تشخیص توزیع‌شده و مشارکتی حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم

یاسر عظیمی [۱]، دانشجوی کارشناسی ارشد، وحید هاشمی‌فرد[۲]، دانشجوی کارشناسی ارشد، جمشید باقرزاده[۳]، استادیار

۱- دانشکده فنی و مهندسی - دانشگاه ارومیه - ارومیه - ایران - azimiyaser@yahoo.com
۲- دانشکده فنی و مهندسی - دانشگاه ارومیه - ارومیه - ایران - v.hashemifard@gmail.com
۳- دانشکده فنی و مهندسی - دانشگاه ارومیه - ارومیه - ایران - j.bagherzadeh@urmia.ac.ir

چکیده: شبکه‌های حسگر بی‌سیم از چندین گره کوچک بنام حسگر تشکیل می‌شوند. این گره‌ها باهم در ارتباط بوده و در راستای انجام‌وظیفه یا وظایفی با همدیگر همکاری می‌کنند. حملات مختلفی وجود دارند که می‌توانند این شبکه‌ها را تهدید کنند. حمله کرم‌چاله از حملاتی است که در لایه شبکه باعث اختلال در پروتکل‌های مسیریابی می‌شود. در حمله کرم‌چاله، بسته‌های یک منطقه از شبکه از طریق لینک سریع و خارج از باند، به منطقه دیگری از شبکه منتقل شده و بازپخش می‌شوند. این عمل باعث می‌شود گره‌هایی که ازنظر فیزیکی در همسایگی هم قرار ندارند، به‌طور ناخودآگاه یکدیگر را به‌عنوان همسایه شناسایی کنند. برای مقابله با این حمله، روش‌های متنوعی ارائه شده‌اند که برخی از آن‌ها به سخت‌افزار یا پیش‌فرض‌های خاصی نیاز دارند. روش پیشنهادی در این تحقیق، یک روش توزیع‌شده است که از اطلاعات همسایگی استفاده می‌کند و نیاز به سخت‌افزار خاصی ندارد. ایده اصلی مقاله حاضر برای یافتن گره‌های همسایه واقعی، استفاده از لیست همسایگی گره‌های همسایه‌ای است که همزمان با گره جاری تحت حمله قرار ندارند. به‌عبارتی‌دیگر، در روش پیشنهادی گره تحت حمله به کمک گره‌های همسایه‌ای که خارج از محدوده حمله‌کننده هستند، گره‌های انتقالی از طریق کرم‌چاله را شناسایی می‌کند.

واژه‌هاي كليدي: شبکه‌های حسگر بی‌سیم، لیست همسایگی، کرم‌چاله، گره، حمله.

Distributed and Collaborative Detection of Wormhole Attack in Wireless Sensor Networks

Y. Azimi, MSc. Student[1], V. Hashemifard, MSc. Student[2], J. Bagherzadeh, assistant professor [3]

1- Faculty of Engineering, University of Urmia, Urmia, Iran, Email: azimiyaser@yahoo.com
2- Faculty of Engineering, University of Urmia, Urmia, Iran, Email: v.hashemifard@gmail.com
3- Faculty of Engineering, University of Urmia, Urmia, Iran, Email: j.bagherzadeh@urmia.ac.ir

Abstract: Wireless sensor networks are made from some small nodes called sensors. These nodes communicate and calibrate for some doing tasks. Various attacks can threat these networks. A wormhole attack is an attack that targets network layer and causes disorder in routing protocols. In the wormhole attack, packets of an area in the network transmit to other area through high-speed and out-of-band links. This causes nodes that are not in each other's transmission range detect each other as neighbors unconsciously. To deal with this attack, various methods are proposed that may require hardware or special defaults. Our proposed method is a distributed one, which uses neighborhood data and requires no special hardware. Our main idea is to use neighborhood list of each legal neighbor node (which is not attacked) to be aware of real neighbor nodes. In the other words, the proposed method identifies transporting nodes in association with its neighbor nodes.

Keywords: Wireless sensor networks, neighborhood list, wormhole, node, attack.

تاریخ ارسال مقاله: ۹۳/۰۹/۱۹
تاریخ اصلاح مقاله: ۹۳/۱۰/۱۶ و ۹۳/۱۱/۲۳ و ۹۴/۱۱/۲۳
تاریخ پذیرش مقاله: ۱۳۹۵/۲/۹
نام نویسنده مسئول: جمشید باقرزاده
نشانی نویسنده مسئول: ایران - ارومیه – ۱۵کیلومتری جاده سرو - دانشگاه ارومیه - دانشکده فنی و مهندسی

۱- مقدمه

شبکه‌های حسگر بی‌سیم یک تکنولوژی در حال پیشرفت است که پتانسیل فراهم کردن زیرساخت‌های قابل‌انعطاف برای کاربردهای نظامی و غیرنظامی ازجمله بهداشت و درمان، صنعت، نظارت و مدیریت و ... را دارا است [۱].

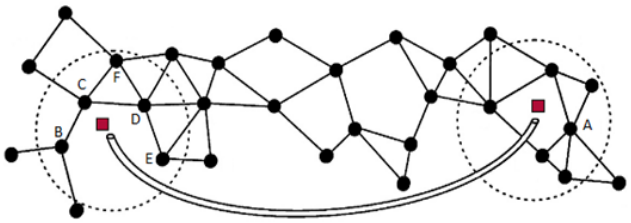
این شبکه‌ها شامل مجموعه‌ای از دستگاه‌های ارزان با قابلیت‌های پردازشی نسبتاً کم (گره‌های حسگر [۲]) می‌باشند که قابلیت‌های محاسباتی، میزان انرژی، میزان حافظه و توان رادیویی محدودی دارند [۶-۳]. در اکثر کاربردهای شبکه‌های حسگر بی‌سیم لازم است تعداد زیادی از گره‌ها بدون نیاز به مراقبت، با همدیگر همکاری کنند و یا با ایستگاه پایه تعامل داشته باشند. بازه ارسالی گره‌های حسگر محدود است. لذا گره‌ها باید بسته‌های ارسالی به ایستگاه پایه را از طریق سایر گره‌های شبکه بفرستند. بنابراین، هر گره در شبکه حسگر بی‌سیم هم به‌عنوان حسگر و هم به‌عنوان روتر عمل می‌کند.

اطلاعات همسایگی به‌وسیله اکثر پروتکل‌های شبکه و الگوریتم‌ها استفاده شده و در لیست همسایگی نگه‌داری می‌شوند. در فرآیند شناسایی همسایه‌ها که منجر به تولید لیست همسایگی برای گره می‌شود، هر گرهی سایر گره‌هایی که در محدوده ارسالش قرار دارند (گره‌هایی که از آن‌ها بسته HELLO دریافت کنند) را در لیست همسایگی خود وارد می‌کند. در حمله کرم‌چاله دو گره همکار حمله‌کننده، در دو موقعیت جغرافیایی متفاوت و معمولاً دور از هم مستقر شده و بسته‌های ارسالی گره‌های منطقه مجاور خود را از طریق لینک پرسرعت و خارج از باند، به گره همکار ارسال می‌نمایند و گره مقصد به‌محض دریافت بسته‌ها آن را بازپخش می‌نماید. بدین ترتیب درصورتی‌که حمله کرم‌چاله رخ داده باشد، بسته‌های HELLO ارسالی یک منطقه از شبکه توسط حمله‌کننده در منطقه دیگری از شبکه بازپخش خواهد شد [۷].

همان‌طور که در شکل ۱ نشان داده شده است، گره A در اثر حمله کرم‌چاله، با گره‌های B، C، D و E همسایه خواهد شد. زیرا A بسته‌های ارسالی B، C، D و E را از طریق کرم‌چاله می‌شنود، ولی متوجه نمی‌شود که به‌صورت فیزیکی با آن‌ها همسایه نیست و این همسایگی ناشی از وجود حمله کرم‌چاله است.

ازآنجایی‌که پروتکل مسیریابی استخوان‌بندی شبکه را تشکیل می‌دهد، نمی‌تواند بدون دید صحیح از لیست همسایگی به‌درستی عمل کند. لذا ما در این مقاله روی تعداد همسایه‌های گره‌ها تمرکز داریم. وقتی حمله کرم‌چاله در شبکه رخ دهد، تعداد همسایه‌های گره‌های در معرض حمله بیش‌ازحد معمول خواهد شد. بنابراین ما از این ایده استفاده کرده و به‌صورت توزیع‌شده، همسایه‌های واقعی گره‌هایی که تحت حمله قرار گرفته‌اند را شناسایی کرده و گره‌های دیگر را به‌عنوان گره مشکوک در نظر گرفته و از لیست همسایگی حذف می‌کنیم.

ادامه مقاله به این صورت است: در بخش ۲ کارهای قبلی برای مقابله با حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم آورده شده است. در بخش ۳ روش پیشنهادی همراه با جزئیات مطرح شده است. در بخش ۴ نتایج شبیه‌سازی‌های روش پیشنهادی و مقایسه روش پیشنهادی با سایر روش‌ها آورده شده و نهایتاً نتیجه‌گیری در بخش ۵ ارائه شده است.



شکل ۱: تأثیر حمله‌کرم‌چاله در تغییر لیست همسایگی گره‌ها. دو گره به شکل مربع حمله‌کننده‌ها و سایر گره‌های به شکل دایره، گره‌های نرمال در شبکه هستند [۸]

۲- کارهای پیشین

در سال‌های اخیر امنیت در شبکه‌های حسگر بی‌سیم موردتوجه بیش‌تری قرار گرفته است [۹]. مطالعات زیادی روی این شبکه‌ها در حال انجام است. حمله کرم‌چاله یک حمله بیرونی معروف در شبکه‌های حسگر بی‌سیم است [۶]. متدهای مختلفی برای مقابله با حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم وجود دارد که برخی از این روش‌ها در ادامه آورده شده‌اند.

مکانیسم‌های رمزنگاری در شبکه‌های حسگر بی‌سیم علیرغم شناسایی و جلوگیری از انواع مختلفی از حملات موجود در این نوع شبکه‌ها، برای شناسایی یا مقابله با حمله کرم‌چاله قابل استفاده نیستند. در حمله کرم‌چاله بسته‌ها به همان شکلی که ارسال شوند، دریافت شده و در منطقه دیگری از شبکه بازپخش می‌شوند و در محتوای بسته‌ها تغییری توسط حمله‌کننده‌ها اعمال نمی‌شود. بنابراین برای شناسایی این حمله‌ها باید روش‌های دیگری غیر از رمزنگاری ارائه شوند.

روش‌های مختلفی تاکنون برای مقابله با حمله کرم‌چاله ارائه شده‌اند که می‌توان در چهار دسته طبقه‌بندی کرد: ۱- متمرکز، ۲- غیرمتمرکز، ۳- مبتنی بر سخت‌افزارهای اضافی ۴- مبتنی بر اطلاعات همسایگی.

۲-۱- روش‌های متمرکز

در روش‌های متمرکز، یک موجودیت مرکزی اطلاعات همسایگی‌ها را از گره‌ها به‌صورت محلی جمع‌آوری کرده، پردازش نموده و مدل کل شبکه را ایجاد می‌کند. سپس با استفاده از مدل ایجادشده شبکه، سعی می‌کند بر اساس ناسازگاری‌هایی که در شبکه تولید شده، وجود کرم‌چاله را شناسایی نماید.

در [۱۰] دو مکانیسم پیشنهاد شده است که در آن گره‌ها فقط لیست همسایه‌های قابل‌اطمینان خود را به موجودیت مرکزی

می‌فرستند. مکانیسم اول افزایش تراکم شبکه را شناسایی می‌کند و دومین مکانیسم، کاهش کوتاه‌ترین مسیر بین دو گره تحت حمله را شناسایی می‌کند. ایده این مکانیسم‌ها این است که حمله کرم‌چاله، درجه رأس‌ها را در گراف همسایگی شبکه، به دلیل ایجاد همسایگی‌های جدید افزایش می‌دهد.

در [۱۱] نویسندگان یک راهکار بصری برای تشخیص کرم‌چاله در شبکه‌های حسگر بی‌سیم ارائه کرده‌اند. در این مکانیسم بین همه گره‌های همسایه تخمین مصافت انجام می‌شود. با مقیاس‌بندی چندبعدی شکل مجازی شبکه ساخته شده و در آخر شبکه مجازی حاصل، مورد تحلیل قرار می‌گیرد. اگر کرم‌چاله‌ای وجود داشت، شکل حاصل از شبکه خمیده خواهد بود و در صورت عدم وجود کرم‌چاله، شبکه مسطح خواهد بود.

در [۱۲] یک چارچوب نظریه گراف مبتنی بر تخمین مسافت ارائه شده است. این روش به تعدادی گارد با محدوده ارتباطی بالا نیاز دارد تا مکان گره‌ها را تشخیص دهد. نشان داده شده است که این مکانیسم با احتمال نزدیک به ۱ حمله کرم‌چاله را شناسایی می‌کند. بااین‌حال، کارایی آن به عملکرد درست گره‌های گاردی که می‌توانند مورد هدف اصلی حمله‌کننده‌ها قرار گیرند، بستگی دارد.

۲-۲- روش‌های نامتمرکز

مزیت اصلی روش‌های نامتمرکز، عدم نیاز آن‌ها به وجود موجودیت مرکزی است و درنتیجه می‌توان به‌صورت گسترده از آن‌ها استفاده کرد. هر گره به‌صورت محلی لیست همسایه‌هایش را تولید کرده و بر اساس الگوریتم‌های مناسب، با توجه به معیارهایی مثل زمان یا مکان، شروع به مقابله با حمله می‌کند. این روش‌ها می‌توانند به دودسته تقسیم شوند: روش‌های مبتنی بر فاصله و روش‌های مبتنی بر زمان.

روش‌های نوع اول از تخمین فاصله واقعی استفاده می‌کنند تا مطمئن شوند دورتر از حداکثر فاصله ممکن از هم قرار ندارند. در [۱۳] به هر بسته‌ای یک محدودیت امن (Leash)، مثل برچسب زمانی یا اطلاعات مکانی ضمیمه می‌شود تا مشخص گردد بسته از کجا آمده و چه موقع ارسال شده است. این تکنیک‌ها برای حالتی که از سخت‌افزارهای اضافی برای مکان‌یابی یا همزمانی گره‌ها استفاده شود، به‌خوبی کار می‌کنند.

در [۱۴] نویسندگان روشی مبتنی بر سازگاری فاصله ارائه کردند که در آن از قدرت سیگنال دریافتی استفاده می‌شود تا فاصله به دست آید. عامل قدرت سیگنال دریافتی از عوامل محیطی تأثیر می‌پذیرد.

در [۱۵] روشی بر اساس فاصله ارائه شده است که در آن نیازی به همزمانی یا تعیین مکان وجود ندارد ولی به چالش «درخواست-پاسخ» امن بستگی دارد و نیازمند اندازه‌گیری دقیق زمان است.

در روش‌های مبتنی بر زمان، گره‌ها نیازمند ساعت‌هایی هستند که به‌درستی همزمان شده باشند. برای مثال LiteWorp [۱۶] مبتنی بر شنود کل بسته‌های انتقالی گره‌ها، توسط گره‌های گارد توزیع‌شده در سرتاسر شبکه است. این روش در شبکه‌های پرتراکم عملکرد درستی دارد ولی دارای سربار اضافی گره‌های گارد است.

روش پیشنهادی در [۱۷] مبتنی بر گره‌های گاردی است که در کل شبکه پخش شده‌اند. گاردها ترافیک محلی را کنترل می‌کنند و به ازای هر عمل خصمانه گره‌های همسایه، شمارنده مربوط به آن گره را افزایش می‌دهند. اگر این شمارنده از حد آستانه بیش‌تر شود، گره موردنظر از لیست همسایگی حذف شده و یک پیام هشدار به ازای آن به گره‌های همسایه فرستاده می‌شود و غیرنرمال بودن آن را به همسایه‌ها اطلاع می‌دهد. هر گره که به ازای هرکدام از همسایه‌های خود تعداد پیام‌های هشدار بیش‌ازحد آستانه دریافت کند، آن گره را از لیست همسایگی خود حذف می‌کند.

در [۱۷] از مکانیسم End-to-End برای تشخیص وجود کرم‌چاله استفاده شده است. به‌طوری‌که مبدأ کم‌ترین گام موردنیاز بین خود و مقصد را تخمین می‌زند و آن را با تعداد گام واقعی موقع ارسال بسته مقایسه می‌کند. اگر تعداد گام تخمینی بیش‌تر از تعداد گام‌ها موقع ارسال بسته شد، کرم‌چاله وجود دارد و مبدأ فرآیند ردگیری کرم‌چاله را شروع می‌کند.

۲-۳- روش‌های مبتنی بر سخت‌افزارهای اضافی

برای کنار گذاشتن نیاز به ساعت دقیق، محققان از سخت‌افزارهای مخصوصی استفاده کردند. در [۱۸، ۱۹] استفاده از آنتن‌های جهت‌دار[۲۰، ۲۱] پیشنهاد شدند. هو و همکارانش در [۱۸] مکانیسمی ارائه کردند که در آن از آنتن‌های جهت‌دار برای شناسایی کرم‌چاله استفاده می‌شود. در روش مذکور فرض می‌شود کل گره‌های شبکه دارای آنتن‌های جهت‌دار هستند که آنتن هر گره به ۶ قسمت مساوی تقسیم می‌شود. همچنین فرض می‌شود جهت سگمنت‌های با شماره یکسان در گره‌ها، به یک سمت مشترک قرار دارد. مثلاً جهت قسمت شماره ۱ آنتن در هر گره به سمت شمال باشد.

روش ارائه‌شده در [۲۱] با استفاده از گره‌های خاصی بنام گره‌های گارد وقوع حمله کرم‌چاله را تشخیص می‌دهد. در این روش گره‌های گارد موقعیت همدیگر را می‌دانند و توان ارسالی بالایی دارند. گره‌های گارد با ارسال پیام‌های probe به همدیگر، با توجه به فاصله از هم و تعداد گام انتقال بسته، وجود کرم‌چاله را مشخص می‌کنند.

چنین روش‌هایی کارایی بالایی دارند ولی به دلیل افزایش هزینه و پیچیدگی و استفاده از سخت‌افزارهای مخصوص، نمی‌توان به‌راحتی برای شبکه‌های حسگر بی‌سیم اعمال کرد.

۲-۴- روش‌های مبتنی بر اطلاعات همسایگی

در این روش‌ها، گره‌ها به‌صورت محلی توپولوژی اتصال شبکه را به دست آورده و وجود اطلاعات توپولوژیکی متناقض را شناسایی می‌کنند. ایده این روش‌ها این است که وقوع حمله کرم‌چاله، منجر به تغییرات قابل‌تشخیص در ساختار توپولوژی یا اتصال گراف شبکه می‌شود.

در [۲۲] روشی بر اساس نظارت بر درجه گره در گراف اتصال شبکه ارائه شده است. ایده این روش افزایش تعداد همسایه‌های گره تحت حمله کرم‌چاله به مقداری بیش از یک حد آستانه است. روش مشابهی بنام SWAT در [۲۳] ارائه شده است که بعد از شناسایی حمله کرم‌چاله، گره‌های کرم‌چاله را با محدود کردن لینک‌های متصل به کرم‌چاله، ایزوله کرده و پروتکل مسیریابی را بازسازی می‌کند. در این روش فرض بر آن است که گره‌ها در محیط به‌صورت یکنواخت و با تراکم بالا پخش شده‌اند و لینک‌هایی به شبکه افزوده و یا از آن کاسته نمی‌شود.

LDAC [۸] یک الگوریتم محلی و نامتمرکز برای مقابله با حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم است. ایده اصلی آن جستجوی زیرساختارهای کوچک در گراف اتصال است که نشان می‌دهد حمله‌ای رخ داده است. مزیت این الگوریتم عدم استفاده از سخت‌افزارهای مخصوص، آنتن‌های جهت‌دار و اندازه‌گیری فاصله بین گره‌ها است. همچنین به همزمانی سخت یا متدهای جغرافیایی نیازی ندارد. فقط نیاز است گره‌ها اطلاعات همسایگی خود را نگه‌داری کنند و چون این کار توسط پروتکل مسیریابی انجام می‌شود، LDAC سربار به شبکه تحمیل نمی‌کند.

در LDAC ابتدا شبکه به مدت بسیار کوتاهی امن در نظر گرفته می‌شود تا گره‌ها همسایه‌های «k گامی» خود را شناسایی کنند. فرض می‌شود در این مدت‌زمان کوتاه، حمله‌ای رخ نمی‌دهد. بعد از زمان t، هر گره بسته‌هایی از گره‌های دیگری را شنود می‌کند که ممکن است از طریق کرم‌چاله آمده باشند یا نه. شناسه گره‌های جدید در همسایگی گره، در لیستی بنام v قرار داده می‌شوند.

گره‌ها به ازای هر شناسه موجود در v تست محلی وجود مسیر را از خود به گره‌های v توسط گره‌های غیرمشکوک انجام می‌دهند. مثلاً برای حالت k=۲ کافی است گره جاری و گره v در لیست همسایگی خود یک گره غیرمشکوک مشترک داشته باشند. این مکانیسم یک الگوریتم اقتضایی است و به‌صورت On-Demand اجرا می‌شود.

در روش ارائه‌شده در [۲۴] نیز از تحلیل خوشه‌ای «k میانگین» برای شناسایی حمله کرم‌چاله استفاده شده است که ایده اصلی آن همبستگی فاصله فیزیکی گره‌ها است.

۳- روش پیشنهادی

در شبکه‌های حسگر بی‌سیم وقتی حمله کرم‌چاله رخ دهد، طبیعی است که تعداد همسایه‌های گره از حد معمول بیش‌تر خواهد شد. بنابراین ما از این اطلاعات می‌توانیم استفاده کنیم تا در صورت وقوع حمله‌ی کرم‌چاله، آن را شناسایی کرده و اقدام به مقابله کنیم. در جدول ۱ مجموعه‌ها و گزاره‌های موردنیاز در ادامه مقاله آورده شده‌اند.

۳-۱- مدل شبکه

در مدل ما شبکه حسگر بی‌سیم شامل یک مجموعه از n گره حسگر $S=\{i, j, k, \ldots\}$ است. گره‌های شبکه دارای محدودیت‌هایی از قبیل مقدار انرژی، حافظه ذخیره‌سازی و بازه ارسال و دریافت محدود می‌باشند. در روش پیشنهادی نیازی به سخت‌افزار اضافی نبوده و هیچگونه شروط محدودیتی، مثل همزمانی گره‌ها وجود ندارد. همچنین انرژی گره‌ها در ابتدا برای همه گره‌ها یکسان در نظر می‌شود. همچنین محدوده ارسال و دریافت را برای تمامی گره‌ها یکسان و برابر r فرض می‌شود. بنابراین هر دو گره در محدوده هم، به‌عنوان همسایه همدیگر خواهند بود که در رابطه (۱) به‌صورت منطق مرتبه اول بیان شده است.

$$\forall i, j \in S;\ NB(i,j) \leftrightarrow NB(j,i) \qquad (۱)$$

فرض کنیم گره‌ها به‌صورت تصادفی در محیط پخش شده‌اند. اگر n گره در یک محیط $m \times m$ پخش شوند، تراکم گره‌ها که با d نشان داده شده است، به‌صورت معادله (۲) خواهد شد.

$$d = n / (m \times m) \qquad (۲)$$

جدول ۱: مجموعه‌ها و گزاره‌های منطق مرتبه اول

عبارت	مفهوم
S={i ,j ,k , ...}	مجموعه گره‌های شبکه
M={(x,y), (s,t), ...}	مجموعه جفت حمله‌کننده‌های همکار
InRange(i,j)	j در محدوده ارسال i قرار دارد
NB(i) یا NB$_i$	لیست همسایگی گره i
NB(i,j)	j در لیست همسایگی i قرار دارند
NNB(i,j)	j یک همسایه فیزیکی واقعی برای i است

۳-۲- مدل حمله

کرم‌چاله یک لینک اختصاصی بین دو گره موجود در مکان‌های فیزیکی مجزا است که تحت کنترل حمله‌کننده قرار دارد. حمله‌کننده‌ای را در نظر می‌گیریم که با استفاده از دو گره همکار، به شبکه حمله می‌کند. گره‌های حمله‌کننده را دو سر کرم‌چاله می‌نامیم. بسته‌های دریافتی در یک سر کرم‌چاله، بدون ایجاد هرگونه تغییری در محتوای آن‌ها، از طریق یک لینک پرسرعت و خارج از باند، به گره همکار در انتهای دیگر کرم‌چاله ارسال شده و در مقصد بازپخش می‌شوند. هدف اصلی این حمله فریب دادن گره‌های شبکه است به‌طوری‌که درنتیجه وقوع آن، گره‌های دور از هم، همدیگر را به‌عنوان همسایه می‌پندارند.

با توجه به جدول ۱ مدل حمله را می‌توان طبق رابطه (۳) نوشت.

$$\forall i, j \in S, \forall (x,y) \in M; \\ (InRange(x,i) \wedge InRange(y,j)) \rightarrow NB(i,j) \qquad (۳)$$

همسایه بودن دو گره نیز در منطق مرتبه اول به‌صورت رابطه (۴) است.

$$\forall i, j \in S;\ InRange(i,j) \rightarrow NB(i,j) \qquad (۴)$$

۳-۳- شناسایی توزیع‌شده و مشارکتی گره‌های انتقالی از طریق کرم‌چاله

این روش توزیع‌شده نامیده می‌شود، برای اینکه در هر گره به‌صورت مستقل و بدون نیاز به اطلاعات اضافی از سایرین، خطر وقوع حمله کرم‌چاله تشخیص داده می‌شود. همچنین این روش مشارکتی است، برای اینکه گره موردحمله، به کمک گره‌های همسایه واقعی، گره‌های انتقالی از طریق کرم‌چاله را شناسایی کرده و از لیست همسایگی خود حذف می‌کند.

طبق قسمت ۳-۱، اگر n گره در یک فضای $m\times m$ به‌صورت تصادفی توزیع شوند، تراکم گره‌ها (d) طبق معادله (۲) خواهد بود. از طرفی چون بازه ارسال گره‌ها یکسان و برابر r است، تعداد همسایه‌های مورد انتظار برای هر گره که با $E[N]$ نشان داده شده است، به‌صورت معادله (۵) خواهد بود.

$$E[N]=\pi\times r^2\times d \qquad (۵)$$

در ادامه برای سادگی به‌جای $E[N]$ از N استفاده می‌کنیم. مقدار N به‌صورت پویا در شبکه می‌تواند تغییر کند و توسط ایستگاه پایه به کمک یک پروتکل همه‌پخشی سبک‌وزن مثل µTESLA به اطلاع همه گره‌های شبکه برسد.

برای تشخیص وقوع کرم‌چاله، هر گره به‌صورت محلی تعداد همسایه‌های خود را کنترل می‌کند. اگر تعداد همسایه‌هایش از یک مقدار آستانه بیش‌تر شد، خطر وقوع حمله را حس می‌کند. ما این حد آستانه را به‌صورت رابطه (۶) تعریف می‌کنیم.

$$K=\alpha\times N \quad 1<\alpha<2 \qquad (۶)$$

که در آن K حد آستانه برای شروع فرآیند و N تعداد همسایه‌های مورد انتظار و α یک ضریب است.

وقتی یک گره احساس خطر کند، مطابق با رابطه (۷) وقوع حمله را شناسایی می‌کند که در آن K از رابطه (۶) به دست می‌آید.

$$\forall i\in S;\ |NB(i)|\geq K \rightarrow \exists(x,y)\in M;\ (InRange(x,i)\vee InRange(y,i)) \qquad (۷)$$

برای شناسایی گره‌هایی که از طریق کرم‌چاله منتقل نشده‌اند، کارهای زیر انجام می‌شود:

۱. گره جاری (گره i)، پیام $NBReq$ را به‌صورت رابطه (۸) به همسایه‌های تک‌گامی همه‌پخشی کرده و لیست همسایگی آن‌ها را درخواست می‌نماید.

$$i\rightarrow *: NB\,\mathrm{Req} \qquad (۸)$$

۲. هر گره همسایه (گره j) که پیام قبلی را دریافت کند، با پیام $NBRep$ که شامل لیست همسایگی‌اش است، طبق رابطه (۹) به گره i پاسخ می‌دهد.

$$j\rightarrow i: NB\,\mathrm{Re}p \qquad (۹)$$

۳. گره i، لیست همسایگی خود و لیست دریافتی از هر همسایه‌اش را به‌صورت جداگانه مقایسه می‌کند و به ازای هر همسایه، لیست همسایه‌های مشترک را به دست می‌آورد. اگر تعداد همسایه‌های مشترک i و j بزرگ‌تر از L باشد، گره i همسایه j را همزمان با خود تحت حمله در نظر می‌گیرد و از آن استفاده نمی‌کند. ما این مقدار آستانه را به‌صورت رابطه (۱۰) در نظر می‌گیریم.

$$L=\beta\times N \quad 0<\beta<1 \qquad (۱۰)$$

که در آن N تعداد همسایه‌های مورد انتظار و β ضریبی بین صفر و یک است. به‌عبارتی‌دیگر می‌توان آن را به‌صورت رابطه (۱۱) بیان کرد.

$$\forall i,j\in S;\ |NB(i)\cap NB(j)|\leq L\rightarrow NNB(i,j)\wedge (\forall k\in S;\ NB(i,k)\wedge NB(j,k)\rightarrow NNB(i,k)) \qquad (۱۱)$$

هر گره عادی مرحله قبل و همسایه‌های مشترک با آن به‌عنوان گره واقعی در همسایگی در نظر گرفته می‌شود.

گره‌های واقعی در همسایگی در رابطه (۱۲) و گره‌های انتقالی از طریق کرم‌چاله در رابطه (۱۳) نشان داده شده‌اند که در آن $Dist(i,j)$ نشان‌دهنده فاصله فیزیکی دو گره i و j است.

$$NB_{i,reall}=\{j\mid j\in NB(i),\ Dist(i,j)\leq r\} \qquad (۱۲)$$

$$NB_{i,worm}=\{k\mid k\in NB(i),\ Dist(i,k)\geq r\} \qquad (۱۳)$$

۴. سایر گره‌هایی که نرمال تشخیص داده نشوند، از لیست همسایگی حذف خواهند شد.

شبه‌کد الگوریتم پیشنهادی در شکل ۲ و فلوچارت آن در شکل ۳ نشان داده شده است. در شکل ۲، RCV نشانگر دریافت یا عدم دریافت پیام از گره همسایه است.

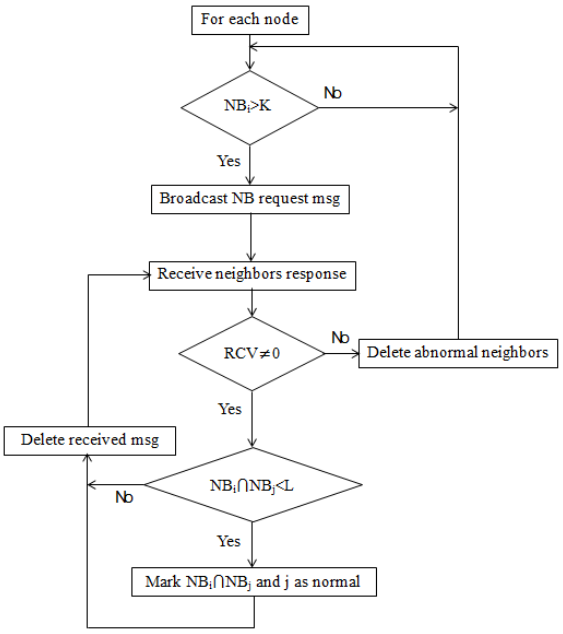
```
1 for each sensor i locally
2   monitor NBi
3   if |NBi|>α×N
4     broadcast NBReq message
5     wait for response from neighbors
6     if there is received message from node j
7       if |NBi∩NBj|<β×N
8         mark j and NBi∩NBj as normal neighbors
9         delete message from buffer and goto 6
10      else delete message from buffer and goto 6
11    else delete abnormal from NBi
12    goto 1
```

شکل ۲: فلوچارت الگوریتم پیشنهادی

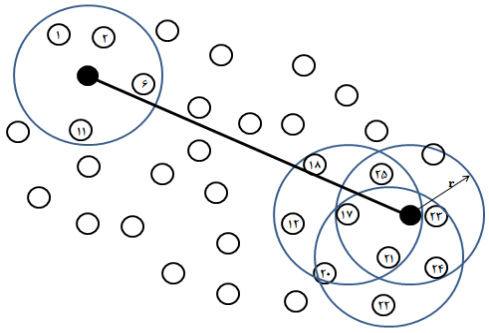
برای مثال شکل ۴ را در نظر می‌گیریم، فرض کنید تعداد همسایه‌های مورد انتظار هر گره، N=۵، α=۱/۲ و β=۰/۵ باشد؛ درنتیجه K=۶ و L=۲/۵ خواهد شد. گره‌های با رنگ سیاه، دو سر کرم‌چاله هستند و محدوده ارسال همه گره‌ها برابر r است. در شکل، گره ۲۱ با گره‌های ۱۷، ۲۰، ۲۲، ۲۳ و ۲۴ به‌صورت فیزیکی همسایه است و با گره‌های ۱، ۲، ۶ و ۱۱ از طریق کرم‌چاله همسایه شده است.

چون تعداد همسایه‌های گره ۲۱ بیش‌ازحد نرمال است، احتمال حمله می‌دهد و از گره‌های همسایه لیست همسایگی درخواست می‌کند و همسایه‌ها پاسخ می‌دهند. با دریافت اطلاعات همسایه‌ها، گره ۲۱ متوجه می‌شود که ۶ همسایه مشترک با گره ۲۴ دارد (گره‌های ۱،

۲، ۶، ۱۱، ۲۲ و ۲۳). چون تعداد همسایه‌های مشترک بیش‌ازحد آستانه (L) است، پس گره ۲۴ نیز یا از طریق کرم‌چاله منتقل شده و یا در محدوده حمله کرم‌چاله قرار دارد.



شکل ۳: شبه‌کد الگوریتم پیشنهادی



شکل ۴: وقوع کرم‌چاله در شبکه و نمایش گره‌های همسایه‌ای که خارج از محدوده حمله‌کننده و یا تحت حمله قرار دارند.

برای لیست دریافتی از گره ۲۲، تعداد همسایه‌های مشترک، ۲ (گره‌های ۲۰ و ۲۴) است و لذا گره ۲۲ خارج از محدوده کرم‌چاله است و همسایه‌های مشترک با او، گره‌های همسایه واقعی هستند. درنتیجه، نرمال بودن گره‌های ۲۰ و ۲۲ تأیید می‌شود. همچنین نرمال بودن گره ۱۷ از طریق گره ۲۰ می‌تواند تأیید شود. گره‌های ۱،۲،۶ و ۱۱ که نرمال شناسایی نشدند، از لیست همسایگی گره ۲۱ حذف می‌شوند.

۳-۴- بررسی مقادیر α و β

مقادیر α و β در میزان موفقیت روش تأثیر زیادی دارند. تأثیر α روی شروع فرآیند شناسایی گره‌های انتقالی از طریق کرم‌چاله اعمال می‌شود. دلیل اینکه α بین ۱ و ۲ در نظر گرفته شده است این است که در حالاتی که تعداد همسایه‌ها کم‌تر از تعداد مورد انتظار باشد، احتمال اینکه حمله‌ای رخ داده باشد خیلی پایین است و جهت صرفه‌جویی در انرژی مصرفی گره، فرآیند را در حالاتی که احتمال وقوع حمله بالا باشد شروع می‌کنیم و برای تعداد همسایه‌های بیش از دوبرابر مورد انتظار، احتمال وقوع حمله خیلی بالاست و به تأخیر انداختن شروع فرآیند نتیجه نامطلوبی دارد.

در رابطه (۶)، اگر α نزدیک به ۱ باشد، مقادیر K و N تقریباً برابر خواهند بود و درنتیجه نمی‌توان با قطعیت در مورد وقوع حمله و یا نرمال بودن تعداد همسایه‌ها نظر داد. چون ممکن است به‌صورت طبیعی، تعداد همسایه‌های گره، نزدیک به تعداد همسایه‌های مورد انتظارش باشد. از طرفی، هرچه α بیش‌تر شود و به ۲ نزدیک باشد، مقدار K به $2\times N$ میل خواهد کرد. در این حالت، گره زمانی احساس خطر خواهد کرد که تعداد همسایه‌هایش ۲ برابر حالت عادی باشد. به‌عبارتی‌دیگر برای برخی از حالات که حمله رخ داده باشد ولی تعداد همسایه‌ها ۲ برابر حالت عادی نشود، فرآیند شناسایی گره‌های انتقالی از طریق کرم‌چاله شروع نخواهد شد.

بر این اساس باید مقدار α بین ۱ و ۲ طوری انتخاب شود که ضمن تشخیص حمله‌های واقعی، در مواردی که حمله رخ نداده و تعداد همسایه‌های گره، به‌صورت عادی از تعداد همسایه‌های مورد انتظارش بیش‌تر است، به‌اشتباه فرآیند تشخیص گره‌های واقعی در همسایگی را شروع نشود. ما مقدار بهینه‌تر α را در آزمایش‌های انجام‌شده به دست می‌آوریم.

تأثیر β بر روی شناسایی گره‌های واقعی در همسایگی است. در رابطه (۱۰)، اگر β نزدیک به صفر باشد، مقدار L خیلی کم خواهد بود و درنتیجه امکان استفاده از برخی گره‌های همسایه که خارج از محدوده کرم‌چاله هستند و تعداد همسایه‌های مشترک با آن‌ها بیش از L است، وجود نخواهد داشت. از طرفی، هرچه β بیش‌تر شود و به ۱ نزدیک باشد، مقدار L به N میل خواهد کرد. در این حالت ممکن است به دلیل در نظر گرفتن تعداد همسایه مشترک بیش‌تر، از گره‌های همسایه‌ای که همزمان تحت حمله هستند، برای تشخیص استفاده شود. درنتیجه باید مقدار β طوری انتخاب شود که گره ضمن تشخیص گره‌های همسایه‌ای که تحت حمله هستند، از گره‌های همسایه واقعی، که تعداد همسایه مشترک بیش‌تری با آن‌ها دارد نیز استفاده نماید. ما مقدار در آزمایش‌های انجام‌شده، مقدار بهینه آن را نشان خواهیم داد.

۳-۵- انرژی و حافظه مصرفی گره‌ها برای روش پیشنهادی

برخلاف سایر روش‌ها که از سخت‌افزار یا گره‌های اضافی با امکانات بیش‌تر نسبت به گره‌های حسگر استفاده می‌شود، روش ما نیاز به هیچگونه سخت‌افزار خاص و گره‌های اضافی ندارد. هر گره لیست همسایه‌هایش را نگه‌داری می‌کند. با توجه به اینکه نگه‌داری لیست همسایه‌ها بخشی از پروتکل مسیریابی است، هزینه‌ای برای روش ما ندارد. وقتی حمله تشخیص داده شود، گره لیست همسایگی را از همسایه‌هایش درخواست می‌کند. درنتیجه، میزان حافظه مصرفی برای ذخیره لیست همسایگی گره همسایه، برای استخراج تعداد

همسایه‌های مشترک، برابر $O(N)$ خواهد بود. برای مثال اگر هر گره به‌طور متوسط m همسایه داشته باشد و شناسه هر گره 1 بیت باشد، حافظه مصرفی در روش پیشنهادی ml بیت خواهد بود، درحالی‌که در روش LDAC با همین فرضیات و با فرض $k=2$، حافظه مصرفی $2mkl$ بیت خواهد بود.

همان‌طور که اشاره شد، وقتی حمله تشخیص داده شود، گره لیست همسایگی همسایه‌هایش را درخواست می‌کند. بنابراین یک بسته برای همه‌پخشی درخواست نیاز است و N بسته که همسایه‌ها به آن پاسخ خواهند داد که درمجموع $N+1$ بسته ارسال خواهد شد. در قسمت بعدی نیز مقدار انرژی مصرفی ناشی از سربار روش پیشنهادی در مقایسه با سایر روش‌ها نشان داده می‌شود.

۴- نتایج شبیه‌سازی‌ها

برای نمایش عملکرد گره‌ها در شناسایی حمله کرم‌چاله تحت روش ارائه‌شده، با استفاده از شبیه‌ساز NS-2، حمله کرم‌چاله را در لایه لینک پیاده‌سازی کرده و برای انجام شبیه‌سازی‌ها، گره‌ها به‌صورت تصادفی در محیطی به ابعاد ۵۰ متر در ۵۰ متر پخش شده و الگوریتم روی هر گره به‌صورت جداگانه اجرا شده است. محدوده ارسال گره‌ها یکسان و برابر ۵ متر در نظر گرفته شده است. همچنین انرژی اولیه گره‌ها نیز یکسان در نظر گرفته شده است. جدول ۲ پارامترهای مورداستفاده در شبیه‌سازی‌ها را نشان می‌دهد.

جدول ۲: پارامترهای شبیه‌سازی

channel type	Channel/WirelessChannel
radio-propagation model	Propagation/TwoRayGround
Network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
interface queue type	Queue/DropTail/PriQueue
Initialenergy	10
antenna model	Antenna/OmniAntenna
rxPower	35.28e-3
txPower	31.32e-3
idlePower	712e-6
sleepPower	144e-9
simulation environment	50*50
Routing protocol type	AODV
CSThresh	5m
RXThresh	5m
Value α	0 < α < 1
Value β	1 < β <2

طبق مکانیسم پیشنهادی، هر گره درصورتی‌که تعداد همسایه‌هایش از یک حد مجاز بیش‌تر شود، فرآیند شناسایی گره‌های انتقالی از طریق کرم‌چاله را شروع می‌کند. این حد آستانه، α برابر تعداد همسایه‌های مورد انتظار برای گره‌ها است (رابطه (۶)). از طرفی دیگر، بعد از شروع فرآیند شناسایی گره‌های انتقالی از طریق کرم‌چاله، گره موردنظر به‌جای استفاده از همه همسایه‌ها، از آن‌هایی کمک می‌گیرد که تعداد همسایه‌های مشترک کم‌تر از یک مقدار آستانه داشته باشند. این حد آستانه نیز برابر β برابر تعداد همسایه‌های مورد انتظار گره‌ها است (رابطه (۱۰)).

لذا مقادیر مختلف α و β به ازای مقادیر مختلفی از شدت تراکم گره‌ها در محیط مورد آزمایش قرار گرفته و نتایج به‌دست‌آمده در قالب دو عامل متمایز نشان داده شده است. یکی از این دو عامل Precision و دیگری Recall است [۲۵]. در روابط (۱۴) و (۱۵) به ترتیب نحوه محاسبه Recall و Precision نشان داده شده‌اند.

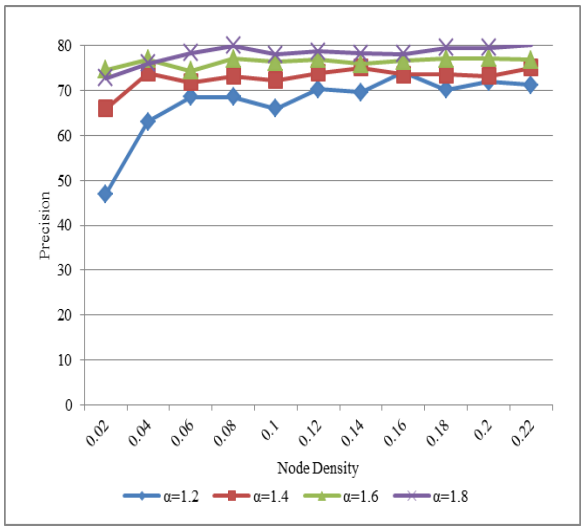
$$R = TP / (TP + FN) \quad (۱۴)$$

$$P = TP / (TP + FP) \quad (۱۵)$$

که در آن TP تعداد گره‌هایی است که از طریق کرم‌چاله انتقال یافته و در شبیه‌سازی‌ها به‌درستی شناسایی شده‌اند، FP تعداد گره‌هایی که به‌اشتباه در شبیه‌سازی‌ها به‌عنوان گره‌های انتقالی از طریق کرم‌چاله معرفی شده‌اند و FN تعداد گره‌هایی که از طریق کرم‌چاله انتقال یافته‌اند ولی در شبیه‌سازی‌ها همسایه‌های واقعی شناسایی شده‌اند.

در شکل‌های ۵ و ۶ با افزایش تراکم گره‌ها در محیط و با در نظر گرفتن مقادیر α از ۱/۲ تا ۱/۸ و β مقدار ثابت ۰/۵ نتایج به‌دست‌آمده به ترتیب برای Precision و Recall روش ارائه‌شده نشان داده شده‌اند.

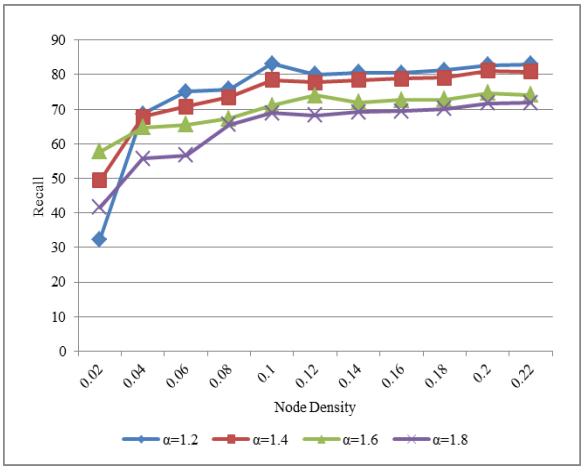
در شکل ۵ هرچه تراکم گره‌ها در محیط افزایش می‌یابد، به‌طور عمومی برای کلیه مقادیر α، Precision بیش‌تر می‌شود. همچنین برای مقادیر مختلف α نیز با افزایش آن میزان Precision بالا می‌رود.



شکل ۵: تأثیر تغییرات α و تراکم گره‌ها در محیط، روی Precision

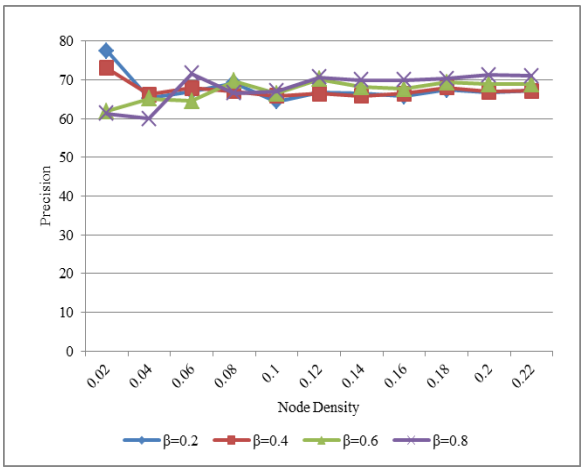
در شکل ۶ با افزایش تراکم گره‌ها در محیط، Recall بیش‌تر می‌شود ولی برای مقادیر مختلف α، با افزایش α مقادیر به‌دست‌آمده برای Recall نزولی است.

در شکل ۷ نتایج شبیه‌سازی برای Precision، به ازای مقدار ثابت α=۱/۵ و تغییرات تراکم گره‌ها و نوسان مقدار β از ۰/۲ تا ۰/۸ نشان داده شده است. مطابق شکل مذکور، تغییرات β ضمن ثابت بودن α، روی Precision تأثیر چندانی ندارد ولی در حالت کلی با افزایش β، تغییرات در Precision بهبود دارد.



شکل ۶: تأثیر تغییرات α و تراکم گره‌ها در محیط، روی Recall

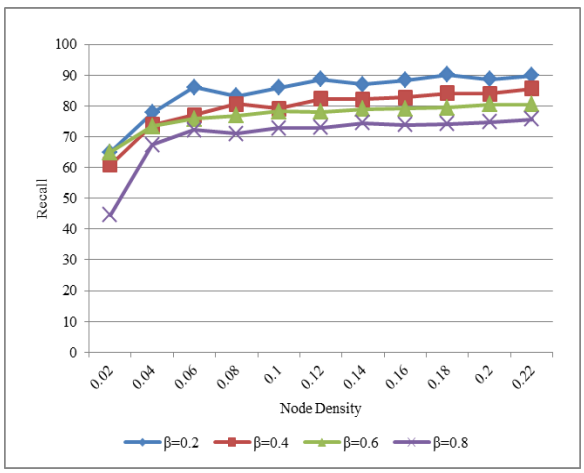
در شکل ۸ نیز نتایج به‌دست‌آمده از شبیه‌سازی‌ها برای Recall، به ازای مقدار ثابت α=۱/۵ با تغییرات β و تراکم گره‌ها در محیط، نشان داده شده است. نمودار مذکور نشان می‌دهد با افزایش تراکم گره‌ها در محیط، با α ثابت، Recall بهبود می‌یابد. از طرف دیگر، با افزایش β، به‌طورکلی Recall پایین می‌آید.



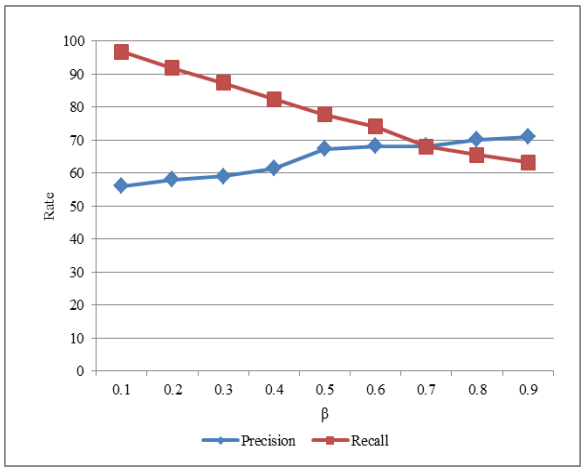
شکل ۷: تأثیر تغییرات β و تراکم گره‌ها در محیط، روی Precision

طبق نمودارهای به‌دست‌آمده، نتیجه می‌گیریم که با افزایش α، Precision بیش‌تر می‌شود ولی Recall کاهش. همچنین با افزایش β، مقدار Recall کاهش یافته و مقدار Precision بهبود جزئی دارد. برای نمایش بهتر این نتایج، ما در آزمایش دیگری ۳۰۰ گره را به‌صورت تصادفی توزیع کرده و نتایج به‌دست‌آمده را به ازای مقادیر مختلف β، با ثابت در نظر گرفتن α موردبررسی قرار دادیم. در این آزمایش، مطابق نتیجه حاصل در شکل ۹، با افزایش β، میزان Precision صعودی بوده و میزان Recall نزولی است.

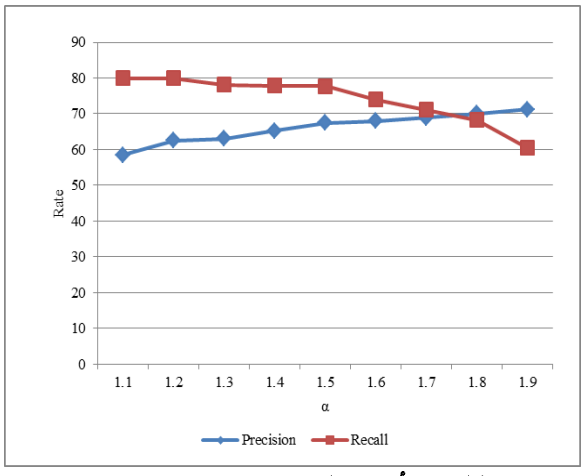
در آزمایش مشابهی مقدار β را ثابت گرفته و تأثیر مقادیر مختلف α را موردبررسی قرار دادیم که در آن، مطابق شکل ۱۰، با افزایش α، Precision صعودی بوده و Recall نزولی است.



شکل ۸: تأثیر تغییرات β و تغییرات تراکم گره‌ها در محیط، روی Recall



شکل ۹: تأثیر تغییرات β روی Recall و Precision



شکل ۱۰: تأثیر تغییرات α روی Recall و Precision

طبق نتایج حاصل‌شده، افزایش α روی Recall تأثیر منفی و روی Precision تأثیر مثبت دارد. تأثیر منفی روی Recall ناشی از آن است که وقتی α بزرگ در نظر گرفته شود، ما برای حالاتی که تعداد همسایه‌ها نسبتاً زیاد هستند، فرآیند شناسایی گره‌های انتقالی از طریق کرم‌چاله را شروع می‌کنیم و لذا برای حالاتی که حمله رخ داده و تعداد

همسایه‌ها بیش‌ازحد موردنظر ما نشده، گره‌ها فرآیند را شروع نمی‌کنند و این عمل باعث افزایش FN شده و Recall را کاهش می‌دهد. با توجه به شکل ۱۰، مقدار مناسب برای α در حالتی است که بین ۱/۴ تا ۱/۶ باشد.

از طرفی دیگر، افزایش β مقدار Precision را بهبود بخشیده و Recall را کاهش می‌دهد. علت تأثیر مثبت β روی Precision، ناشی از آن است که با افزایش β، گره موردحمله قرار گرفته از همسایه‌هایی استفاده خواهد کرد که همسایه مشترک زیادی دارند و لذا گره‌های واقعی بیش‌تری شناسایی خواهند شد. همچنین تأثیر منفی β روی Recall، ناشی از آن است که موقع استفاده از همسایه‌های با تعداد همسایه مشترک بالا، ممکن است از همسایه‌هایی که خودشان نیز تحت حمله هستند استفاده شود و مقدار FP بیش‌تر شود. طبق نمودار ۹ حالتی که β نتیجه متعادلی بین Precision و Recall می‌دهد، مقدار ۰/۵ است.

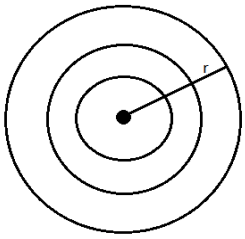
عامل دیگر در روش پیشنهادی، شدت تراکم گره‌ها در محیط است. طبق آزمایش‌ها، در تمامی حالات با افزایش تراکم گره‌ها در محیط، مقدار Precision و Recall حالت کاملاً صعودی دارند. ولی چون با افزایش گره‌ها در محیط هزینه شبکه بیش‌تر می‌شود، می‌توان بین تراکم گره‌ها و مقدار Precision و Recall به‌دست‌آمده متناسب با نیاز شبکه، حالت بینابین انتخاب کرد.

۴-۱- استفاده از قدرت سیگنال دریافتی (RSS) جهت بهبود عملکرد مکانیسم ارائه‌شده

برای ایجاد بهبود در عملکرد مکانیسم پیشنهادی، می‌توان با دخیل کردن قدرت سیگنال دریافتی فاصله از گره همسایه را تا حدودی تشخیص داد.

با داشتن فاصله گره‌ها از همدیگر، در صورت وقوع حمله کرم‌چاله، با توجه به نحوه توزیع گره‌ها در محیط، تعداد همسایه‌های گره در یک قطاع مشخصی از محدوده ارسال بیش‌ازحد معمول خواهد شد. در شکل ۱۱ قطاع‌های اطراف گره نشان داده شده است.

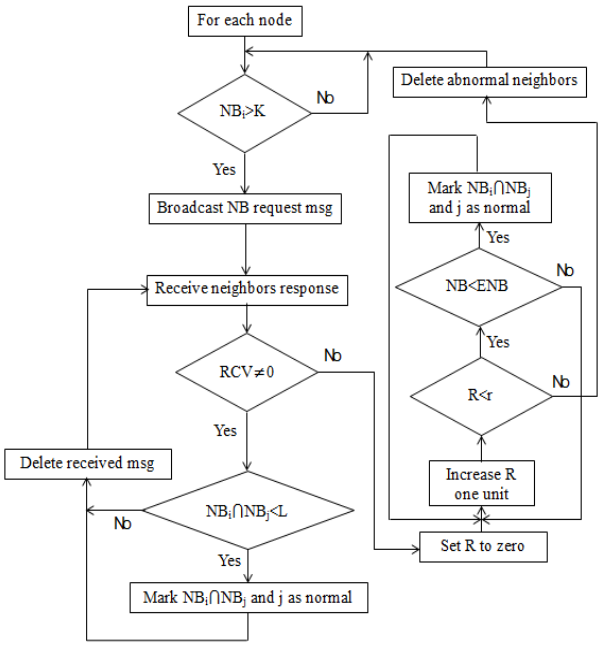
در روش پیشنهادی، ما بعد از شناسایی گره‌های همسایه واقعی اقدام به حذف سایر گره‌ها می‌کردیم ولی می‌توان بعد از مراحل مذکور در قسمت ۳-۳ و قبل از حذف گره‌های غیرنرمال، تعداد گره‌ها در قطاع‌های مختلف از همسایگی را با استفاده از قدرت سیگنال به دست آورد. در قطاع‌هایی که تعداد گره‌های عادی در خود جای داده است، احتمال وجود گره کرم‌چاله کم است، زیرا در صورت وجود گره کرم‌چاله تعداد گره‌های همسایه در این فاصله بالا خواهد بود. با اعمال این مکانیسم، فلوچارت و شبه‌کد الگوریتم پیشنهادی به ترتیب به‌صورت شکل ۱۲ و ۱۳ خواهد شد که در آن R بازه ارسال متغیر برای گره جاری است و به‌صورت $R_{\epsilon\mathbb{Z}^+} \le r$ است.



شکل ۱۱: قطاع‌بندی محدوده ارسال گره

تعداد همسایه‌های نرمال در هر قطاع از همسایگی گره را می‌توان به‌صورت رابطه (۱۶) به دست آورد که در آن S_i سطح مساحت قطاع iام است.

$$NB = d \times S_i \qquad (۱۶)$$



شکل ۱۲: فلوچارت روش ارائه‌شده به کمک قدرت سیگنال دریافتی

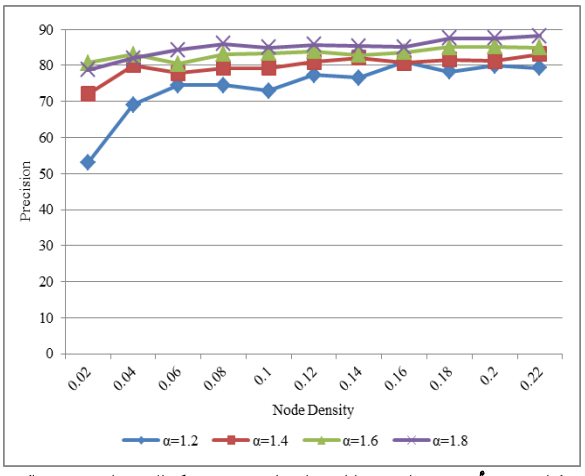
```
1 for each sensor i locally
2 monitor NBi
3  if |NBi|>α×N
4    broadcast NBReq message
5    wait for response from neighbors
6    if there is received message from node j
7      if |NBi∩NBj|<β×N
8        mark j and NBi∩NBj as normal neighbors
9        delete message from buffer and goto 6
10     else delete message from buffer and goto 6
11   else delete abnormal neighbors from NBi
12  set variable R to zero
13  increase R
14  if R less than node transmission range
15    if neighbors in range R is less than expected neighbors in
      this range
16      mark this neighbors as normal
17      goto 13
18  goto 1
```

شکل ۱۳: شبه‌کد روش پیشنهادی به کمک قدرت سیگنال دریافتی

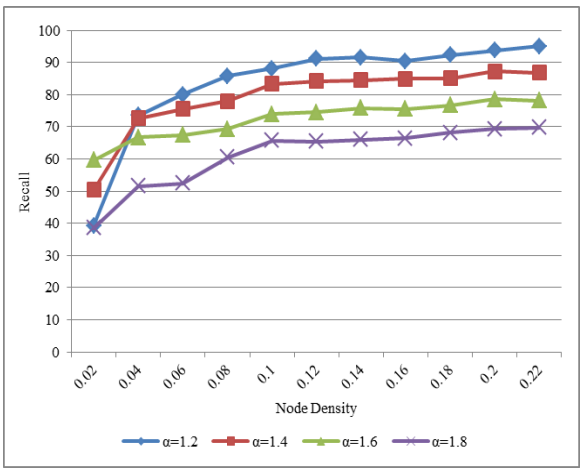
۴-۲- نتایج شبیه‌سازی‌ها موقع استفاده از RSS

با توزیع تصادفی گره‌ها در محیط و اجرای الگوریتم پیشنهادی به همراه قابلیت استفاده از قدرت سیگنال دریافتی به روی آن‌ها، نتایج به‌دست‌آمده در این قسمت آمده است.

در شکل‌های ۱۴ و ۱۵ نتایج به‌دست‌آمده به ترتیب برای Precision و Recall در αهای مختلف در شدت تراکم مختلفی از گره‌ها نشان داده شده است. در این آزمایش‌ها مقدار β ثابت و برابر ۰/۵ است.



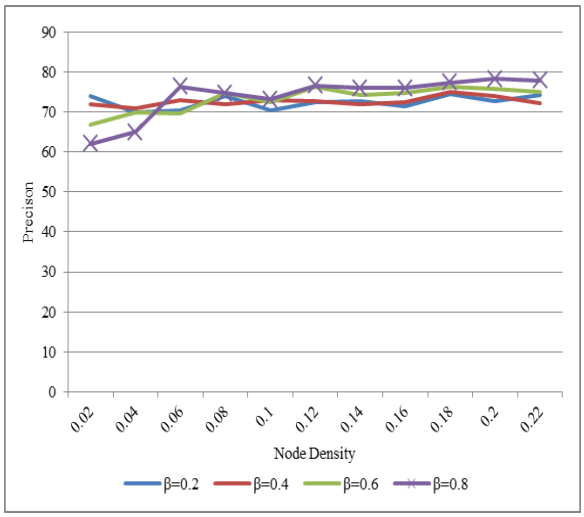
شکل ۱۴: تأثیر تغییرات α با استفاده از قدرت سیگنال دریافتی در تراکم مختلف گره‌ها، روی Precision



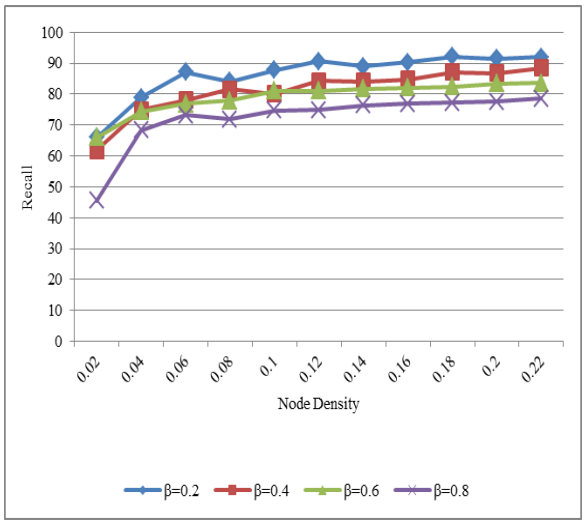
شکل ۱۵: تأثیر تغییرات α با استفاده از قدرت سیگنال دریافتی در تراکم مختلف گره‌ها، روی Recall

در شکل‌های ۱۶ و ۱۷ نیز نتایج به‌دست‌آمده به ترتیب برای Precision و Recall در βهای مختلف و شدت تراکم مختلفی از گره‌ها نشان داده شده است. در این آزمایش‌ها مقدار α ثابت و برابر ۰/۵ است. نمودارها نشان‌دهنده بهبود نتایج به‌دست‌آمده در قسمت ۴ هستند. نمودارها همچنین نشان می‌دهند که نتایج به‌دست‌آمده، در همه حالات نسبت به زمانی که از قابلیت قدرت سیگنال دریافتی استفاده نمی‌شود، دارای بهبود است.

در شکل ۱۸ نیز روش پیشنهادی با [۸] که جدیدترین روش ارائه‌شده در این زمینه است، مقایسه شده است. در این شکل نتایج به‌دست‌آمده از [۸] برای حالاتی که گره از درصد همسایه‌های معینی از لیست همسایه‌های ۲ گامی استفاده می‌کند، با روش پیشنهادی مقایسه شده است. طبق شکل مذکور روش [۸] در حالات ۲۰ و ۴۰ درصد همواره از روش پیشنهادی بهتر عمل می‌کند و در حالت ۸۰ درصد، در تعداد همسایه‌های مورد انتظار بیش‌تر از ۵ عملکرد بهتری دارد.

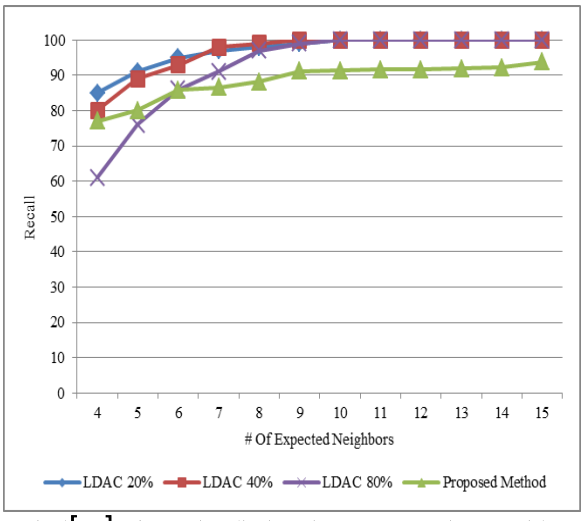


شکل ۱۶: تأثیر تغییرات β با استفاده از قدرت سیگنال دریافتی در تراکم مختلف گره‌ها، روی Precision



شکل ۱۷: تأثیر تغییرات α با استفاده از قدرت سیگنال دریافتی در تراکم مختلف گره‌ها، روی Recall

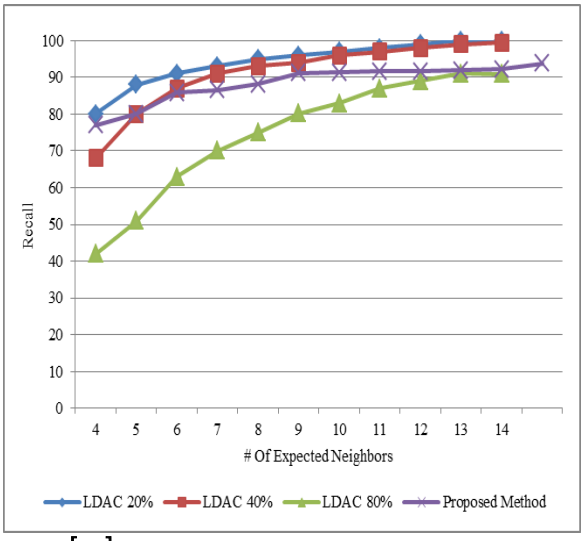
در شکل ۱۹ روش پیشنهادی با [۸] طوری مقایسه شده که روش [۸] فقط از اطلاعات همسایه‌های تک‌گامی استفاده کرده است. در این شکل نیز نتایج به‌دست‌آمده برای حالتی که گره از درصد همسایه‌های معینی از لیست همسایگی خود استفاده می‌کند، مورد مقایسه قرار گرفته است که طبق آن روش پیشنهادی از حالت ۸۰ درصد روش [۸] در همه حالات بهتر عمل می‌کند.



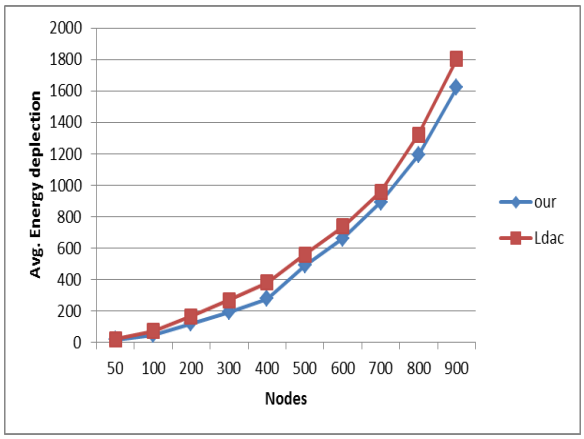
شکل ۱۸: مقایسه روش پیشنهادی با حالت‌های مختلف [۲۳] که از همسایه‌های ۲ گامی استفاده می‌کند.

به‌منظور مقایسه انرژی مصرفی روش پیشنهادی (حالت اول، بدون استفاده از RSS) با روش LDAC، آزمایش‌های مختلفی با تعداد گره‌های متفاوت انجام داده و متوسط انرژی مصرفی گره‌ها در روش پیشنهادی را با روش LDAC مورد مقایسه قرار دادیم که نتیجه آن در شکل ۲۰ آورده شده است. در این آزمایش‌ها با توجه به نتایج قسمت ۳-۶ مقادیر α و β به ترتیب ۰/۵ و ۱/۵ در نظر گرفته شده است. نتایج به‌دست‌آمده نشان می‌دهند که روش پیشنهادی در حالت‌های مختلف از تراکم گره‌ها، از دید متوسط انرژی مصرفی، نسبت به روش LDAC بهتر عمل می‌کند.

در جدول ۳ روش پیشنهادی با سایر روش‌ها مقایسه شده است و در جدول ۴ نیز روش پیشنهادی با روش‌های مبتنی بر اطلاعات همسایگی مقایسه شده است.



شکل ۱۹: مقایسه روش پیشنهادی با حالت‌های مختلف [۲۳] که از همسایه‌های تک‌گام استفاده می‌کند



شکل ۲۰: مقایسه متوسط انرژی مصرفی روش پیشنهادی با روش LDAC

جدول ۳: مقایسه روش‌های ارائه‌شده برای جلوگیری/مقابله با حمله کرم‌چاله با روش پیشنهادی [۲۳]

روش	سخت‌افزار اضافی	نرخ تشخیص/مقابله	سربار
[۱۱]	ندارد	کم	خیلی زیاد
[۱۲]	دارد	زیاد	زیاد
[۱۴]	دارد	زیاد	کم
[۱۵]	دارد	زیاد	زیاد
[۱۹]	دارد	کم	زیاد
[۸]	ندارد	زیاد	کم
[۲۴]	ندارد	زیاد	کم
روش پیشنهادی	ندارد	نسبتاً زیاد	خیلی کم

جدول ۴: مقایسه روش پیشنهادی با سایر روش‌هایی که از لیست همسایگی استفاده می‌کنند

روش	لیست همسایگی	توزیع گره‌ها	تراکم گره‌ها
[۲۲]	2-hop	تصادفی	بسیار زیاد
[۲۳]	2-hop	یکنواخت	زیاد
[۸]	k-hop	تصادفی	همه حالات
روش پیشنهادی	1-hop	تصادفی	زیاد

۵- نتیجه‌گیری

در این مقاله یک راه‌حل با انرژی و حافظه مصرفی کم برای نگه‌داری لیست همسایگی برای کشف حمله کرم‌چاله در شبکه‌های حسگر بی‌سیم ارائه کردیم. این راه‌حل از تعداد همسایه‌های گره استفاده می‌نماید تا تشخیص دهد گره تحت حمله قرار گرفته است یا نه. در صورت وقوع حمله نیز، گره‌ها از همسایه‌هایی که همزمان با گره جاری در محدوده کرم‌چاله قرار ندارند، استفاده کرده و گره‌های انتقالی از طریق کرم‌چاله را از لیست همسایگی خود حذف می‌کنند. روش پیشنهادی نیاز به سخت‌افزار یا فرضیات خاصی ندارد و به‌صورت توزیع‌شده، اقدام به شناسایی و مقابله با حمله کرم‌چاله می‌نماید.

کارهای آتی

بدیهی است که داشتن هدفی مشخص و دوراندیشی در هر زمینه‌ای می‌تواند به پیشرفت فناوری در آن زمینه کمک بزرگی نماید. ما در این قسمت برای افرادی که به شبکه‌های حسگر بی‌سیم و مخصوصاً بعد امنیتی این شبکه‌ها علاقه‌مند باشند، تعدادی از تکنیک‌ها را معرفی می‌کنیم که در ادامه می‌توانند از آن‌ها استفاده کرده و با ارائه روش‌های ترکیبی و جدید، به نتایج بهتری دست یابند و باعث ارتقای سطح امنیت در شبکه‌های حسگر بی‌سیم شوند.

- استفاده از تکنیک‌های خوشه‌بندی یا سطح‌بندی گره‌ها در شبکه و استفاده از مکانیسم‌های درهم‌سازی برای ارائه روش‌های جدید در بخش مدیریت کلیدها.
- استفاده از پایه‌ی ریاضیاتی رمزنگاری خم بیضوی برای مبادله کلید بین گره‌های شبکه به‌صورت کارآمد.
- استفاده از انواع حملات در شبکه به‌صورت عمدی برای شناسایی سایر حملات. در این تکنیک می‌توان با استفاده از حملات به‌صورت قانونی، وجود حملات دیگری را شناسایی کرد. برای مثال می‌توان از حمله کرم‌چاله به‌صورت قانونی در شبکه استفاده کرد و وجود گره‌های تکراری و حمله تکرار گره را شناسایی نمود.
- استفاده از خوشه‌بندی گره‌ها به‌منظور ارائه تکنیک‌های جدید در حوزه روش‌های IDS.

مراجع

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102-114, 2002.

[2] S. Schmidt, H. Krahn, S. Fischer, and D. Wätjen, *A* "Security architecture for mobile wireless sensor networks," *ESAS, Lecture Notes in Computer Science, Springer*, vol. 3313, pp. 166-177, 2004.

[3] E. Sabbah, and K. D. Kang, "Guide to wireless sensor networks," *Subhas Chandra Misra, Isaac Woungang, Sudip Misra*, pp. 491-512, 2009.

[4] E. Shi, and A. Perrig, "Designing secure sensor networks," *Wireless Communication Magazine*, vol. 11, no. 6, pp. 38-43, 2004.

[5] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 1-4, pp. 2-23, 2006.

[6] P. Hämäläinen,M. Kuorilehto, T. Alho, M. Hännikäinen, and T. Hämäläinen, "Security in wireless sensor networks: Considerations and Experiments," *SAMOS, Lecture Notes in Computer Science*, vol. 4017, Springer, pp. 167-177, 2006.

[7] A. D. Wood, and J. A. Stankovic, "Denial of service in sensor networks," *IEEE Computer*, vol. 35, no. 10, pp. 54-62, 2002.

[8] T. Giannetsos, and T. Dimitriou, "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks," *Computer and System Sciences*, vol. 80, no. 3, pp. 618-643, 2014.

[9] S. Stent, "A security framework for wireless sensor networks," *FGIT-FGCN, Communications in Computer and Information Science*, vol. 56, Springer, pp. 444-454, 2009.

[10] L. Buttyán, L. Dóra, and I. Vajda, "Statistical wormhole detection in sensor networks," *ESAS, Lecture Notes in Computer Science*, vol. 3813, Springer, pp. 128-141, 2005.

[11] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," *3rd ACM Workshop on Wireless Security*, pp. 51-60, 2004.

[12] R. Poovendran, and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27-59, 2007.

[13] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," *IEEE INFOCOM*, vol. 3, pp. 1976-1986, 2003.

[14] H. Chen, W. Lou, X. Sun, and Z. Wang, "A secure localization approach against wormhole attacks using distance consistency," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, pp. 1-12, 2010.

[15] S. S. Capkun, L. Buttyan, J. P. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," *Workshop on Security of ad Hoc and Sensor Networks – SASN*, pp. 21-32, 2003.

[16] I. Khalil, S. Bagchi, and N. B. Shroff, "LiteWorp: Detection and isolation of the wormhole attack in static multihop wireless networks," *Computer Networks*, vol. 51, no. 13, pp. 3750-3772, 2007.

[17] X. Wang, and J. Wong, "An end-to-end detection of wormhole attack in wireless ad-hoc networks," *International Computer Software and Applications Conference – COMPSAC*, vol. 1, pp. 39-48, 2007.

[18] L. Hu, and D. Evans, "Using directional antennas to prevent wormhole attacks," *Network and Distributed System Security Symposium - NDSS*, 2004.

[19] L. Lazos, and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 1, pp. 73-100, 2005.

[20] Y. B. Ko, V. Shankarkumar, and N. H. Vaidya, "Medium access control protocols using directional antennas in ad hoc networks," *IEEE INFOCOM*, vol. 1, pp. 13-21, 2000.

[21] R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya, "Using directional antennas for medium access control in ad hoc networks," *Mobile Computing and Networking – MOBICOM*, pp. 59-70, 2002.

[22] Y. T. Hou, C. M. Chen, and B. Jeng, "Distributed detection of wormholes and critical links in wireless sensor networks," *International Information Hiding and Multimedia Signal Processing, IIH-MSP*, pp. 639-642, 2007.

[23] C. Lee, and J. Suzuki, "Swat: A decentralized self-healing mechanism for wormhole attacks in wireless sensor networks," *Sensor Networks*, Chapter 24.

[24] B. Tian, Q. LiI, Y. X. Yang, D. LiI, and Y. Xin, "A ranging based scheme for detecting the wormhole attack in wireless sensor networks," *The Journal of China Universities of Posts and Telecommunications*, vol. 19, Supplement 1, pp. 6-10, 2012.

[25] Bing Liu, *Web Data Mining: Exploring Hyperlinks, Contents, and Usage Data (Data-Centric Systems and Applications)*, Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.