گره‌های تکراری استفاده می‌شود. به‌این‌ترتیب که دو گره قانونی، مثلاً u و v در شبکه جهت راه‌اندازی یک حمله کرم‌چاله قانونی گسترش می‌یابند و یک کانال کرم‌چاله بین آن دو برقرار می‌شود. گره u در هر دوره زمانی t به پیغام‌های "Hello" ارسال‌شده از سوی گره‌های همسایه خود گوش‌داده، یک لیست همسایگی حاوی شناسه همسایه-های خود را ایجاد و از طریق این کانال به‌طور مستقیم به گره v ارسال می‌کند. گره v نیز همین عملیات را انجام می‌دهد. اگر در یک دوره

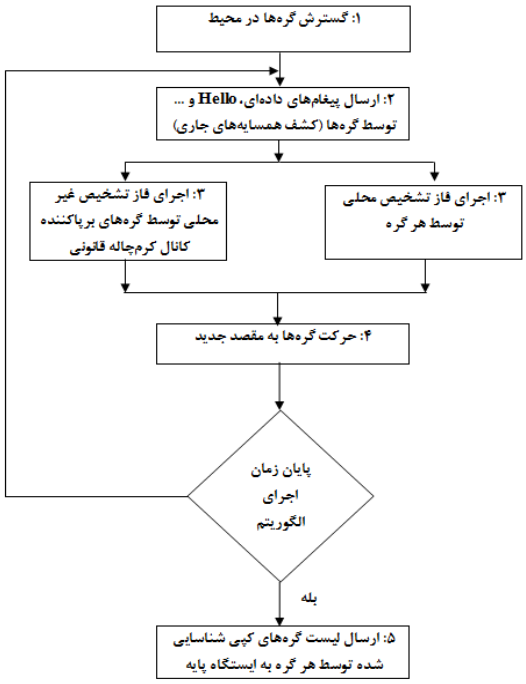
زمانی خاص، یک گره با شناسه w در همسایگی هر دو گره u و v قرار داشته باشد، با توجه به این‌که گره‌های u و v در دو نقطه مختلف (و دور از هم) از شبکه و در فاصله بیش‌تر از $2r$ واقع شده‌اند، می‌توان نتیجه گرفت که گره w تکراری است. در این صورت گره‌های u و v در یک پیغام رمزگذاری شده با کلید خصوصی اشتراکی بین خود و ایستگاه پایه، این موضوع را به ایستگاه پایه اطلاع داده، سپس ایستگاه پایه فرآیند باطل‌سازی شناسه w در شبکه را آغاز می‌کند. شکل (۲) به‌طور خلاصه نحوه عملکرد الگوریتم پیشنهادی را نشان می‌دهد.



شکل (۲): یک مثال از مدل شبکه و الگوریتم پیشنهادی

در شکل (۲)، گره‌های u و v به‌طور قانونی یک تونل بین خود برقرار می‌کنند. گره‌های با شناسه w هم گره‌های تکراری می‌باشند. در فاز تشخیص محلی، گره y می‌تواند وجود گره تکراری را تشخیص دهد، چراکه دو پیغام "Hello" با شناسه یکسان w را دریافت می‌کند. هم‌چنین در فاز تشخیص غیرمحلی، گره‌های u و v می‌توانند وجود گره تکراری با شناسه w را تشخیص دهند. هر چه تعداد تونل‌های کرم‌چاله بیش‌تری در شبکه گسترش یابد و یا دشمن تعداد کپی بیش‌تری از گره ضبط‌شده را در شبکه تزریق کند، گره‌های تکراری سریع‌تر شناسایی می‌شوند.

روند انجام مراحل الگوریتم پیشنهادی در شکل (۳) نشان داده شده است.



شکل (۳): فلوچارت الگوریتم پیشنهادی

۵-۳- حالت‌های خاص

حالت اول: دشمن ممکن است گره‌های کپی را طوری برنامه‌ریزی کند که با همدیگر همکاری کنند. به‌این‌ترتیب که اگر در یک دوره زمانی، یک گره کپی u پیغام "Hello" از یک گره کپی دیگر، نظیر u'، دریافت کند، یعنی بیش از یک گره کپی در همسایگی هم قرار گرفته باشند، در این صورت گره کپی u در آن دوره زمانی پیغام "Hello" منتشر نکند. به‌عبارت‌دیگر، گره‌های کپی فقط زمانی که در همسایگی هم قرار نگرفته باشند از خود پیغام "Hello" منتشر کنند. در چنین شرایطی ممکن است گره کپی توسط فاز تشخیص محلی شناسایی نشود. ولی فاز تشخیص غیرمحلی قادر به غلبه بر چنین شرایطی خواهد بود.

حالت دوم: دشمن ممکن است گره‌های کپی را به‌طور ثابت در مکان‌های غیرمجاور مستقر کند و در طول حیات شبکه این گره‌های کپی هرگز حرکت نکنند. در چنین حالتی نیز فاز تشخیص محلی قادر به تشخیص گره‌های کپی نخواهد بود. ولی با راه‌اندازی کانال‌های کرم‌چاله قانونی متحرک، یعنی حالتی که دو گره برقرارکننده کانال کرم‌چاله در محیط شبکه متحرک باشند، می‌توان گره‌های کپی را در چنین شرایطی نیز شناسایی کرد.

۶- ارزیابی روش پیشنهادی

در این بخش ابتدا به ارزیابی کارایی الگوریتم پیشنهادی در قالب سربار حافظه، سربار ارتباطات و سربار محاسباتی، هم‌چنین انرژی مصرفی می‌پردازیم. سپس به ارائه نتایج شبیه‌سازی الگوریتم پیشنهادی در

قالب نرخ تشخیص درست و نرخ تشخیص غلط و هم‌چنین مقایسه نتایج حاصل با دیگر الگوریتم‌ها می‌پردازیم.

۶-۱- ارزیابی کارایی

سربار حافظه: در الگوریتم پیشنهادی هر گره نیاز دارد لیست همسایه‌هایی که در یک دوره زمانی t برای آن پیغام Hello ارسال کرده‌اند را ذخیره کند (لیست همسایگی). پس از هر دوره زمانی t، گره‌ها لیست همسایگی خود را پاک می‌کنند. بنابراین، با فرض این‌که هر گره به‌طور میانگین d همسایه داشته باشد، نیاز به یک فضای ذخیره‌سازی از مرتبه $O(d)$ جهت نگهداری لیست همسایگی در یک دوره زمانی t دارد. البته، گره‌های برپاکننده یک کانال کرم‌چاله نیاز به نگهداری موقت جدول همسایگی همدیگر دارند. ازاین‌رو، هر گره برپاکننده کانال کرم‌چاله نیاز به یک فضای حافظه $2d$ دارد. بنابراین، سربار حافظه تحمیلی به گره‌های برپاکننده کانال‌های کرم‌چاله نیز از مرتبه $O(d)$ می‌باشد. جدول (۱)، سربار حافظه الگوریتم پیشنهادی و دیگر الگوریتم‌های مطرح‌شده را نشان می‌دهد. در جدول (۱)، n تعداد کل گره‌ها در شبکه می‌باشد.

سربار ارتباطات: با توجه به محدودیت‌های انرژی گره‌های حسگر، میزان انرژی مصرفی الگوریتم‌های ارائه‌شده برای شبکه‌های حسگر یک موضوع مهم است. ازآنجاکه عمل ارسال بسته‌ها نسبت به عمل پردازش بسته‌ها و دریافت بسته‌ها انرژی خیلی بیش‌تری مصرف می‌کند، محاسبه تعداد بسته‌های ارسالی که به دلیل استفاده از یک الگوریتم خاص به شبکه تحمیل می‌شود (یا همان سربار ارتباطات)، یک معیار مهم جهت ارزیابی کارایی الگوریتم مطرح برای شبکه‌های حسگر است. در الگوریتم پیشنهادی، هر گره (به‌جز گره‌های برپاکننده کانال‌های کرم‌چاله) در هر دوره زمانی t، یک پیغام "Hello" به همسایه‌هایش منتشر می‌کند. هم‌چنین، در پایان هر دوره زمانی t، هر گره برپاکننده کانال کرم‌چاله، لیست همسایگی خود را در یک بسته نهاده و آن را برای گره دیگر سر کانال کرم‌چاله ارسال می‌کند. بنابراین، الگوریتم پیشنهادی در هر دوره زمانی t، فقط یک عمل ارسال به هر گره تحمیل می‌کند. لذا سربار ارتباطات کل گره‌های شبکه در یک دوره زمانی t، از مرتبه $O(n)$ است. البته باید توجه شود این میزان سربار ارتباطی تحمیلی به گره‌های غیر از برپاکننده کانال‌های کرم‌چاله، صرفاً به خاطر عمل ارسال پیغام‌های "Hello" است که این عمل (یعنی ارسال پریودیک پیغام "Hello" توسط گره‌ها) معمولاً در شبکه‌های حسگر بی‌سیم متحرک لازم است (فارغ از وجود الگوریتم پیشنهادی). یعنی اگر ارسال پریودیک پیغام‌های "Hello" توسط گره‌ها را برای شبکه‌های حسگر متحرک ضروری بدانیم، در این صورت سربار ارتباطات الگوریتم پیشنهادی در هر دوره زمانی t، فقط مربوط به گره‌های برپاکننده کانال‌های کرم‌چاله، برابر $(2\times W)$ و از مرتبه $O(W)$ می‌شود. بنابراین الگوریتم پیشنهادی از نظر سربار ارتباطات، در مقایسه با دیگر الگوریتم‌های مطرح‌شده، عملکرد خوبی خواهد داشت.

جدول (۱)، میزان سربار ارتباطات الگوریتم پیشنهادی و دیگر الگوریتم‌ها را نشان می‌دهد.

جدول (۱): مقایسه سربار حافظه و ارتباطات الگوریتم پیشنهادی با دیگر الگوریتم‌ها

الگوریتم	سربار حافظه	سربار ارتباطات
LSM [7]	$O(\sqrt{n})$	$O(n\sqrt{n})$
SET [8]	$O(\frac{n}{T})$	$O(n)$
P-MPC, SDC [9]	$O(w)$	$O(r\sqrt{n})+O(s)$
RED [10]	$O(d)$	$O(n\sqrt{n})$
RAWL**Error! Reference source not found.**	$O(\log n\times\sqrt{n})$	$O(\log n\times\sqrt{n})$
XED [14]	$O(4\times d\times E[X])$	$O(1)$
SPRT [15]	$O(n\sqrt{n})$	$O(n)$
EDD, SEDD [16]	$O(1)/O(n)$	$O(n)$
Algorithm [18]	$O(d)$	$O(n\times\log n)$
TDD, SDD [23]	$O(n)$	$O(\sqrt{n}), O(d)$
الگوریتم پیشنهادی	$O(d)$	$O(W)$

سربار محاسباتی: در الگوریتم پیشنهادی، در پایان هر دوره زمانی t، هر گره نیاز دارد لیست همسایگی خود را در مرتبه زمانی $O(d)$ پیمایش کرده و گره همسایه‌ای که بیش از یک بار پیغام "Hello" ارسال کرده باشد را به‌عنوان گره تکراری علامت زند.

۶-۲- نتایج شبیه‌سازی‌ها

به‌منظور ارزیابی کارایی الگوریتم پیشنهادی، تعدادی آزمایش انجام گرفته، نتایج حاصل با نتایج به‌دست‌آمده از الگوریتم‌های ارائه‌شده در [۷، ۱۰، ۱۴، ۱۵ و ۱۹] مقایسه شده است. معیارهای مورد ارزیابی، احتمال تشخیص و سرعت تشخیص است.

احتمال تشخیص (P_s): این معیار به‌صورت زیر محاسبه می‌شود [۱۲]:

$$P_s=\frac{\#\text{successful detection times}}{\#\text{repeat times}}$$

که برابر است با تعداد اجراهای منجر به تشخیص موفق بر تعداد کل اجراها، به‌طوری‌که در هر اجرا R دور الگوریتم تشخیص گره‌های کپی تکرار شود.

سرعت تشخیص (E_m): این معیار تعداد دورهای مورد انتظار از اجرای الگوریتم (یا تعداد حرکت گره‌ها) جهت شناسایی گره‌های کپی است.

برای شبیه‌سازی محیط شبکه از نرم‌افزار شبیه‌ساز JSIM [25] استفاده شده است. در اجرای شبیه‌سازی‌ها فرض می‌شود شبکه حاوی

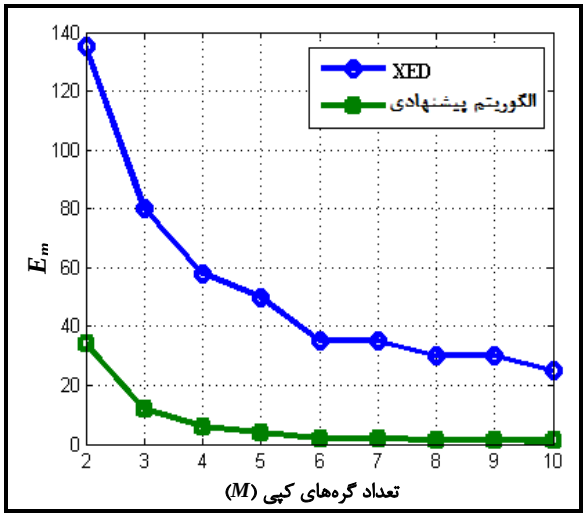
n گره حسگر است که به‌طور تصادفی در یک ناحیه دوبعدی ۲۵۰×۲۵۰ مترمربع پراکنده شده‌اند. محیط شبکه حاوی W کانال کرم‌چاله قانونی و M گره تکراری است که به‌طور تصادفی پراکنده می‌شوند. گره‌های نرمال و تکراری در محیط عملیاتی متحرک می‌باشند. ما از مدل حرکت در نظر گرفته‌شده در [۱۴] جهت حرکت گره‌ها در محیط عملیاتی استفاده می‌کنیم. در این آزمایش‌ها کانال‌های کرم‌چاله به‌طور ثابت در محیط عملیاتی در نظر گرفته شده‌اند (مطابق جدول ۲). میانگین تعداد همسایه‌های هر گره یا به‌عبارت‌دیگر درجه هر گره d است. به‌منظور اطمینان از اعتبار نتایج، هر شبیه‌سازی ۵۰۰ بار تکرار شده و نتیجه نهایی از میانگین نتایج این ۵۰۰ تکرار به‌دست‌آمده است.

آزمایش ۱: هدف این آزمایش، ارزیابی الگوریتم پیشنهادی از نظر سرعت تشخیص گره‌های تکراری است. در این آزمایش، n=۱۰۰۰، d=۱۰، W=۳ و تعداد گره‌های تکراری، یعنی M را از ۲ تا ۱۰ تغییر داده، تعداد دورهایی که نیاز است الگوریتم پیشنهادی و الگوریتم XED [۱۴] اجرا شوند تا گره‌های کپی شناسایی شود را ارزیابی نموده‌ایم. شکل (۵) نتایج حاصل از این آزمایش را نشان می‌دهد. همان‌طور که از نتایج این آزمایش مشخص است، زمانی که تعداد گره‌های کپی M=۲ باشد، الگوریتم XED جهت شناسایی گره کپی تقریباً به ۱۳۵ جابه‌جایی یا حرکت گره‌ها نیاز دارد. درحالی‌که الگوریتم پیشنهادی تقریباً به ۳۴ حرکت یا جابه‌جایی گره‌ها نیاز دارد تا گره کپی را شناسایی کند. به همین ترتیب زمانی که تعداد گره‌های کپی برابر ۵ و ۱۰ باشد، الگوریتم XED به ترتیب به ۵۰ و ۲۵ مرتبه حرکت گره‌ها و الگوریتم پیشنهادی به ترتیب به ۴ و ۱/۱۵ حرکت گره‌ها جهت شناسایی گره کپی دارند. نتیجه این آزمایش نشان می‌دهد الگوریتم پیشنهادی سریع‌تر از الگوریتم XED گره‌های کپی را شناسایی می‌کند.

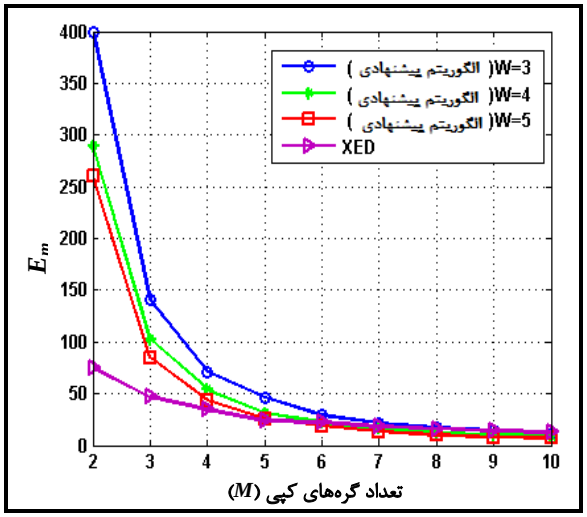
آزمایش ۲: هدف این آزمایش بررسی قدرت کانال‌های کرم‌چاله قانونی در تشخیص گره‌های کپی است. در این آزمایش، فقط فاز تشخیص غیرمحلی الگوریتم پیشنهادی، یعنی کانال‌های کرم‌چاله قانونی در شناسایی گره‌های کپی استفاده می‌شود و فاز تشخیص محلی فعال نیست. در این آزمایش n=۱۰۰۰، d=۲۰، M=۲، ۳، ... ۱۰ و تعداد کانال‌های کرم‌چاله قانونی را از ۳ تا ۵ تغییر داده، تاثیر آن بر سرعت تشخیص گره‌های کپی را ارزیابی نموده‌ایم. نتایج به‌دست‌آمده با نتایج حاصل از الگوریتم XED مقایسه شده است. شکل (۵) نتیجه این آزمایش را نشان می‌دهد. همان‌طور که نتیجه این آزمایش نشان می‌دهد، با افزایش تعداد کانال‌های کرم‌چاله، W، سرعت تشخیص الگوریتم پیشنهادی نیز افزایش می‌یابد. چراکه با افزایش تعداد این کانال‌های کرم‌چاله، نواحی بیش‌تری از محیط عملیاتی تحت نظارت گره‌های برپاکننده کانال‌های کرم‌چاله قرار می‌گیرد و این سبب می‌شود گره‌های کپی سریع‌تر شناسایی شوند. هم‌چنین، نتایج این آزمایش نشان می‌دهد سرعت تشخیص گره‌های کپی در الگوریتم XED به ازای $M \le 5$ بهتر از فاز دوم تشخیص الگوریتم پیشنهادی است ولی به ازای $M > 5$ کانال‌های کرم‌چاله سریع‌تر از الگوریتم XED گره‌های کپی را شناسایی می‌کنند.

آزمایش ۳: در این آزمایش به ارزیابی الگوریتم پیشنهادی از نظر معیار احتمال تشخیص، P_s، می‌پردازیم. در این آزمایش، پارامترها به‌صورت n = ۱۰۰۰، d =۳۰ و M=۱۰ تنظیم شده، معیار P_s برای دورهای ۲ تا ۲۰ اجرای الگوریتم پیشنهادی، LSM [7] و RED [۱۰] (c=0.5) ارزیابی گردیده است. شکل (۶) نتایج به‌دست آمده از این آزمایش را نشان می‌دهد. در این آزمایش نیز فقط از فاز دوم تشخیص الگوریتم پیشنهادی جهت شناسایی گره‌های کپی استفاده شده است. همان‌طور که از نتیجه این آزمایش مشخص است، احتمال تشخیص در الگوریتم پیشنهادی زمانی که W=۳ باشد بالاتر از الگوریتم LSM و پایین‌تر از الگوریتم RED است و زمانی که W=۵ باشد برای R>۱۰ همانند الگوریتم RED احتمال تشخیص گره‌های کپی ۱۰۰٪ خواهد شد. البته باید توجه شود که الگوریتم‌های LSM و RED جهت شناسایی گره‌های کپی در شبکه‌های حسگر ثابت مطرح شده‌اند. نتیجه این آزمایش عملکرد مطلوب الگوریتم پیشنهادی در تشخیص گره‌های کپی را نشان می‌دهد.

آزمایش ۴: در این آزمایش نیز به مقایسه الگوریتم پیشنهادی با الگوریتم ارائه شده در [18] در قالب معیار احتمال تشخیص، P_s، پرداخته می‌شود. در این آزمایش، پارامترهای n=۲۵۰، d=۱۲ و R=۱۰ تنظیم‌شده و نرخ معیار P_s به ازای M=۲، ۳، ... ۱۰ ارزیابی شده است. شکل (۷) نتایج حاصل از این آزمایش را نشان می‌دهد. در این آزمایش، یک‌بار فاز اول و دوم تشخیص الگوریتم پیشنهادی به ازای W=۳، یک‌بار فاز دوم تشخیص الگوریتم پیشنهادی به ازای W=۳ و یک‌بار دیگر فاز دوم تشخیص الگوریتم پشنهادی را به ازای W=۵ ارزیابی می‌کنیم. هم‌چنین، الگوریتم [18] با پارامترهای $V_{\max}=3, V_{\min}=1, t_{pause}=20, Threshold=4\times T(N)$ تنظیم شده است. نتیجه آزمایش نشان می‌دهد کارآیی الگوریتم پیشنهادی زمانی‌که هر دو فاز تشخیص فعال باشند بهتر از الگوریتم [18] و زمانی‌که فقط فاز دوم تشخیص فعال باشد به ازای W =۵ و M>۶ نرخ معیار P_s همانند الگوریتم [۱۸] می‌باشد. نتیجه این آزمایش، عملکرد مطلوب الگوریتم پیشنهادی در مقایسه با الگوریتم مطرح شده در [۱۸] را نشان می‌دهد.

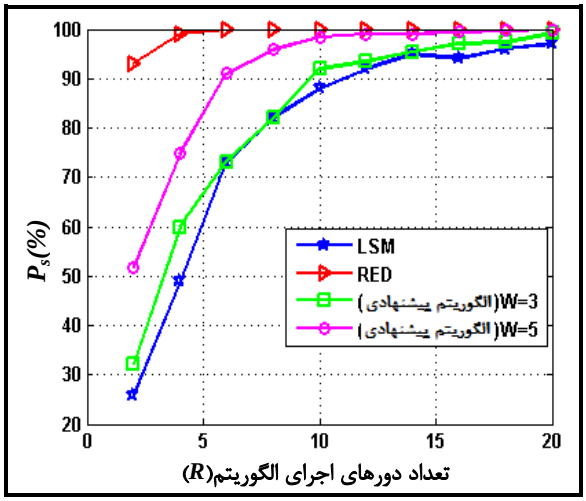


شکل (۴): مقایسه سرعت تشخیص گره‌های کپی در الگوریتم پیشنهادی و XED

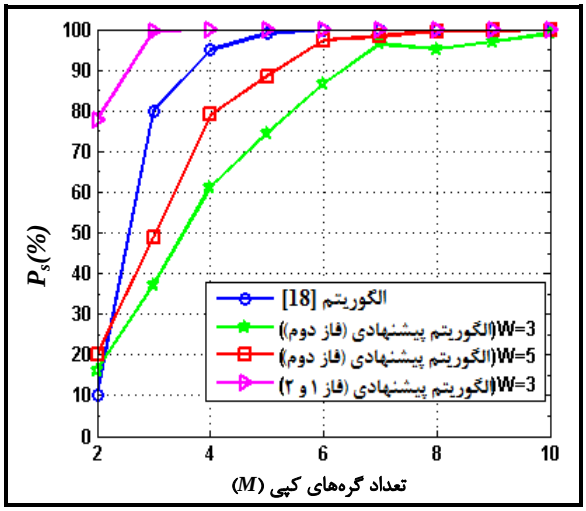


شکل (۵): تاثیر پارامتر W بر سرعت تشخیص گره‌های کپی در الگوریتم پیشنهادی و مقایسه نتایج با الگوریتم XED

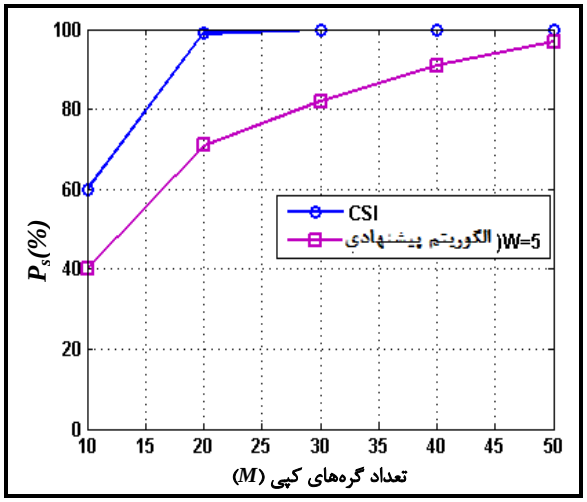
آزمایش ۵: این آزمایش نیز به مقایسه الگوریتم پیشنهادی با الگوریتم CSI از نظر معیار احتمال تشخیص، P_s، می‌پردازد. در این آزمایش، فقط حالتی که ۲ گره کپی (یعنی $M=2$) در شبکه وجود داشته باشد مورد ارزیابی قرار می‌گیرد. باید توجه شود که هرچه تعداد گره‌های کپی در شبکه کم‌تر باشد گرچه دشمن تاثیر کم‌تری بر شبکه می‌گذارد ولی تشخیص این گره‌های کپی توسط الگوریتم‌های امنیتی مشکل‌تر خواهد بود. از این‌رو، با این آزمایش، کارایی الگوریتم پیشنهادی خود را برای چنین حالتی مورد ارزیابی قرار می‌دهیم. در این آزمایش، پارامترها به‌صورت $n=1000$، $d=20$، $W=5$ و $M=2$ تنظیم شده، نرخ معیار P_s برای دورهای ۱۰ تا ۵۰ اجرای الگوریتم پیشنهادی و الگوریتم CSI ارزیابی گردیده، نتایج حاصل در شکل (۶) آمده است. در این آزمایش، فاز اول و دوم تشخیص الگوریتم پیشنهادی فعال است و الگوریتم CSI با پارامتر $\alpha=1$ تنظیم شده است. همان‌طور که از نتیجه آزمایش مشخص است بعد از ۲۰، ۳۰، ۴۰ و ۵۰ دور اجرای الگوریتم پیشنهادی، احتمال تشخیص به ترتیب ۷۰٪، ۸۲٪، ۹۱٪ و ۹۸٪ خواهد بود درحالی‌که نرخ این معیار در الگوریتم CSI بالاتر از الگوریتم پیشنهادی است. البته الگوریتم CSI گره‌های کپی در شبکه‌های حسگر ثابت را شناسایی می‌کند درحالی‌که الگوریتم پیشنهادی گره‌های کپی در شبکه‌های حسگر متحرک را شناسایی می‌کند.



شکل (۶) مقایسه احتمال تشخیص فاز دوم الگوریتم پیشنهادی با الگوریتم‌های LSM و RED



شکل (۷): مقایسه احتمال تشخیص الگوریتم پیشنهادی با الگوریتم مطرح‌شده در [۱۸]



شکل (۸): مقایسه الگوریتم پیشنهادی به الگوریتم CSI از نظر معیار احتمال تشخیص برای حالتی که ۲ =M باشد.

۷- نتیجه‌گیری

در این مقاله یک الگوریتم جدید مبتنی بر اطلاعات محلی و استفاده از لینک‌های کرم‌چاله قانونی جهت شناسایی گره‌های کپی در شبکه‌های حسگر بی‌سیم متحرک پیشنهاد گردید. الگوریتم پیشنهادی از دو فاز تشخیص محلی و تشخیص غیرمحلی تشکیل شده است. در فاز تشخیص محلی، هر گره به‌طور مستقل با توجه به پیغام‌های "Hello" منتشرشده، گره‌های کپی موجود در همسایگی خود را شناسایی می‌کند. در فاز تشخیص غیرمحلی، گره‌های برپاکننده لینک‌های کرم‌چاله قانونی با توجه به انتشار پیغام‌های "Hello" اقدام به شناسایی گره‌های کپی می‌کنند. الگوریتم پیشنهادی نیاز به تعیین مکان گره‌ها، انتشار پیغام‌های ادعای مکانی، کلیدهای عمومی (و امضای دیجیتال) و فرایندهای پیچیده تشخیص گره‌های کپی ندارد. کارایی الگوریتم پیشنهادی ازنقطه‌نظرهای سربار حافظه و سربار ارتباطات ارزیابی و با دیگر الگوریتم‌های موجود مقایسه شده است. هم‌چنین، الگوریتم پیشنهادی شبیه‌سازی‌شده، نتایج شبیه‌سازی‌ها در قالب معیارهای نرخ تشخیص و سرعت تشخیص با الگوریتم‌های مطرح در [۷، ۱۰، ۱۴، ۱۵ و ۱۹] مقایسه گردید که نتایج این شبیه‌سازی‌ها عملکرد مطلوب الگوریتم پیشنهادی را نشان می‌دهد.

مراجع

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayircl, "A survey on sensor networks," in: Proceedings of the IEEE Communication Magazine, Vol. 40, pp. 102-114, August 2002.

[2] F. Akyildiz Ian and H. Kasimoglu Ismail, "Wireless sensor and actor networks: research challenges," in: Proceedings of the Ad Hoc Networks 2, pp. 351–367, 2004.

[3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in: Proceedings of the AdHoc Networks, pp. 299-302, 2003.

[4] J. P. Walters, Z. Liang, W. Shi and V. Chaudhary, "Wireless sensor network security: a survey," in: Proceedings of the Security in Distributed, Grid and Pervasive Computing, Yang Xiao (Eds), 2006.

[5] G. Padmavathi and D. shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks,", in: Proceedings of the International Journal of Computer Science and Information Security (IJCSIS), Vol. 4, No. 1-2, August 2009.

[6] B. Parno, A. Perrig and V. D. Gligor, "Distributed detection of node replication attacks in sensor networks," in: Proceedings of the IEEE Symposium on Security and Privacy, 2005.

[7] H. Choi, S. Zhu and T. F. Porta, "SET: detecting node clones in sensor networks," in: Proceedings of the Secure Comm '07, pp. 341–350, 2007.

[8] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia and S. Roy, "efficient distributed detection of node replication attacks in sensor networks," in: Proceedings of the Annual Computer Security Applications Conference (ACSAC), December 2007.

[9] M. Conti, R. D. Pietro and L. V. Mancini, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," In: Proceedings of the ACM MobiHoc, September 2007.

[10] M. Conti, R. D. Pietro, L. V. Mancini and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," in: Proceedings of the IEEE Transactions on Dependable and Secure Computing, 2010.

[11] C. Kim, C. Park, J. Hur, H. Lee and H. Yoon, "A distributed deterministic and resilient replication attack detection protocol in wireless sensor networks," in: Proceedings of the Communications in Computer and Information Science, Vol. 56, pp. 405-412, 2009.

[12] Y. Zeng, J. Cao, S. Zhang, S. Guo and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, Vol. 28, No. 5, 2010

[13] C.-M. Yu, C.-S. Lu and S.-Y. Kuo, "CSI: compressed sensing-based clone identification in sensor networks," in: Proceedings of the 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing, March 2012.

[14] C.-M. Yu, C.-S. Lu and S.-Y. Kuo, "Mobile sensor network resilient against node replication attacks," In: Proceedings of the IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), June 2008.

[15] D. Unnikrishnan, "Detecting mobile replica node attacks in wireless sensor networks using sequential probability ratio test," in: Proceedings of the 13th International Conference on Distributed Computing and Networking (ICDCN), Hong Kong, China, January 3-6, 2012.

[16] C.-M. Yu, C.-S. Lu and S.-Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," In: Proceedings of the IEEE Vehicular Technology Conference Fall (VTC Fall), September 2009.

[17] B. Gowtham and S. Sharmila, "location traced hybrid detection of node replication attack in mobile wireless sensor network," in: Proceedings of the Special Issue of International Journal of Computer Applications (0975 – 8887) on Information Processing and Remote Computing – IPRC, August 2012.

[18] X. Deng and Y. Xiong, "A new protocol for the detection of node replication attacks in mobile wireless sensor networks," In: Proceedings of the Journal of Computer

Science and Technology, Vol. 26, No. 4, pp. 732-743, July 2011.
[19] L. Yanxiang, Z. Yong and L. Shengli, "single hop detection of node clone attacks in mobile wireless sensor networks," in: Proceedings of the International Workshop on Information and Electronics Engineering (IWIEE), Vol. 29, pp. 2798–2803, 2012.
[20] J.-W. Ho, M. Wright and S. Das, "fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing," in: Proceedings of the IEEE Transactions on Mobile Computing, Vol. 10, No. 6, June 2011.
[21] W. T. Zhu, J. Zhou, R. Deng and F. Bao, "Detecting node replication attacks in mobile sensor networks: theory and approaches," in: Proceedings of the Security and Communication Networks Vol. 5, No. 5, pp. 496–507, May 2012.
[22] M. Conti, R. D. Pietro and A. Spognardi, "wireless sensor replica detection in mobile environments," Proceedings of the ICDCN, pp. 249-264, 2012.
[23] K. Xing and X. Cheng, "From time domain to space domain: detecting replica attacks in mobile ad hoc networks," Proceedings of the IEEE INFOCOM, 2010.
[24] S. Ratnasamy, B. Karp, L. Yin and F. Yu, "GHT: A geographic hash table for data-centric storage," in: Proceedings of the First ACM International Workshop on Wireless Sensor Networks and Applications (WSNA), pp. 78–87, 2002.
[25] JSIM Simulator, http://www.j-sim.org.

زیرنویس‌ها

1 Node replication attack
2 Keying materials
3 Sequential Probability Ratio Test
4 Wormhole
5 Node-To-Network Broadcasting
6 Deterministic Multicast
7 Randomized Multicast
8 Line-Selected Multicast
9 Witness nodes
10 Single Deterministic Cell
11 Parallel Multiple Probabilistic Cells
12 Localized Multicast
13 Resilient
14 Random WaLk
15 Table-assisted Random WaLk
16 Trace table
17 Compressed sensing
18 Compressed Sensing-Based Clone Identification
19 Descendant nodes
20 Efficient and Distributed Detection
21 Pairwise key
22 Single Hop Detection
23 Eavesdropping
24 Broadcast
25 Omni-directional