نشریه علمی «پدافند الکترونیکی و سایبری»
سال هفتم، شماره ۱، بهار ۱۳۹۸؛ ص ۱۰-۱

یک مدل اعتماد مبتنی بر الگوریتم‌های هوش جمعی در شبکه‌های حسگر بی‌سیم

افشار خسروی[۱]، علی کریمی[۲*]، محمدعلی جوادزاده[۳]، محمدجواد خسروی[۴]

۱- کارشناسی ارشد، ۲ و ۳- استادیار دانشگاه جامع امام حسین(ع)، ۴- دانشجوی کارشناسی ارشد دانشگاه علامه طباطبایی

(دریافت: ۹۶/۰۳/۱۶، پذیرش: ۹۶/۱۰/۱۶)

چکیده

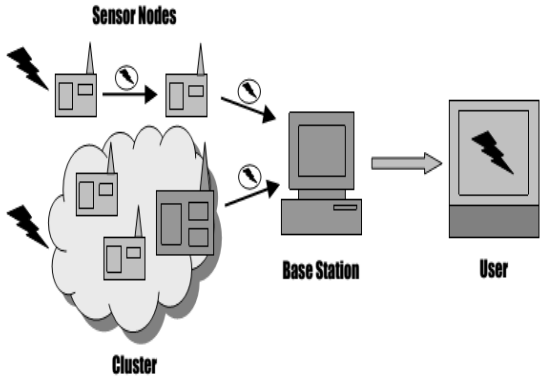
بیشتر کاربردهای گره‌های حسگر در مکان‌های خطرناک، غیرقابل‌دسترس و یا محیط دشمن است که همین موضوع نیاز به امنیت در این شبکه‌ها را ضروری می‌سازد. روش‌های اعتماد، ابزاری قدرتمند برای تشخیص رفتار غیرمنتظره گره‌ها (خواه گره‌های بدخواه و یا گره‌های دچار خرابی) هستند. در این مقاله مدل اعتماد TBSI پیشنهاد شده است که ویژگی بارز این مدل، سربار محاسباتی کم، مصرف انرژی ناچیز و مقابله با حملات صورت‌گرفته در شبکه‌های حسگر بی‌سیم است. این مدل با استفاده از نرم‌افزار شبیه‌ساز NS-2 شبیه‌سازی شده و رفتار آن بر اساس نتایج این شبیه‌سازی‌ها مورد ارزیابی قرار گرفته است. بررسی نتایج عملی نشان می‌دهد که میزان مصرف انرژی، سربار مسیریابی، زمان مرگ گره‌ها کاهش و نرخ تحویل بسته به ایستگاه پایه افزایش پیدا می‌کند. مطلوب بودن این نتایج ثابت می‌کند که بهره‌گیری از روش اعتماد راه‌حل مناسبی برای دست‌یابی به یک شبکه امن برای حل مسائل مطرح در حوزه امنیت شبکه‌های حسگر بی‌سیم است.

واژه‌های کلیدی: شبکه‌های حسگر بی‌سیم، اعتماد، مسیریابی، حملات شبکه

۱- مقدمه

با افزایش کاربردهای شبکه‌های حسگر بی‌سیم[۱] از قبیل کاربرد در صنایع نظامی، حفظ امنیت یک محیط فیزیکی، اعلام‌خطر ورود مهاجم به یک محل کنترل‌شده، گسترش و ماندگاری در مکان‌های بیابانی و صعب‌العبور، نظارت بر محل‌های مسکونی، ردیابی هدف‌های متحرک، آشکارسازی حریق، نظارت ترافیک و غیره لزوم حفظ امنیت و جلوگیری از بدرفتاری در این سیستم‌ها روزبه‌روز افزایش می‌یابد. بدرفتاری در شبکه‌های حسگر بی‌سیم به شکل‌های مختلفی دیده می‌شود؛ از بین رفتن بسته‌ها، تغییر ساختارهای داده‌ای مهم در امر مسیریابی، ایجاد انحراف در همبندی شبکه و درنهایت ایجاد گره‌های جعلی نمونه‌هایی از این بدرفتاری‌ها محسوب می‌شوند. شبکه‌های حسگر بی‌سیم باید بتوانند عوامل مخل امنیت خود را در کوتاه‌ترین زمان ممکن و با دقت بالا شناسایی نمایند.

شبکه‌های حسگر بی‌سیم معمولاً از محدودیت منابعی مانند منابع انرژی، منابع محاسباتی و ارتباطی رنج می‌برند، به همین دلیل روش‌هایی مانند رمزنگاری در این نوع از شبکه‌ها با هزینه‌های زیادی همراه است. در شکل (۱) نمای کلی یک شبکه حسگر بی‌سیم نشان داده شده است.



شکل (۱): نمای کلی یک شبکه حسگر بی‌سیم [۱]

معماری شبکه‌های حسگر بی‌سیم می‌تواند مسطح[۲] یا سلسله‌مراتبی[۳] باشد. در این مقاله معماری سلسله‌مراتبی انتخاب شده است. مسئله اصلی شناسایی گره‌های مهاجم در شبکه و جلوگیری از حذف، تغییر و یا سرقت اطلاعات با کمترین سربار و اتلاف انرژی است. این مسئله در این مقاله با تمرکز بر حمله‌های هم‌خانواده سیاه‌چاله[۴] بررسی می‌گردد که در شناسایی این حمله‌ها چالش اصلی شناسایی گره‌هایی هستند که قصد حمله را دارند.

*رایانامه نویسنده پاسخگو: a.karimi@ihu.ac.ir

1- Wireless Sensor Networks

2- Flat
3- Hierarchical
4- Black Hole

از آنجاکه از معماری سلسله مراتبی استفاده شده است و با توجه به دوره خواب و بیداری گره‌ها، تشخیص حملات می‌تواند فقط در گره‌های سرخوشه[1] (ایستگاه پایه[2]) به‌تنهایی صورت گیرد و یا این‌که گره سرخوشه و گره‌های معمولی باهم مسئول تشخیص این نوع حملات باشند. اگر گره سرخوشه به‌تنهایی عهده‌دار روال پردازش داده باشد، آشکارا باعث مصرف انرژی در این گره می‌شود. اگر بسته موردنظر در پایان انتقال، فقط در ایستگاه پایه بررسی شود، خطر انتقال یک بسته خراب (ویروسی) به قسمت زیادی از شبکه، باعث افزایش بار ترافیکی و مصرف منابع ارزشمند شبکه می‌شود. در مدل پیشنهادی TBSI، گره سرخوشه و گره‌های معمولی برای مقابله با حملات بدخواهانه همکاری دارند که این امر موجب می‌شود وظیفه شناسایی گره‌های مخرب بر دوش یک گره یا گره‌های خاصی نباشد. این مقاله در پنج بخش تنظیم شده است. در بخش دوم پروتکل لیچ و تحقیقات صورت گرفته در حوزه اعتماد[3] ارائه می‌شود. در بخش سوم مدل TBSI با استفاده از الگوریتم کلونی مورچه‌ها[4] و نظریه بازی‌ها[5] ارائه می‌شود. در بخش چهارم شبیه‌سازی مدل و ارزیابی نتایج آن انجام می‌گیرد و در پایان هم نتیجه‌گیری و بیان نقاط قوت و ضعف این مدل ارائه می‌گردد.

۲- مروری بر کارهای انجام‌شده

۲-۱- پروتکل لیچ[6]

پروتکل لیچ یک پروتکل خوشه‌بندی خودسازمان‌ده[7] است که بار انرژی را بر روی حسگرهای شبکه توزیع می‌کند. در این پروتکل گره‌ها خودشان را در خوشه‌های محلی سازمان‌دهی می‌کنند، به‌گونه‌ای که یک گره در خوشه به‌عنوان سرخوشه عمل می‌کند. برای این‌که با اتمام انرژیِ گره سرخوشه، کل خوشه از کار نیفتد و عمر خوشه تمام نشود، گره‌ها در خوشه به‌صورت چرخشی و تصادفی سرخوشه می‌شوند. به‌علاوه، داده‌ها به‌صورت محلی باهم تجمیع می‌شوند تا مقدار داده‌هایی که باید به گره سرخوشه (ایستگاه پایه) ارسال شوند کمتر شده و درنتیجه مصرف انرژی کاهش و عمر شبکه افزایش یابد. از محاسن این پروتکل می‌توان به خوشه‌بندی توزیع‌شده و عدم نیاز به موقعیت مکانی گره‌ها اشاره کرد. از معایب این پروتکل می‌توان به عدم مقیاس‌پذیری مناسب به‌علت ارتباطات تک‌جهشه، عدم توزیع مناسب خوشه‌ها در شبکه که در این حالت ممکن است دو یا چند سرخوشه در فاصله بسیار کوتاهی از یکدیگر قرار گیرند، عدم در نظر گرفتن انرژی باقی‌مانده گره‌ها، عدم توزیع مناسب تعداد اعضای خوشه‌ها و درنهایت، احتمال انتخاب نشدن یک سرخوشه در یک یا چند دور[8] اشاره نمود [۲].

۲-۲- پروتکل مسیریابی آگاه از اعتماد TARF[9]

این پروتکل، یک مسیریابی چندمسیره در شبکه‌های حسگر را از طریق ارزیابی قابلیت اعتماد گره‌های همسایه انجام می‌دهد. همچنین گره‌های غیرقابل‌اعتماد را مشخص می‌کند و در مسیریابی آن‌ها را دور می‌زند. این پروتکل بر کارایی انرژی و قابلیت اعتماد گره‌ها تمرکز دارد. اصالت این پروتکل بر حملاتی متمرکز است که در آن یک مهاجم، ترافیک شبکه را از طریق تکرار اطلاعات مسیریابی با جعل هویت، به مسیر نادرست هدایت می‌کند. مزیت این پروتکل آن است که به محدودیت‌های هم‌زمانی شدید و یا اطلاعات جغرافیایی نیاز ندارد. این پروتکل به‌عنوان یک ماژول با سربار کم در سیستم‌عامل TinyOS پیاده‌سازی شده است و می‌تواند با کمترین سازوکار نرم‌افزاری در پروتکل‌های مسیریابی موجود جاسازی شود. اهداف آن گذردهی بالا، بهره‌وری انرژی، تطبیق‌پذیری و مقیاس‌پذیری هستند. از معایب آن می‌توان به عدم ارائه راه‌کار در مورد حملات اختلال سرویس[10]، و نیز عدم توجه به معیارهایی مانند تأخیر پایین، بار ترافیکی متعادل و عدالت توزیع منابع اشاره نمود. از این‌رو، هنگام تشخیص وجود گره خطاکار در مسیر، مسیر را از ابتدا بنا می‌کند [۳].

۲-۳- پروتکل تشکیل مسیر قابل‌اعتماد TLSRP[11]

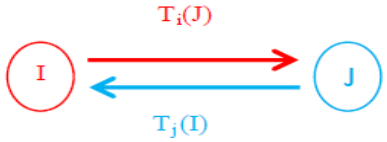
یک الگوریتم جدید برای ساخت مسیری قابل‌اعتماد از گره مبدأ به چاهک[12] با در نظر گرفتن اعتماد مستقیم و غیرمستقیم در [۴] ارائه‌شده است. مقاومت این پروتکل در برابر حملات مختلف ارزیابی نشده است. در این الگوریتم گره‌ها خوشه‌بندی شده و انتخاب سرخوشه بر مبنای انرژی باقی‌مانده گره‌ها انجام می‌گیرد. گره سرخوشه پیام تبلیغ[13] خود را برای همسایگانش ارسال می‌کند و منتظر دریافت پیام عضویت از گره‌های خوشه می‌شود. سپس، گره‌ها را برای دو منظور مسیریابی و جمع‌آوری داده از محیط، خوشه‌بندی می‌کند. گره‌هایی که در مرز خوشه‌ها قرار می‌گیرند وظیفه دریافت و ارسال پیام برای سرخوشه از

1- Head Cluster
2- Base Station
3- Trust
4- Ant Colony
5- Game Theory
6- Leach
7- Self Organize
8- Round
9- Trust Aware Routing Framework for WSNs
10- Denial Of Service
11- Trust-based Link State Routing Protocol
12- Sink
13- Advertisement Message

خوشه‌های مجاور یا برعکس را به عهده دارند. روند محاسبه اعتماد دو گره نظیر به نظیر، طبق رابطه (۱) محاسبه می‌گردد:

$$TE_{i,j}\ or\ TE_{j,i} = + \frac{\left(T_i(J)+T_j(i)\right)}{2} \qquad (۱)$$

رابطه (۱)، ارزیابی اعتماد دو گره نظیر به نظیر در پروتکل TLSRP را نشان می‌دهد. همچنین در شکل (۲)، ارزیابی اعتماد بین دو گره نظیر به نظیر نشان داده شده است.



شکل (۲): ارزیابی اعتماد بین دو گره نظیر به نظیر [۴]

۲-۴- پروتکل مسیریابی آگاه از انرژی و اعتماد ATSR[1]

یک الگوریتم کاملاً توزیع‌شده برای ارزیابی قابلیت اعتماد گره‌ها است. طبق این الگوریتم، گره‌ها با توجه به معیارهای اعتماد خاصی بر رفتار همسایه‌های خود نظارت می‌کنند و یک مقدار اعتماد مستقیم را برای هر گره همسایه محاسبه می‌کنند. پروتکل ATSR از اعتماد غیرمستقیم هم استفاده می‌کند. سپس این دو مقدار را برای به‌دست آوردن اعتماد نهایی باهم ترکیب کرده و درنهایت، گره‌های امن شبکه را شناسایی و جهت مسیریابی، صرفاً با این گره‌ها ارتباط برقرار می‌کند [۵].

۲-۵- پروتکل مسیریابی مبتنی بر اعتماد در انرژی محدود TRUSTEE[2]

این پروتکل جهت مسیریابی مبتنی بر اعتماد در شبکه‌های حسگر با محدودیت انرژی پیشنهاد شده است. این پروتکل یک روش انعطاف‌پذیر و عملی است که کیفیت مسیرها را ارزیابی می‌کند. لذا مسیری را انتخاب می‌کند که از سایر مسیرها نیازمندی‌های امنیتی را بهتر تأمین کند. در این روش فرض شده است که هر گره شامل اطلاعاتی در رابطه با همسایگانش است و به‌منظور ارتباط امن همسایه‌ها کلیدهایی را از طریق روش‌های پیش‌توزیع باهم به اشتراک می‌گذارند. این روش نه‌تنها مصرف منابع از قبیل حافظه، انرژی و سربار محاسباتی[3] را به حداقل می‌رساند، بلکه می‌تواند به دلیل احراز هویت گره‌ها در مقابل حملات خارجی به‌خوبی عمل کند. درنتیجه توان عملیاتی شبکه را به میزان زیادی افزایش می‌دهد [۶].

۲-۶- پروتکل مسیریابی مبتنی بر مدیریت اعتماد TRANS

یک پروتکل مسیریابی است که برای اجتناب از مکان‌های ناامن، مسیرها را از بین گره‌ها بر مبنای اطلاعات اعتماد و نه بر مبنای تعداد گام و یا معیارهای دیگر انتخاب می‌کند. این پروتکل بر مبنای فرضیاتی است که حسگرها موقعیت تقریبی خود را می‌دانند و در آن از مسیریابی جغرافیایی استفاده می‌کنند. در پروتکل TRANS یک همسایه قابل‌اعتماد، حسگری است که می‌تواند درخواست را رمزگشایی کند و به‌اندازه کافی قابل‌اعتماد باشد (با توجه به سابقه ارسال‌های ثبت‌شده آن به‌وسیله چاهک و سایر گره‌های میانی). چاهک، پیام‌ها را فقط به همسایه‌های قابل‌اعتماد خود می‌فرستد (گره‌هایی که مقدار اعتماد آن‌ها بیشتر از آستانه اعتماد مشخص شده است)، به همین ترتیب همسایه‌های آن‌ها نیز بسته‌ها را به همسایه‌های قابل‌اعتمادی می‌فرستند که نزدیک‌ترین مکان را تا مقصد داشته باشند؛ بنابراین بسته‌ها از طریق مسیری از حسگرهای قابل‌اعتماد به مقصد می‌رسند. یک ویژگی مهم TRANS این است که ایجاد فهرست سیاه در آن به‌وسیله چاهک، توزیع شده است.

این مورد، از این فرض ناشی می‌شود که گره چاهک درخطر نمی‌افتد. گره چاهک با مشاهده پاسخ‌ها سوءرفتارها را شناسایی، مکان‌های بالقوه سوءرفتارها را کاوش و مکان‌های ناامن را ایزوله می‌کند. بعد از حذف بسته‌ها به میزان زیاد، گره چاهک جستجویی را برای مکان‌های ناامن در طول مسیر آغاز کرده و با کشف این مکان‌ها آن‌ها را ثبت می‌کند و این اطلاعات را به گره‌های همسایه اعلام می‌نماید [۷].

۲-۷- پروتکل مسیریابی مبتنی بر مدیریت اعتماد SPINS

مجموعه‌ای از پروتکل‌های امنیتی بهینه‌شده برای شبکه‌های حسگر جهت ایجاد محرمانگی داده، احراز هویت دوطرفه و اثبات محرمانگی ارائه داده است. با این‌حال، در رابطه با حملات انکار سرویس یا گره‌های به خطر افتاده کار خاصی را انجام نمی‌دهد و فقط اطمینان حاصل می‌کند که آیا گره به خطر افتاده کلیدهای شبکه را فاش می‌کند یا خیر [۸].

۲-۸- پروتکل آگاه از انرژی با استفاده از الگوریتم ترکیبی

در این پروتکل، یک الگوی ارسال داده با استفاده از تلفیقی از ارتباطات چندگامی و ارسالات سلسله‌مراتبی ارائه شده است که در محتوای آن، روشی برای انتخاب تعداد و اندازه مناسب خوشه‌ها بر اساس بهینه‌سازی همزمان انرژی دورن‌خوشه‌ای و

1- Ambient Trust Sensor Routing
2- Trust-Based Routing Framework in Energy-Constrained
3- Computational Overhead

انرژی ارسال داده‌ها به پایگاه اصلی وجود دارد. در این پروتکل، با استفاده از الگوریتم بهینه‌سازی ژنتیک، تعداد و اندازه خوشه‌ها بهینه می‌گردند. در الگوریتم ارائه‌شده، ابتدا محیط تحت‌پوشش گره‌های حسگر که یک فضای دایره‌ای شکل است به قطاع‌های گوناگون تقسیم گشته و سرخوشه‌های هر قطاع، در طی دفعات مختلف ارسال، بر اساس حداکثر انرژی باقیمانده میان گره‌های موجود در هر قطاع، انتخاب می‌شوند [۹]. تمرکز این پروتکل، بهینه‌سازی مصرف انرژی بوده و دغدغه اصلی آن هم، کمبود انرژی در شبکه‌های حسگر بی‌سیم است. در این پروتکل، اگر گره‌ای یک رفتار بدخواهانه داشته باشد می‌تواند شبکه را مختل نماید. در خوشه‌بندی این پروتکل، تنها معیار انتخاب سرخوشه انرژی باقیمانده گره‌ها بوده و گره‌های مخرب می‌توانند به‌عنوان سرخوشه انتخاب شده و اطلاعات جمع‌آوری‌شده را به مقصد نامعتبر ارسال نمایند.

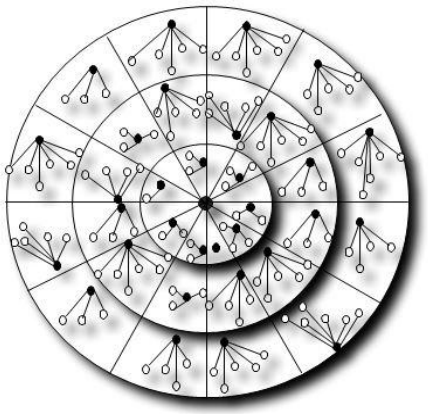
۲-۹- پروتکل مسیریابی سلسله‌مراتبی TSBC[1]

TSBC، یک پروتکل مسیریابی بوده که هدف آن کاهش انرژی مصرفی و افزایش طول‌عمر شبکه است. این پروتکل، برمبنای تقسیم مساحت شبکه به چندین قطاع و سطح و انتخاب سرخوشه‌ها از سطح پایین‌تر که مسافت کمتری تا ایستگاه مرکزی دارند، ارائه شده است. برای کمینه کردن جریان معکوس داده از سمت ایستگاه مرکزی، از ساختار درختی در هر قطاع استفاده شده است [۱۰].

در این پروتکل، به علت صرفه‌جویی در مصرف انرژی، فقط گره‌های نزدیک به ایستگاه مرکزی می‌توانند سرخوشه شوند و این نقش به گره‌های دوردست داده نمی‌شود. پروتکل TSBC، مناسب کاربردهایی می‌باشد که در آن‌ها، صرفه‌جویی در مصرف انرژی کاملاً اجباری است. یکی از نقطه‌ضعف‌های این پروتکل، این است که موارد امنیتی در آن، لحاظ نشده است.

۳- مدل پیشنهادی

در شبکه‌های حسگر به‌ویژه زمانی که گره‌ها فاقد امکانات حرکتی هستند، مقصد نهایی معمولاً گره‌ای به نام چاهک یا ایستگاه پایه است. این گره معمولاً از منابع بیشتری نسبت به سایر گره‌ها برخوردار است. گره‌ها در یک یا چند گام اطلاعات خود را برای چاهک ارسال می‌کنند. در این مقاله یک مدل اعتماد معرفی می‌شود که سربار کمتری روی شبکه اعمال نماید. به دلیل اصرار بر حداقل سربار، در این مقاله از اعتماد غیرمستقیم چشم‌پوشی شده است. البته باید توجه داشت که این رویکرد زمانی امکان‌پذیر است که گره‌ها ثابت باشند. مدل اعتماد پیشنهادی در این مقاله عبارت است از مدل TBSI[2]. همان‌گونه که در شکل (۳) نشان داده شده است در این مدل، محیط شبکهِ تحت بررسی به نواحی مختلفی تقسیم‌بندی می‌شود. در هر ناحیه قطاع‌ها و درنتیجه قطعه‌های مختلفی به‌وجود می‌آیند. گره‌ها داخل قطعه‌های مختلف تشکیل خوشه می‌دهند. بعد از تشکیل خوشه، تمامی گره‌ها اطلاعات جمع‌آوری شده را به گره سرخوشه می‌دهند و گره سرخوشه نیز در انتهای هر دور، داده‌ها را تجمیع کرده و به گره چاهک ارسال می‌کند.



شکل (۳): نمای کلی مدل TBSI

مراحل مختلف عملکرد مدل TBSI شامل: مکان‌یابی، ناحیه‌بندی محیط، قطاع‌بندی و قطعه‌بندی، خوشه‌بندی و در پایان مدل اعتماد ارائه‌شده به شرح ذیل توضیح داده می‌شود.

۳-۱- مکان‌یابی

مکان‌یابی گره‌ها در شبکه، مبتنی بر این فرض است که گره چاهک قابلیت جابجایی و GPS را در شبکه دارا می‌باشد. در مدل TBSI، گره چاهک یک پیام حاوی مختصات مکانی خود را در شبکه همه‌پخشی می‌کند. سپس یک جابجایی مثلثی را انجام داده و در هر یک از رئوس مثلث اطلاعات مکانی خود را برای گره‌ها ارسال می‌کند و تا انتهای طول عمر خود در آن نقطه باقی می‌ماند. گره‌ها با استفاده از اطلاعات مکانی چاهک در زمان ارسال پیام و فاصله به‌دست‌آمده از طریق شدت سیگنال پیام، قادر خواهند بود مکان تقریبی خود را با استفاده از حل دستگاه زیر محاسبه نمایند. رابطه (۲) محل تقریبی هر گره را محاسبه می‌کند.

$$\begin{cases} d_1 = \sqrt{(x-x_1)^2 + (y-y_1)^2} \\ d_2 = \sqrt{(x-x_2)^2 + (y-y_2)^2} \\ d_3 = \sqrt{(x-x_3)^2 + (y-y_3)^2} \end{cases} \quad (۲)$$

1- Tree Sector Bi-level Clustering

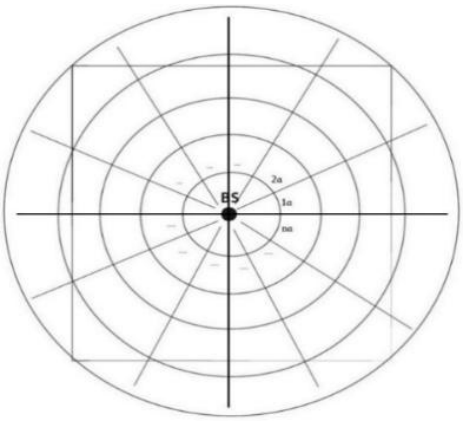
2- Trust Model Based On Swarm Intelligence

۳-۲- ناحیه‌بندی محیط

برای انجام ناحیه‌بندی از الگوریتم کلونی مورچه‌ها استفاده شده است. گره چاهک با توجه به آشنایی با طول و عرض شبکه، از قسمت طولی، محیط تحت‌بررسی را به چندین ناحیه تقسیم می‌کند. ناحیه‌ها دوایری متحدالمرکز هستند. گره چاهک برای شناسایی ناحیه‌بندی‌ها به گره‌ها، از مورچه استفاده می‌کند. هر مورچه مسافت مشخصی را طی کرده و سپس دوران زندگی‌اش به پایان می‌رسد. مورچه‌ها فرومون[1] α را در محیط باقی می‌گذارند. هر دسته از گره‌ها فرومون α را به فرومون خود می‌افزایند و گره‌هایی که فرومون برابر دارند، در یک ناحیه قرار می‌گیرند. ناحیه‌ها در حقیقت دایره‌هایی به مرکز آخرین مختصات گره چاهک است.

۳-۳- قطاع‌بندی

پس از این‌که گره چاهک کل شبکه را ناحیه‌بندی کرد، اقدام به قطاع‌بندی می‌کند که در نتیجه‌ی آن و ناحیه‌بندی، قطعه‌های مختلفی تشکیل می‌شوند. قطاع‌بندی به این‌صورت است که گره چاهک یک پیامِ حاوی مختصات نهایی خود و یک زاویه را ارسال می‌کند. گره‌ها پس از دریافت این پیام، مختصات گره چاهک را مبدأ مختصات (۰،۰) در نظر می‌گیرند و مختصات جدید خود را محاسبه می‌کنند. گره‌ها در هر قطعه‌ای که مختصاتشان در آن صدق کرد، آن را به‌عنوان قطعه خود برمی‌گزینند. انتخاب زاویه قطاع‌بندی، با توجه به عرض شبکه انجام می‌شود. حاصل تقسیم عرض شبکه به مسافت طی‌شده توسط مورچه‌های دسته‌ی اول، تعداد قطاع‌ها را مشخص می‌کند. سپس گره چاهک، 2π را به تعداد قطاع‌ها تقسیم کرده و این عدد را به‌عنوان زاویه قطاع به اطلاع گره‌ها می‌رساند. شکل (۴)، نحوه انجام قطاع‌بندی را نشان می‌دهد.



شکل (۴): نحوه انجام قطاع‌بندی

۳-۴- خوشه‌بندی

گره‌های درون یک قطعه باهم تشکیل خوشه می‌دهند. گره‌ها برای بار اول کوچک‌ترین شناسه‌ی موجود را به‌عنوان سرخوشه انتخاب می‌کنند و سپس زمان حالت پایدار را بر تعداد گره‌های موجود در خوشه تقسیم می‌کنند؛ و به‌ترتیب شناسه اقدام به ارسال داده‌های خود برای سرخوشه می‌کنند. در انتهای هر دور، گره‌های سرخوشه داده‌ها را تجمیع و برای گره چاهک ارسال می‌کنند. در انتهای دور، چون هیچ گره‌ای خوشه را ترک نمی‌کند، نیازی به انجام کامل الگوریتم خوشه‌بندی برای دورهای بعدی نیست. در دورهای بعد گره‌ها بر اساس میزان انرژی خود به‌عنوان سرخوشه انتخاب می‌شوند.

۳-۵- اعتماد و تحمل‌پذیری خطا

در مرحله راه‌اندازی اعتماد باید برای هر گره مقدار اعتبار اولیه‌ای در نظر گرفت. اگر مقدار اعتبار اولیه گره‌ها زیاد و نزدیک به ۱۰۰ باشد همه گره‌ها به یکدیگر اعتماد زیادی خواهند داشت و تشخیص گره قابل‌اعتماد از گره بدخواه مشکل خواهد بود. از طرف دیگر، اگر مقدار اولیه اعتبار، مقدار کمی در نظر گرفته شود در ابتدا، همه اعضا نسبت به سایرین دچار عدم اعتماد هستند و در این حالت نیز مشابه مشکل قبلی می‌باشد؛ بنابراین، در ابتدای کار، گره‌ها با میزان اعتبار ۵۰ در شبکه قرار می‌گیرند و در طول تراکنش‌های مختلف این مقدار به‌روزرسانی شده و به مقدار واقعی نزدیک‌تر می‌شود. گره‌های مخرب به‌مرور از اعتبارشان کاسته شده و گره‌هایی که اعتبار آن‌ها به زیر ۲۰ می‌رسد نقش سرخوشه‌گی به آن‌ها تعلق داده نمی‌شود و گره‌هایی که اعتبار آن‌ها به صفر برسد بلوکه می‌شوند. از گره‌هایی که بلوکه شده‌اند، هیچ پیامی دریافت نمی‌شود و پیامی برایشان ارسال نمی‌گردد. لازم به ذکر است که میزان اعتبار از ۰ تا ۱۰۰ تغییر می‌کند. گره‌هایی که اَعمال درست انجام دهند، به مقدار اعتبارشان افزوده می‌شود. هرچقدر اعتبار یک گره بالاتر باشد میزان اعتماد به آن در شبکه بالاتر می‌رود.

مدل اعتماد پیشنهادی با توجه به قوانین پروتکل که از آن‌ها به‌عنوان قواعد بازی یاد می‌شود، تعریف خواهد شد. در حقیقت در انتهای هر دور انتظار می‌رود که سرخوشه داده‌های خود را برای گره چاهک ارسال نماید. سرخوشه‌ای که از این عمل سرباز زند، از میزان اعتبارش به مقدار ۱۵ واحد کاسته می‌شود. ازآنجاکه ممکن است این شرایط به دلیل مسائلی همچون عدم تخصیص کانال و غیره باشد، درصورتی‌که در دورهای بعد سرخوشه عمل درست را انجام دهد میزان اعتبارش ۱۵ واحد افزایش می‌یابد.

1- Pheromone

در مدل TBSI که به‌منظور رفع مشکلات پروتکل لیچ ارائه شده است، حوزه‌ای که گره مخرب می‌تواند حمله خود را انجام دهد، محدود به بلوکی می‌شود که در آن قرار می‌گیرد؛ اما در مورد حمله کرم‌چاله که گره مخرب، داده‌ها را برای گره دیگری به‌جز چاهک قانونی شبکه ارسال کند گره‌های دیگر به‌سرعت میزان اعتماد به این گره را به صفر تغییر می‌دهند و آن گره سریعاً بلوکه می‌شود. انتظار می‌رود گره سرخوشه، قواعد بازی را رعایت کند و چنانچه گره‌ای، داده‌ها را برای گره دیگری به جز چاهک قانونی شبکه ارسال کند، قواعد بازی را رعایت نکرده و به‌عنوان گره متخلف شناسایی می‌شود. با این تفصیل، مدل اعتماد پیشنهادی سربار زیادی را به شبکه تحمیل نمی‌کند، هرچند که برای گره‌ها سربار محاسباتی را به همراه دارد.

۴- ارزیابی مدل TBSI

۴-۱- پارامترهای شبیه‌سازی

برای تحلیل مدل TBSI، سه سناریوی مختلف بررسی می‌شود که در هر سناریو تعداد گره‌ها دو برابر سناریو قبلی است درحالی‌که بقیه پارامترهای معرفی‌شده در جدول (۱) در همه سناریوها ثابت هستند. در جدول (۱) مقادیر پارامترهای سناریوها مطرح شده و در جدول (۲) تعداد گره‌های هر سناریو بیان می‌شود.

جدول (۱): پارامترهای شبیه‌سازی جهت مقایسه پروتکل‌های TLSRP، LEACH و مدل TBSI

پارامترهای شبیه‌سازی	مقادیر
نوع صف	Taildrop
اندازه شبکه	۱۰۰ ×۱۰۰ مترمربع
آنتن	همه‌جهته[1]
زمان شبیه‌سازی	۱۰۰۰ ثانیه
تعداد نقطه‌های دسترسی (چاهک)	۱ نقطه دسترسی
موقعیت نقطه دسترسی	تصادفی
انرژی اولیه نقطه دسترسی	۱۰۰ ژول
محدوده انتقال	۱۰۰ متر
موقعیت گره‌ها	تصادفی
انرژی اولیه گره‌ها	۵ ژول
محدوده انتقال گره‌ها	۵۰ متر
فاصله‌های حس‌کردن	۵ ثانیه
طول صف	۵۰
باتری	مدل انرژی

جدول (۲): تعداد گره‌های هر سناریو

سناریو	سناریو اول	سناریو دوم	سناریو سوم
تعدادگره‌ها	۵۰	۱۰۰	۲۰۰

برای شبیه‌سازی و ارزیابی کارایی مدل TBSI از نرم‌افزار شبیه‌سازی NS-2 استفاده می‌شود. نتایج به‌دست‌آمده از مدل TBSI را با نتایج شبیه‌سازی‌های الگوریتم‌های TLSRP و لیچ مورد مقایسه قرار گرفته می‌شوند. تمامی گره‌های حسگر دارای شعاع حس و شعاع انتشار رادیویی یکسانی هستند. در تمام سناریوها تعداد گره‌های مخرب ۵٪ تعداد کل گره‌ها است. انرژی اولیه تمامی گره‌ها ثابت در نظر گرفته می‌شود. در این شبکه هیچ‌گونه تحرکی برای گره‌ها در نظر گرفته نشده و از مدل انرژی موجود در NS-2 استفاده شده است.

۴-۲- نتایج شبیه‌سازی

برای شبیه‌سازی، دو نوع گره مخرب در نظر گرفته می‌شود:

۱- گره خودخواه: گره‌ای که به‌خاطر حفظ منابع خود، داده را جذب ولی ارسال نمی‌کند.
۲- گره خرابکار: گره‌ای که یا داده را برای یک گره سوم می‌فرستد و یا داده را جذب کرده و چیزی نمی‌فرستد و نیز می‌تواند فقط یک قسمت از داده را به‌دلخواه ارسال کند.

در این مقاله، ۳ سناریو با تعداد گره‌های متفاوت برای اطمینان از صحت عملکرد مدل خود در نظر گرفته می‌شود که در همه آن‌ها ۵٪ گره خرابکار وجود دارد. نتایج شبیه‌سازی صحت عملکرد مدل TBSI را به‌وضوح نشان می‌دهد.

۴-۲-۱- مرگ اولین گره

در این بخش به بررسی زمان مرگ اولین گره پرداخته می‌شود. هرچقدر این مقدار کوچک‌تر باشد، یعنی انرژی گره سریع‌تر تمام شده و توزیع بار به شکل مناسبی انجام نمی‌شود. تحلیل بر این است که این امر دو علت متفاوت دارد. علت اول، احتمال تشکیل خوشه با حجم بالای تعداد گره بوده و علت دوم احتمال اینکه توزیع خوشه‌ها طوری باشد که گره نتوانسته برای چندین دور به عضویت خوشه‌ای درآمده باشد. لازم به ذکر است با توجه به عدم اتمام انرژی گره‌ها با ۵ ژول انرژی در مدت‌زمان اجرای شبیه‌سازی، انرژی اولیه گره‌ها در این بخش را ۰/۱ ژول در نظر گرفته می‌شود. جدول (۳)، زمان مرگ اولین گره در سناریوهای مختلف را نشان می‌دهد.

1- Omni Directional

جدول (۳): مرگ اولین گره در سناریوهای مختلف در واحد ثانیه

	سناریو اول	سناریو دوم	سناریو سوم
LEACH	۳۷/۸۱۲۵	۳۰/۵۹۷۲	۲۵/۴۸۱۵۶
TBSI	۴۲/۳۵۴۹	۳۸/۷۲۰۵۶	۳۸/۲۶۰۰۸

۴-۲-۲- مرگ آخرین گره

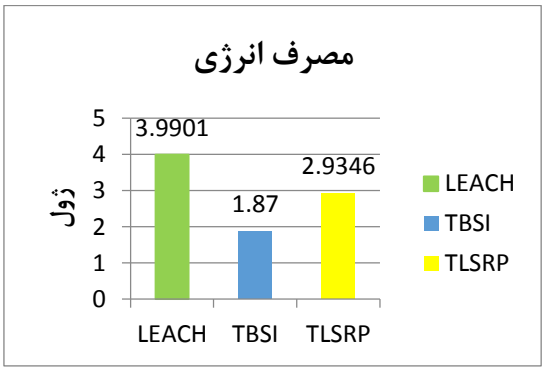
این بخش به مرگ آخرین گره‌ای تعلق دارد که داده‌های خود را به‌تنهایی برای گره چاهک یا ایستگاه پایه ارسال می‌کند. هرچه انرژی آخرین گره دیرتر تمام شود، به این معنی است که طول عمر شبکه حسگر طولانی‌تر بوده است. به همین دلیل از این پارامتر به‌عنوان طول عمر شبکه نیز می‌توان نام برد. لازم به ذکر است در این بخش نیز به‌مانند بخش قبلی، با توجه به عدم اتمام انرژی گره‌ها با ۵ ژول انرژی در مدت‌زمان اجرای شبیه‌سازی، انرژی اولیه گره‌ها را ۰/۱ ژول در نظر گرفته می‌شود. جدول (۴)، زمان مرگ آخرین گره در سناریوهای مختلف را نشان می‌دهد.

جدول (۴): مرگ آخرین گره در سناریوهای مختلف در واحد ثانیه

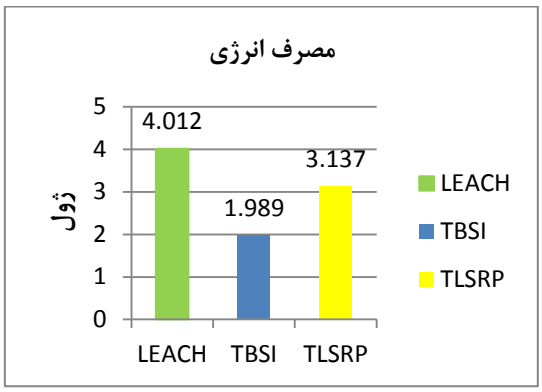
	سناریو اول	سناریو دوم	سناریو سوم
LEACH	۲۳۸/۰۶۵۳	۲۰۴/۹۸۰۳	۱۹۱/۳۷۲۴
TBSI	۳۳۶/۵۸۰۰۱	۳۵۱/۰۶۵۹	۲۶۳/۹۱۴

۴-۲-۳- مصرف انرژی

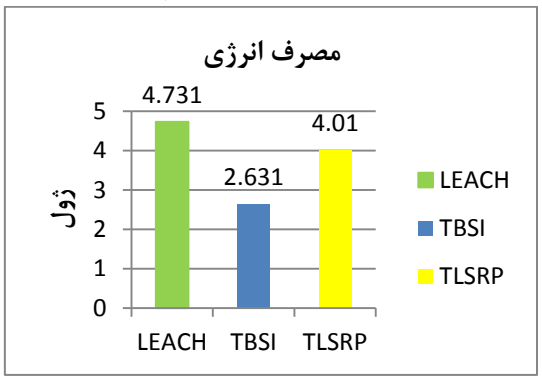
در این بخش میزان مصرف انرژی[1] گره‌ها بررسی می‌شود. محاسبه مرگ آخرین گره، به معنای مصرف انرژی کامل تمامی گره‌ها است. در این شبیه‌سازی‌ها انرژی اولیه گره‌ها برابر با پنج ژول در نظر گرفته می‌شود. سپس از فایل‌های خروجی شبیه‌ساز، اطلاعات به شرح زیر استخراج می‌شود. شکل‌های ۵، ۶ و ۷ این اطلاعات را نشان می‌دهند.



شکل (۵): مصرف انرژی در سناریو اول با ۵۰ گره



شکل (۶): مصرف انرژی در سناریو دوم با ۱۰۰ گره

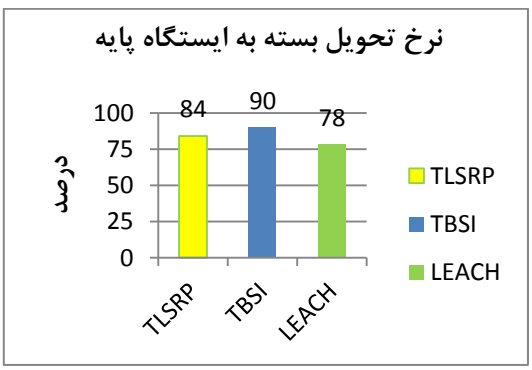


شکل (۷): مصرف انرژی در سناریو سوم با ۲۰۰ گره

۴-۲-۴- نرخ تحویل

نرخ تحویل[2]، تعداد بسته‌هایی است که با موفقیت در مقصد دریافت می‌شوند. برای محاسبه نرخ تحویل، اقدام به محاسبه نسبت تعداد بسته‌های دریافتی در مقصد بر تعداد بسته‌های ارسالی بر اساس رابطه (۳) می‌کنیم؛ اما توجه به این موضوع ضروری است که فقط تعداد بسته‌های ارسالی و دریافتی داده در لایه کاربرد محاسبه می‌شوند، چراکه در این لایه بسته‌های دیگری هم ارسال می‌گردند. شکل‌های (۸-۱۰) نتایج این محاسبات را نشان می‌دهند.

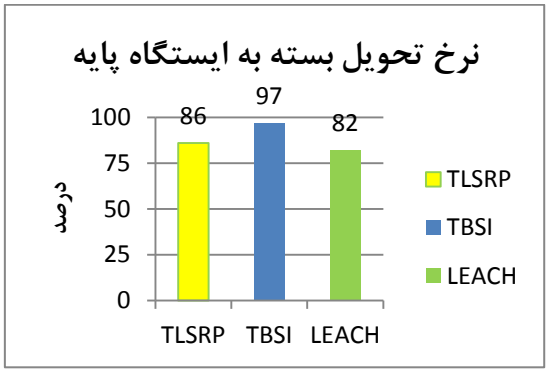
$$\text{pdf} = \frac{\text{Number of received lines}}{\text{Number of send lines}} \qquad (۳)$$



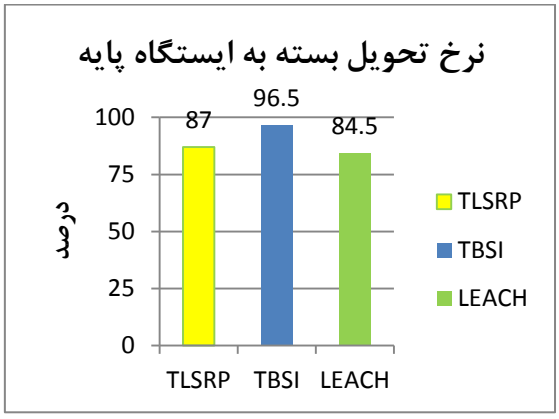
شکل (۸): نرخ تحویل بسته به ایستگاه پایه در سناریو اول با ۵۰ گره

1- Energy Consumption

2- Packet Delivery



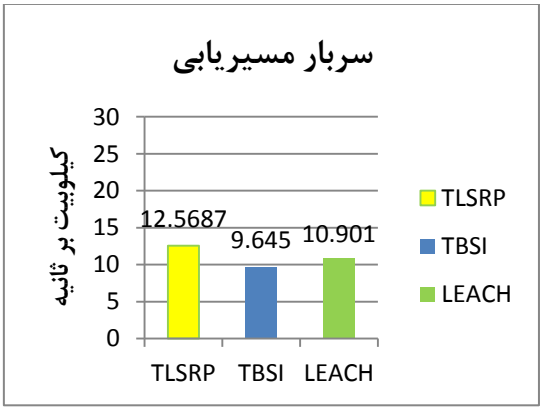
شکل (۹): نرخ تحویل بسته به ایستگاه پایه در سناریو دوم با ۱۰۰ گره



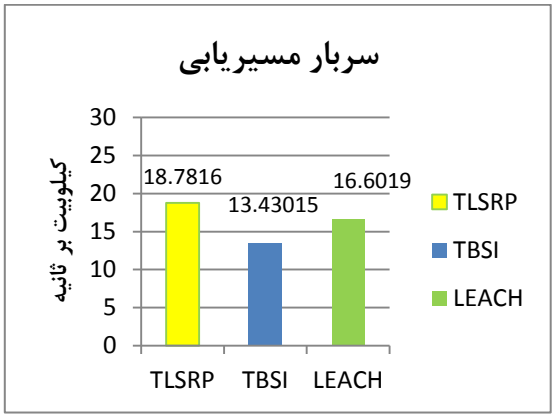
شکل (۱۰): نرخ تحویل بسته به ایستگاه پایه در سناریو سوم ۲۰۰ گره

۴-۲-۵- سربار مسیریابی

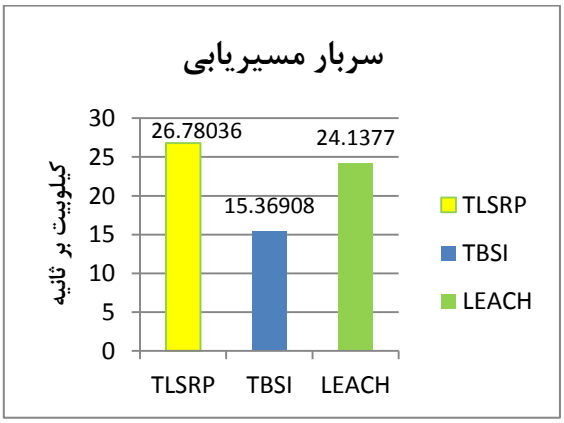
در این بخش، سربار مسیریابی[1] محاسبه می‌شود. این سربار برابر با نسبت تعداد بسته‌های ارسالی برای ارسال یک بسته اطلاعاتی است. این پارامتر صرفاً برای لایه کاربرد محاسبه می‌شود؛ یعنی نسبت میزان حجم بسته‌های داده را بر میزان حجم اطلاعات ارسالی برای تشکیل خوشه‌ها و تحمل‌پذیری خطا محاسبه می‌شود. شکل‌های ۱۱، ۱۲ و ۱۳ نتایج این محاسبات را نشان می‌دهند.



شکل (۱۱): سربار مسیریابی در سناریو اول با ۵۰ گره



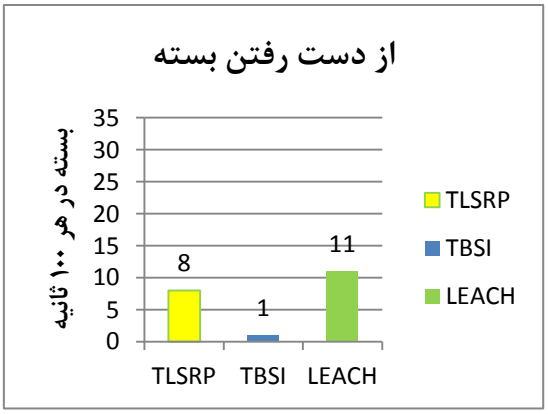
شکل (۱۲): سربار مسیریابی در سناریو دوم با ۱۰۰ گره



شکل (۱۳): سربار مسیریابی در سناریو سوم با ۲۰۰ گره

۴-۲-۶- از دست‌رفتن بسته

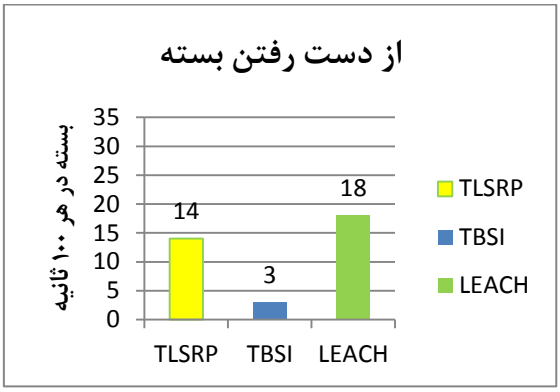
تعداد بسته‌هایی که گم می‌شود[2]، با افزایش تأخیر نیز افزایش می‌یابد و همان‌طور که در شکل‌های ۱۴، ۱۵ و ۱۶ دیده می‌شود مدل TBSI، نرخ گم‌شدن بسته‌ها را به علت بلوکه‌کردن گره‌های مخرب به‌طور چشم‌گیری کاهش می‌دهد. از طرفی ازآنجاکه نرخ تأخیر به دلیل خوشه‌بندی سریع‌تر کاهش داده شده است داده‌های بیشتری جمع‌آوری می‌شود.



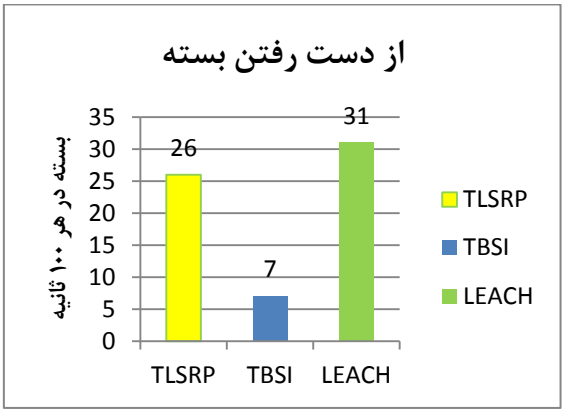
شکل (۱۴): از دست رفتن بسته در سناریو اول با ۵۰ گره

1- Routing Overhead

2- Packet Loss



شکل (۱۵): از دست رفتن بسته در سناریو دوم با ۱۰۰ گره



شکل (۱۶): از دست رفتن بسته در سناریو سوم با ۲۰۰ گره

۵- نتیجه‌گیری

در این مقاله، یک مدل اعتماد مبتنی بر الگوریتم‌های هوش جمعی معرفی و با دو پروتکل لیچ و TLSRP مقایسه شده است. با توجه به سادگی الگوریتم خوشه‌بندی لیچ، از آن برای خوشه‌بندی گره‌ها استفاده شده است. البته نقطه ضعف‌های آن نیز در این مقاله مطرح و برطرف گردید. از جمله این نقطه ضعف‌ها که توسط مدل پیشنهادی برطرف شدند، می‌توان به عدم توزیع مناسب خوشه‌ها در شبکه، عدم در نظر گرفتن انرژی باقی‌مانده گره‌ها، عدم توزیع مناسب تعداد اعضای خوشه و نیز عدم انتخاب سرخوشه در یک یا چند دور اشاره نمود. در مدل پیشنهادی با تقسیم‌بندی شبکه به قطعه‌های مختلف و تشکیل خوشه داخل هر قطعه، مشکل عدم توزیع مناسب خوشه‌ها در شبکه حل شده است. همچنین با ارسال انرژی باقی‌مانده توسط گره‌ها در انتهای هر دور، میزان انرژی باقیمانده در گره‌ها موردتوجه قرار می‌گیرد. از سوی دیگر با تقسیم شبکه به قطعه‌های مختلف، مشکل عدم توزیع مناسب تعداد اعضای خوشه‌ها نیز رفع گردید.

ازآنجاکه پروتکل لیچ صرفاً برای خوشه‌بندی انتخاب شده است، لذا مدل TBSI جداگانه با این پروتکل از دیدگاه مرگ اولین و آخرین گره مقایسه شده است. یکی از اهداف این مقاله دست‌یابی به مصرف نسبتاً یکنواخت‌تر انرژی در کل شبکه بوده که بر اساس بخش‌های ۴-۲-۱ تا ۴-۲-۳ به این هدف رسیده شده است.

در قسمت دوم مدل TBSI، هدف ارائه یک مدل اعتماد بود. مدل TBSI از این لحاظ با پروتکل‌های لیچ و TLSRP مقایسه شده است که پارامترهای بررسی‌شده برتری مدل TBSI را نسبت به این دو پروتکل نشان می‌دهد. اشاره به این نکته ضروری است که در مدل TBSI، همه گره‌ها بر مشاهدات مستقیم خود تکیه می‌کنند. در نتیجه ارائه گزارش برای گره‌های دیگر لزومی ندارد، چراکه هر گره به‌صورت مستقیم فقط با گره‌های درون خوشه خود در ارتباط است. مهم‌ترین مزیت مدل TBSI، توزیع مناسب خوشه‌ها در شبکه و نیز امکان رشد خوشه‌ها در فاصله‌های طولانی‌تر است (که احتمال کم‌چگال‌شدن توزیع گره‌ها در آن فاصله‌ها بالاست). سربار بسیار کم خوشه‌بندی و خوشه‌بندی سریع گره‌ها در هر دور از مزایای دیگر این مدل محسوب می‌شود. نظریه بازی، کار نظارت بر سرخوشه‌ها را انجام می‌دهد نظارتی که به‌واسطه آن، سازوکار اعتمادسنجی و تحمل‌پذیری خطا توأمان اعمال می‌گردد. درصورتی‌که به هر دلیل سرخوشه نتواند داده‌های خود را برای گره چاهک ارسال کند، گره‌ها با شناسایی این رفتار، داده‌های خود را برای سرخوشه بعدی در دور بعد هم مجدد ارسال می‌کنند. البته بار بیشتری هم در دور بعد به سرخوشه وارد می‌گردد. مزیت دیگر امکان افزایش اعتماد به گره‌ای است که رفتار مناسب از خود نشان می‌دهد.

همچنین در مدل TBSI، رویکرد تک‌جهشه برای ارسال داده‌ها مورد استفاده قرار گرفته است. نقطه‌ضعف این مدل در واقع همین رویکرد است که مسئله مقیاس‌پذیری شبکه را زیر سؤال می‌برد. البته این مسئله با استفاده از رویکرد چندجهشه که همان تبادل داده بین سر خوشه‌ها است به‌راحتی قابل‌حل است.

پیشنهاد می‌شود که مدل ارائه‌شده در این مقاله برای حالت‌هایی که گره‌ها قابلیت جابه‌جایی داشته باشند و همچنین حالتی که از چندین گره چاهک استفاده می‌شود توسعه داده شود. از طرف دیگر با شناسایی مناطقی که انرژی گره‌ها در آن‌ها رو به اتمام است گره چاهک به آن خوشه‌ها نزدیک‌تر شود و امکان ذخیره انرژی را به گره‌های آن خوشه بدهد.

۶- منابع

[1] J. Lopez, R. Roman, I. Agudo, and C. Fernandez-Gago, "Trust management systems for wireless sensor networks: Best practices," Computer Communications, vol. 33, pp. 1086-1093, 2010.

[2] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in Proceedings of the 33rd annual Hawaii international conference on System sciences, pp. 1-10, 2000.

[3] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs," in Transactions on Dependable and Secure Computing, IEEE, vol. 9, pp. 184-197, 2012.

[4] S. S. Babu, A. Raha, and M. K. Naskar, "Trustworthy Route formation Algorithm for WSNs," International Journal of Computer Applications (0975–8887), vol. 27, 2011.

[5] T. Zahariadis, H. Leligou, P. Karkazis, P. Trakadas, I. Papaefstathiou, C. Vangelatos, et al., "Design and implementation of a trust-aware routing protocol for large WSNs," International Journal of Network Security and Its Applications (IJNSA), vol. 2, pp. 52-68, 2010.

[6] C. Weifang, L. Xiangke, S. Changxiang, L. Shanshan, and P. Shaoliang, "A trust-based routing framework in energy-constrained wireless sensor networks," in Wireless Algorithms, Systems, and Applications, ed: Springer, pp. 478-489, 2006.

[7] A. A. Pirzada and C. McDonald, "Trusted greedy perimeter stateless routing," in 15th IEEE International Conference on Network ICON, pp. 206-211, 2007.

[8] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks," in IEEE International Conference on Performance, Computing, and Communications, pp. 463-469, 2004.

[9] S. M. Hosseini and A. Rezaei, "Energy Optimization in WSNs with Hybrid Algorithm," in The First National Conference on Interdisciplinary Reseaches in Computer, Electrical, Mechanical and Mechatronics Engineering, 2016 (In Persian).

[10] S. Nasirian and F. Faghani, "A novel hierarchical routing algorithm for wireless sensor networks in order to reduce energy consumption and increase network lifetime using a tree-sector structure," in 2nd National Conference On Computer Engineering and IT Management, 2015 (In Persian).

Journal of Electronical & Cyber Defence
Vol. 7, No. 1, 2019, Serial No. 25

A Trust Model Based on Swarm Intelligence Algorithms in WSNs

A. Khosravi, A. Karimi*, M. A. Javadzadeh, M. J. Khosravi

*Imam Hossein University
(Received: 06/06/2017, Accepted: 06/01/2018)

ABSTRACT

Most applications of sensor nodes are in hazardous areas, inaccessible or hostile environments. Therefore, the need for security in these networks is essential. Trust methods are powerful tools for diagnosing unexpected behavior of nodes (malicious nodes or failure nodes). In this paper, we have proposed TBSI trust model whose main features are low computational overhead, low energy consumption and confronting attacks in WSNs. This model is simulated and evaluated by NS-2 simulator and its behavior has been evaluated based on the results of these simulations. Examining practical results shows that energy consumption, routing overhead, and the time of death of nodes are reduced and the rate of packet delivery to the base station is increased. These desirable outcomes prove that using the method of trust to achieve a secure network is a good solution to solve security issues in wireless sensor networks.

Keywords: Wireless Sensor Network, Trust, Routing, Network Attack

*Corresponding Author Email: a.karimi@ihu.ac.ir