دوره چهاردهم، شماره دوم، پاییز و زمستان ۱۴۰۰
مجله فناوری اطلاعات در طراحی مهندسی
Information Technology in Engineering Design
http://ited.sinaweb.net

# مسیریابی مبتنی بر اعتماد پویا و پنجره‌ی لغزان بهبودیافته در شبکه‌های حسگر بی‌سیم

موهبه سادات کاتبی[۱] حسن شاکری[۲*] فرزاد تشتریان[۳]

[۱] گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران
[۲] گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران*
[۳] گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران

(تاریخ دریافت : ۱۴۰۱/۰۴/۰۳ تاریخ پذیرش : ۱۴۰۱/۰۶/۱۷)

**چکیده**

همان‌طورکه اعتماد بین انسان‌ها حاصل تجربیاتی است که از ارتباط مستقیم با یکدیگر داشته‌اند و یا درصورت عدم وجود رابطه مستقیم، از پیشنهادهای افراد مورد وثوق برای برقراری یک رابطه جدید استفاده می‌کنند؛ در دنیای شبکه‌های مختلف نیز هر موجودیتی برای ایجاد یک ارتباط، نیاز به آگاهی از قابلیت اعتماد طرف مقابل خود دارد. بر این اساس، این تحقیق به مطالعه و مدلسازی اعتماد در شبکه‌های حسگر بی‌سیم پرداخته و جهت حصول نتایج دقیق‌تر، از پارامترهایی چون باقیمانده‌ی انرژی، میزان تعاملات موفق و ناموفق، فاصله‌ی زمانی دریافت و ارسال بسته توسط گره‌ها و مدارکی دیگر استفاده می‌نماید. لذا هدف تحقیق حاضر آن است که در شبکه‌های حسگر بی‌سیم، به ارائه یک مدل اعتماد به شکل پویا، شامل انواع مستقیم و غیرمستقیم و با رویکرد واکنشی پرداخته و علاوه‌برآن، میزان اطمینان به اعتماد حاصل‌شده را نیز بررسی نماید. رویکردهای اصلی این تحقیق، بکارگیری مدل منطق ذهنی در محاسبه‌ی اعتماد و ارائه‌ی یک ساختار پنجره‌ی لغزان بهبود یافته برای بازنمایی و مدیریت بهینه اطلاعات موجود می‌باشد. نتایج شبیه‌سازی راهکار پیشنهادی در مقایسه با مدل شناخته‌شده EDTM حاکی از افزایش ۱۱,۹۹٪ در انرژی باقیمانده‌ی شبکه و رشد ۱,۵۲٪ در دقت تشخیص گره‌های مخرب می‌باشد.

**واژه‌های کلیدی:** اعتماد – شبکه‌ی حسگر بی‌سیم – مدل منطق ذهنی – پنجره‌ی لغزان – اطمینان

* عهده دار مکاتبات:
حسن شاکری
نشانی: **گروه مهندسی کامپیوتر، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران**
پست الکترونیک: hassan.shakeri@gmail.com

## ۱. مقدمه

امروزه شبکه‌های حسگر بی‌سیم در همه‌جا گسترده شده‌اند. کاربرد این شبکه‌ها ازجمله در زمینه‌هایی چون تشخیص آتش‌سوزی در جنگل، تشخیص زمین لرزه، نظارت بر فشارخون بیماران، نظارت بر رطوبت هوا، نظارت بر سرعت خودرو، تشخیص مواد شمیایی و گازهای سوزآور، تشخیص هدف در عملیات نظامی و غیره می‌باشد.

از طرف دیگر به تبع افزایش کاربرد شبکه‌های حسگر بی‌سیم، این شبکه‌ها در معرض بسیاری از حملات امنیتی قرار دارند، برای تأمین امنیت این شبکه‌ها لازم است روش‌های امنیتی جدید جایگزین روش‌های قدیمی شوند. تخمین و برقراری اعتماد بین گره‌ها یکی از رویکردهای کارآمد در این راستا محسوب می‌شود.

به‌صورت کلی می‌توان گفت برقراری اعتماد در شبکه‌های حسگر بی‌سیم با دو هدف عمده انجام می‌گیرد: بهبود همکاری و افزایش امنیت [۱]. چرا که همکاری بین گره‌های حسگر در شبکه‌های حسگر بی‌سیم، برای حفظ بهره‌برداری از شبکه، یک نقش حیاتی دارد.

ویژگی‌هایی که معمولاً برای حصول اعتماد مورد ارزیابی قرار می‌گیرند مواردی چون داده، انرژی و یا رفتارهای ارتباطی می‌باشند، اما هنوز جنبه‌های دیگری همچون فاصله‌ی زمانی ارسال و دریافت بسته‌ها در این محیط وجود دارد که اعتماد را تحت تأثیر قرار می‌دهد. همچنین نباید از تأثیر مقادیر بدست‌آمده‌ی مقادیر اعتماد در گذشته، غفلت داشت؛ چرا که استفاده از این مقادیر می‌تواند باعث تخمین دقیق‌تر مقدار اعتماد گردد. بنابراین می‌توان با به‌کارگیری پنجره‌ی لغزان و استفاده از ضریب تأثیر سابقه در آن، به این هدف دست یافت.

همچنین وجود ویژگی بسیار مهم عدم قطعیت در این نوع شبکه‌ها، تأثیری قابل ملاحظه برروی کارکرد آن داشته و با بهره‌بردن از نتایج آن، می‌توان دقت مقادیر ارزیابی‌شده‌ی اعتماد را افزایش داد.

در این مقاله مدل جدیدی با هدف بهبود مسیریابی در شبکه‌های حسگر بی‌سیم ارائه می‌کنیم. مدل پیشنهادی از نظریه منطق ذهنی برای بازنمایی و محاسبه اعتماد گره‌های شبکه به یکدیگر و نیز اطمینان به تخمین اعتماد استفاده می‌کند. همچنین جهت حصول نتایج دقیق‌تر، پارامترهایی چون باقیمانده‌ی انرژی، میزان تعاملات موفق و ناموفق، فاصله‌ی زمانی دریافت و ارسال بسته توسط گره‌ها در تصمیم‌گیری نهایی برای انتخاب مسیر مورد استفاده قرار می‌گیرد. هدف مقاله ارائه یک مدل اعتماد به شکل پویا، شامل انواع مستقیم و غیرمستقیم و با رویکرد واکنشی است و علاوه‌برآن، میزان اطمینان به اعتماد حاصل‌شده محاسبه و اعمال می‌گردد.

ساختار این مقاله در ادامه به صورت زیر است: در بخش ۲ کارهای تحقیقاتی مرتبط مرور و بررسی می‌شود. در بخش ۳ راهکار پیشنهادی معرفی می‌گردد و در ادامه بخش ۴ به رویکرد شناسایی گره‌های بدخواه در راهکار پیشنهادی می‌پردازد. در بخش ۵ نتایج ارزیابی مبتنی بر شناسایی و در بخش ۶ تحلیل کارایی و دقت راهکار پیشنهادی ارائه می‌گردد و بالاخره بخش ۷ به نتیجه‌گیری و پیشنهادها برای ادامه کار اختصاص دارد.

۲. کارهای مرتبط

در زمینه مسیریابی مبتنی بر اعتماد در شبکه‌های حسگر بی‌سیم کارهای تحقیقاتی مختلفی به ویژه در سال‌های اخیر ارائه شده است. در این بخش، تعدادی از مهم‌ترین کارهای ارائه‌شده در این حوزه مورد بررسی قرار می‌گیرد.

طی تحقیقی که در سال ۲۰۰۶ با موضوع ساده‌سازی و آنالیز شبکه‌های اعتماد متعدی انجام شد [۲]، نظریه‌ی منطق ذهنی توسط Josang و همکاران مطرح گردید. در این مدل، یک نظر اعتماد به صورت یک سه‌گانه (b, d, u) ارائه می‌شود که در آن b، d و u به ترتیب میزان باور[۱]، بی‌باوری[۲] و عدم قطعیت را در مورد اعتماد نشان می‌دهند و $b + d + u = 1$. پس از ارائه‌ی این پژوهش، نظریه‌ی منطق ذهنی، به یکی از معروف‌ترین روش‌های بازنمایی اعتماد تبدیل شد.

در سال ۲۰۱۱، Feng و همکاران، الگوریتمی برای ارزیابی اعتماد شبکه‌های حسگر بی‌سیم برمبنای رفتار گره‌ها و نظریه‌ی شواهد D-S[۳] پیشنهاد دادند. این تحقیق، روش‌های رفتاری گره‌ها و نظریه‌ی گواهی را ادغام می‌کند. برطبق رفتار گره‌های حسگر، چندین معیار گوناگون اعتماد و عوامل مشترک مرتبط با کاربرد شبکه، برای بدست‌آوردن مقادیر اعتماد مستقیم و غیرمستقیم، از طریق محاسبه‌ی میانگین معیارهای اعتماد، استقرار یافته‌اند. ضمناً، روش مجموعه فازی، برای تشکیل بردار ورودی اصلی گواهی، مورد استفاده قرارگرفته است. براین اساس، تفاوت مدارک بین مقادیر اعتماد مستقیم و غیرمستقیم، محاسبه می‌شوند که قانون ترکیب گواهی D-S تجدیدنظرشده را به مقدار نهایی اعتماد، پیوند می‌دهد [۳].

Bao و همکاران [۴] در سال ۲۰۱۲، پیشنهادی با عنوان مدیریت اعتماد مرتبه‌ای برای شبکه‌های حسگر بی‌سیم و کاربرد آن در مسیریابی مبتنی بر اعتماد و تشخیص نفوذ، ارائه دادند. در این پژوهش شبکه‌ی حسگر بی‌سیم خوشه‌بندی شده مدّنظر قرارگرفته است. با درنظرداشتن شبکه‌ای دوسطحی، این پروتکل مدیریت اعتماد با استفاده از ارزیابی دوره‌ای اعتماد نقطه به نقطه بین دو گره و نیز بین دو سرخوشه اداره می‌شود.

در سال ۲۰۱۳، Li و همکاران [۵] یک سیستم اعتماد قابل اطمینان و سبک‌وزن را برای شبکه‌های حسگر بی‌سیم خوشه‌بندی شده ارائه کردند. در این مقاله اعتماد در دو سطح کلی درون خوشه‌ای و بین خوشه‌ای مورد بررسی قرار گرفته است. در سطح درون خوشه‌ای به محاسبه‌ی اعتماد در دو شاخه‌ی اعتماد بین اعضای خوشه و اعتماد بین اعضای خوشه و سرخوشه پرداخته‌اند. در سطح بین خوشه‌ای اعتماد در دو شاخه‌ی اعتماد بین سرخوشه‌ها و اعتماد بین سرخوشه و ایستگاه مرکزی محاسبه می‌شود.

Geetha و همکاران در سال ۲۰۱۴ با معرفی یک چارچوب ارتباط امن مبتنی براعتماد، یک سیستم مدیریت اعتماد را برای شبکه‌های حسگر بی‌سیم طراحی کردند [۶]. این سیستم در چندلایه پیاده‌سازی شده و شامل مولفه‌هایی چون مدیریت

---

[۱] Belief

[۲] Disbelief

[۳] Dempster-Shafer Theory

اعتماد، ذخیره‌سازی اطلاعات و کاربرد اعتماد می‌باشد. در این مقاله، برای اعتماد هفت معیار ارتباط، داده، عاملیت[۱]، موقعیت، انرژی، زمان به‌روزرسانی و احتمال زیان و ضرر، مورد ارزیابی قرار گرفته است.

در طرحی جدید که توسط Zhang و همکاران در سال ۲۰۱۴ ارائه شد، یک چارچوب مدیریت اعتماد چندسطحی برای شبکه‌های حسگر بی‌سیم ایجاد گردید [۷]. این مدل، از سه سطح اعتماد برای برقراری ارتباط مبتنی بر اعتماد بین گره‌ها استفاده می‌کند. سطح اول، یک اعتماد نظری است که به عنوان اعتقاد[۲] و یا باور معرفی شده و سه جنبه از اعتقاد را دربرمی‌گیرد: ۱. داوری‌های گذشته، ۲.گواهی شاهد[۳] و ۳. ارزیابی توانایی. سطح دوم، اعتماد عینی[۴] است که با درنظر گرفتن دو مشخصه، به عنوان اعتبار معرفی شده است. مشخصه‌ی اول تعداد جوامع دایر[۵] و مشخصه‌ی دوم داوری وزن‌دارشده از طریق رتبه‌بندی اعتبار گره است. در این سطح، همچنین یک سری قوانین و تست فاکتور تقلب معرفی شده‌اند که از درجه‌بندی اعتبار توسط گره‌های مخرب، جلوگیری می‌کنند. سطح سوم، روش اعتماد توصیه شده است که برای بدست آوردن نظرات قابل اعتماد از توصیه‌های ناشناس معرفی شده است که شامل چندین مشخصه‌ی سازگاری برای تعیین قابلیت اعتماد توصیه‌ها می‌باشد.

در پژوهشی که در سال ۲۰۱۵ انجام شد، Ahmed و همکاران [۸] یک پروتکل مسیریابی آگاه از اعتماد برای شبکه‌های حسگر بی‌سیم با محدودیت انرژی معرفی کردند که از مدل اعتماد توزیع‌شده برای تشخیص و جداسازی گره‌های بدرفتار استفاده می‌کند. این مدل، از یک تابع مسیریابی مرکب که شامل اعتماد، باقیمانده‌ی انرژی و تعداد بندهای گره‌های همسایه می‌باشد، برای تصمیم‌گیری در مسیریابی استفاده می‌کند. به گفته‌ی نویسندگان این مقاله، این مدل مسیریابی چندبندی، در مسیریابی داده‌ها، با استفاده از مسیرهای کوتاه‌تر به تعادل مصرف انرژی در میان گره‌های مورد اعتماد، کمک می‌کند.

در سال ۲۰۱۵، Fang و همکاران [۹] یک سیستم ارزیابی شهرت و اعتماد مبتنی بر B برای شبکه‌های حسگر بی‌سیم ارائه نمودند. این طرح برمبنای نظارت رفتار گره‌ها و توزیع بتا ایجاد شده و برای تشریح توزیع اعتبار گره‌ها مورد استفاده قرارمی‌گیرد. در این طرح، مقدار اعتماد گره که برای راهنمایی انتخاب یک گره کمکی استفاده می‌شود، تأثیر حملات داخلی را کاهش می‌دهد.

بنا بر تحقیق ارائه شده توسط Singh و همکارانش [۱۰] در سال ۲۰۱۵، یک مدل اعتماد سبک‌وزن برای شبکه‌های حسگر بی‌سیم خوشه‌بندی‌شده طراحی شده است. این مدل براساس ماهیت پویای مکانیسم ایجاد اعتماد واقعی برای مقابله با محدودیت منابع گره‌های حسگر کوچک، طراحی شده است. در این تحقیق همانند پژوهش Li و همکاران (مورد ۲)، مقدار اعتماد در دو بخش درون خوشه‌ای و بین خوشه‌ای مورد ارزیابی قرارمی‌گیرد با این تفاوت که در این تحقیق، برای اعتماد

---

[۱] Functionality

[۲] Belief

[۳] Witness Evidence

[۴] Objective Trust

[۵] Functioning Communities

معیارهایی از مشخصات QoS تعریف شده که برای هرکدام اولویتی درنظرگرفته‌شده‌اشت. از جمله معیارهای با اولویت بالا، پردازش پیام‌های بسته‌های کنترلی می‌باشد.

در یک روش جدید که بر پایه‌ی منطق فازی استوار است، Jadidoleslamy و همکاران [۱۱] در سال ۲۰۱۵ به ارائه‌ی یک سیستم مدیریت اعتماد کاملاً توزیع‌شده‌ی فازی برای شبکه‌های حسگر بی‌سیم با نام DTMS[۱] پرداخته‌اند. این روش بر پایه‌ی ۹ مرحله بنیان گذاشته شده است. مرحله‌ی اول: مقداردهی اولیه‌ی DTMS. مرحله‌ی دوم: تعریف محدودیت‌های طبیعت فازی محاسبه‌ی اعتماد مستقیم. مرحله‌ی سوم: جمع‌آوری اطلاعات مورد نیاز برای محاسبه‌ی اعتماد مستقیم و ایجاد ماتریس تصمیم‌گیری فازی. مرحله‌ی چهارم: تخصیص وزن‌های فازی به محدودیت‌های محاسبه‌ی اعتماد مستقیم طبیعت فازی. مرحله‌ی پنجم: نرمال‌سازی ماتریس تصمیم‌گیری فازی. مرحله‌ی ششم: تخصیص وزن‌های فازی به ماتریس تصمیم‌گیری فازی نرمال‌شده. مرحله‌ی هفتم: محاسبه‌ی قابلیت اعتماد یا پیش‌بینی قابلیت اعتماد. مرحله‌ی هشتم: تشخیص همسایگان مخرب، آسیب‌دیده[۲] و یا خودخواه[۳] و نهایتاً مرحله‌ی نهم: تکرار مراحل فوق و به‌روزکردن مقادیر اعتماد.

در سال ۲۰۱۵، Jiang وهمکارانش [۱۲] مدل اعتماد توزیع‌شده‌ای را برای شبکه‌های حسگر بی‌سیم با نام مخفف EDTM (Efficient Distributed Trust Model)، ارائه دادند. اعتماد مستقیم بین دو گره همسایه با استفاده از رابطه ۱ و اعتماد غیر مستقیم از رابطه‌های ۲ و ۳ محاسبه می‌شوند:

$$T_{n-direct} = W_{com}T_{com} + W_{ene}T_{ene} + W_{data}T_{data} \quad (۱)$$

که در آن، $W_{cam}$ ، $W_{ene}$ و $W_{data}$ به ترتیب وزن‌های مربوط به اعتمادهای ارتباط، انرژی و داده می‌باشد.

$$T_{n-indirect}\binom{B}{C_1} = \begin{cases} T_{C_1} * T_{c_1}^B, & if\ T_{c_1}^B < 0.5 \\ 0.5 + \left(T_{c_1} - 0.5\right) * T_{c_1}^B, & else \end{cases} \quad (۲)$$

$$T_{n-indirect}\binom{B}{C_{i+1}} = \begin{cases} T_{C_{i+1}} * T_{n-indirect}\binom{B}{C_i}, & if\ T_n \\ 0.5 + \left(T_{c_{i+1}} - 0.5\right) * T_{n-indire} \end{cases} \quad (۳)$$

ایده‌ی تجمیع تحمل‌پذیری خطا و روش مسیریابی امن برای شبکه‌های حسگر بی‌سیم، توسط طراحان مدل [۱۳] در سال ۲۰۱۶، جهت استقرار مسیری امن از منبع تا ایستگاه مرکزی حتی در شرایط وجود گره‌های خرابکار، ارائه شد. در این ایده، از مدل اعتماد مبتنی‌بر عامل استفاده شده است. همچنین، داده‌ها از مسیری امن و فاقد گره‌های بدخواه و یا گره‌های مصالحه‌کار، به ایستگاه مرکزی منتقل می‌شوند.

---

[۱] Distributed Trust Management System

[۲] Compromised

[۳] Selfish

در [۱۴] یک الگوریتم مسیریابی امن با انرژی بهینه به نام EOSR[۱] برای مقابله با حملات گره‌های داخلی در شبکه‌های حسگر بی‌سیم معرفی شده است. این الگوریتم برای شناسایی و منزوی‌کردن گره‌های مخرب از یک مدل ارزیابی اعتماد توزیع‌شده استفاده می‌کند. در EOSR یک راهبرد مسیریابی چندفاکتوری طراحی شده است که سطح اعتماد گره، انرژی باقیمانده و طول مسیر را در نظر می‌گیرد.

مرجع [۱۵] یک پروتکل مسیریابی مبتنی بر اعتماد تطبیقی با عنوان ATRP[۲] ارائه می‌کند که اعتماد مستقیم، اعتماد غیرمستقیم و اعتماد شاهد را ترکیب می‌کند و فاکتورهای متعدد مربوط به امنیت و منابع را در ارزیابی اعتماد در نظر می‌گیرد. سازوکار پیشنهادی در این مقاله امکان ارزیابی بیشتر در مورد گره‌های بالقوه در چندین گام را فراهم می‌آورد تا مصرف انرژی متوازن شود.

در [۱۶] برای حل چالش‌های ارائه یک پروتکل مسیریابی چندپخشی آگاه از انرژی، پروتکلی به نام CrowWhale-ETR ارائه شده است. در این پروتکل، ابتدا سطح اعتماد و انرژی گره‌ها برای برقراری مسیرهای انتخابی بهینه ارزیابی می‌شود. سپس مسیر بهینه انتخاب‌شده برای انتقال داده‌ها مورد استفاده قرار می‌گیرد و در پایان فرایند ارسال، انرژی و اعتماد گره‌های مسیر بروزرسانی می‌شود.

در مرجع [۱۷] یک پروتکل مبتنی بر مدیریت اعتماد و کم‌انرژی تطبیقی با خوشه‌بندی سلسله‌مراتبی به نام LEACH-TM ارائه شده است. این پروتکل از سرخوشه‌های پویا، انرژی باقی‌مانده و تراکم گره‌های همسایه استفاده می‌کند تا اندازه خوشه به صورت بهینه انتخاب شود و مصرف انرژی کارآمد گردد.

مرجع [۱۸] یک پروتکل مسیریابی مبتنی بر اعتماد ارائه می‌کند که برای برقراری مسیریابی امن قابل استفاده است. این پروتکل از الگوریتم بهینه‌سازی آکویلا برای انتقال امن اطلاعات در شبکه‌های حسگر بی‌سیم استفاده می‌کند. پروتکل مذکور با بهره‌گیری از یک تابع برازش شامل سه پارامتر انرژی باقی‌مانده، فاصله تا ایستگاه پایه و سطح اعتماد، یک مجموعه بهینه از مسیرها به ایستگاه پایه (BS) تعیین می‌کند.

در این مقاله، مدل جدیدی برای بهبود مدل EDTM ارائه می‌کنیم که در بخش‌های بعدی به معرفی و تشریح آن خواهیم پرداخت.

## ۳. معرفی روش پیشنهادی

### ۳-۱ کلیات راهکار ارائه‌شده

در این پژوهش، سیستم محاسبه‌ی اعتماد برروی شبکه‌های حسگر بی‌سیم با استفاده از ساختار بهبود یافته‌ی پنجره‌ی لغزان و مدل منطق ذهنی، معرفی شده است. نحوه‌ی محاسبه‌ی اعتماد براساس سه فاکتور باقیمانده‌ی انرژی، رفتار گره و زمان ارسال

---

[۱] Energy-optimized Secure Routing

[۲] Adaptive Trust-based Routing Protocol

و دریافت پیام، انجام می‌گیرد. جهت تشـخیص گره‌های مخرب و جلوگیری از انتخاب شـدن آن‌ها در فرآیند مسـیریابی، دو الگوریتم با هدف تشخیص دو نوع رفتار مختلف، معرفی شده است.

۳-۲ مدل توپولوژی شبکه

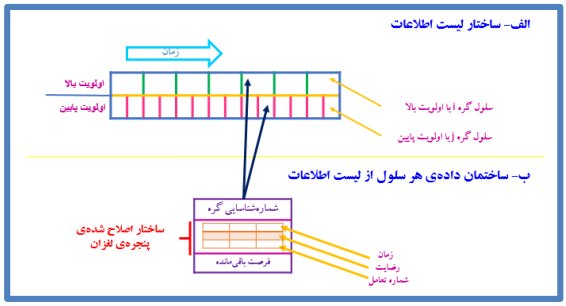
هر گره، لیسـتی از آخرین مقدار اعتماد گره‌های همسـایه‌ای که سـابقاً با آن‌ها تعامل داشـته است را در جدولی با نام «لیست اطلاعات» نگه‌داری می‌کند. سـاختمان این جدول شـامل طرح پیشنهادی اصلاح شده‌ی ساختار پنجره‌ی لغزان می‌باشد. برای ذخیره‌سـازی اعتماد، مقادیر آن در بازه‌ی (۱۵ – ۰) درنظر گرفته می‌شـود، این انتخاب، این مزیت را خواهد داشـت که محاسبه‌ی مقدار اعتماد با داشتن چنین بازه‌ای برای ذخیره‌سازی، سربار حافظه و ارتباطات را کاهش می‌دهد.

۳-۳ لیست اطلاعات و ارائه‌ی ساختار بهبودیافته‌ی پنجره‌ی لغزان

ساختار لیست اطلاعات حاوی دو سطح اولویت می‌باشد (شکل ۱ – الف). اولویت بالا با گره‌هایی است که میزان تعاملات بیشـتری با گره مبدأ دارند و بنابراین مقادیر آن‌ها در فاصـله‌ی زمانی بیشتری در پنجره باقی می‌ماند. به مابقی گره‌ها، اولویت پایین اختصاص داده می‌شود. پیاده‌سازی این لیست، این مزیت مهم و ارزنده را در بردارد که دیگر نیازی به همه‌پخشی مقدار اعتماد از سـوی ایسـتگاه مرکزی نخواهد بود و نیز گره‌ها ملزم نخواهند شـد مقادیر اعتماد را به اشـتراک گذارند. همچنین استفاده از این لیست، با کاهش در سربار ارتباطی شبکه، کارآیی منابع سیستم را افزایش می‌دهد.

ساختمان‌داده‌ی هر سلول از لیست اطلاعات شامل شماره‌شناسایی گره، پنجره‌ی لغزان و فرصت باقی‌مانده می‌باشد (شکل ۱- ب).

سـاختار پیشـنهادی پنجره‌ی لغزان نیز شـامل سه قلم داده می‌باشد. داده‌ها به ترتیب: زمان بدست آمدن اعتماد ($t_{trust}$)؛ مقدار اعتماد ($V_{trust}$) و شماره تعامل ($No_{int}$) است. (شکل ۱-ب).




شکل ۱ – الف- ساختار لیست اطلاعات و ب- ساختمان داده‌ی هر سلول از لیست اطلاعات

۳-۴ بررسی نحوه‌ی عملکرد مبتنی‌بر اعتماد شبکه در تعاملات

زمانی‌که گره A قصـد تعامل با گره B داشـته باشـد، چنانچه اطلاعات قبلی گره B در لیسـت اطلاعات وجود نداشته باشد، اطلاعات مورد نیاز از طریق گره‌های توصـیه‌گر حاصل می‌شوند و چنانچه اطلاعات گره B در لیست اطلاعات وجود داشته باشـد، اطلاعات گره B در مکان جدیدی متناسـب با زمان جاری قرارگرفته می‌شود. سناریوی این کار را می‌توان بدین شرح توضیح داد:

۱- گره شروع کننده(گره A)، گره مقصد(گره B) را که قصد تعامل با آن دارد، معین می‌کند.

۲- وجود یا عدم وجود آدرس گره B در لیست اطلاعاتی گره A بررسی می‌شود.

۲-۱ آدرس گره B در لیست اطلاعاتی گره A وجود دارد:

۲-۱-۱ اگر مقدار اعتماد قابل قبول نبود، گره A از تعامل با گره B صرف‌نظر می‌کند و تمام می‌شود.

۲-۱-۲ اگر مقدار اعتماد بازیابی شده از لیست اطلاعاتی قابل قبول باشد، زمان ثبت مقدار اعتماد با زمان کنونی مقایسه می‌شود.

۲-۱-۲-۱ اگر این فاصله‌ی زمانی قابل پذیرش بود، گره A اقدام به تعامل با گره B کرده و اطلاعات اعتماد گره B را با زمان کنونی در محل مناسب لیست اطلاعاتی درج می‌کند و تمام می‌شود.

۲-۱-۲-۲ اگر فاصله‌ی زمانی تا ثبت زمان قبلی اعتماد قابل پذیرش نباشد، به مرحله‌ی بعد می‌رود.

۲-۲ آدرس گره B در لیست اطلاعاتی گره A وجود ندارد و یا فاصله‌ی زمانی ثبت مقدار اعتماد در لیست اطلاعاتی قابل پذیرش نیست.

۲-۲-۱ گره A بسته‌ی درخواست پیشنهاد درمورد اعلام میزان اعتماد فردی هریک از گره‌های همسایه به گره B را به آن‌ها می‌فرستد و نظر آن‌ها را درمورد گره B جویا می‌شود.

۲-۲-۲ هرکدام از همسایگان نظر مستقیم یا غیرمستقیم خود را که براساس همین سناریو بدست آمده، به گره A می‌فرستند.

۲-۲-۳ گره A، نظرات بدست‌آمده را جمع‌آوری می‌کند. نظراتی که اعتمادی پایین‌تر از مقدار حد آستانه دارند، حذف می‌شوند.

۲-۲-۳-۱ اگر تعداد نظرات حذف شده، بیش از نصف بعلاوه یک تعداد کل نظرات باشد، نظر نهایی گره A درمورد گره B مبنی بر بی‌اعتمادی به آن گره خواهد بود و پردازش تمام می‌شود.

۲-۲-۳-۲ اگر تعداد نظرات حذف شده کمتر از نصف بعلاوه یک تعداد کل نظرات باشد، گره A بر اساس میزان اعتمادی که به اولین گره مابعد خود دارد، مقادیر نظرات بدست‌آمده را مرتب کرده و وزن‌دهی می‌کند. آنگاه میانگین جمع وزنی آن‌ها را محاسبه کرده و اگر نتیجه‌ی بدست‌آمده قابل قبول باشد مقدار جدید اعتماد گره B با زمان اعتماد بدست‌آمده در لیست اطلاعاتی نزد گره A ذخیره می‌شود. آنگاه گره A تصمیم به تعامل با گره B گرفته و مسیری را انتخاب می‌کند که بیشترین مقدار اعتماد را گزارش می‌کند. اگر بیش از یک مسیر، مقدار اعتماد یکسانی را اعلام کرده باشند، مسیر ایجاد تعامل مسیری خواهد بود که کمترین پرش را داشته باشد.

۴. شناسایی گره بدخواه

باتوجه به مفروضات مطرح شده، دو نوع گره بدخواه وجود خواهد داشت، گره‌ای که مقدار اعتماد آن در حال کاهش باشد و یا گره‌ای که از ارسال بسته‌ی اطلاعاتی دریافت شده به مقصد بسته، جلوگیری می‌کند. از همین‌رو، دو الگوریتم مجزا برای شناسایی این گره‌ها معرفی می‌شود:

الف – الگوریتم محاسبه اعتماد نزولی گره (NDTC)

چنانچه $N_{use\text{-}chance}$ دفعه‌ی متوالی، جدیدترین اعتماد ارزیابی شده‌ی یک گره، نسبت به اعتماد ماقبل، ۰,۹٪ کاهش داشته باشد، گره مذکور به عنوان گره مظنون شناسایی شده و از لیست اطلاعات و متعاقباً از عملیات مسیریابی، حذف شده و نظارت آن به عهده‌ی همسایگانش خواهد بود. برای پیاده‌سازی این نظریه، از فاکتور فرصت باقی‌مانده، استفاده می‌شود. به‌این‌ترتیب که با مقداردهی اولیه‌ی فاکتور فرصت باقی‌مانده برای هر گره، به محض مشاهده‌ی شرط (حالتی که اعتماد $Tr_{new}$ نسبت به $Tr_{last}$، ۰,۹٪ کاهش یافته باشد)، یک واحد از فاکتور فرصت باقی‌مانده کسر شده و برای استفاده در آینده، ذخیره می‌شود.

خاطرنشان می‌سازد که الگوریتم فوق، علاوه بر شناسایی گره بدخواه، وزن‌های مورد نیاز برای استفاده در رابطه ۱۶، که سابقه‌ی مقادیر قبلی اعتماد را در مقدار جدید اعتماد نیز تأثیر می‌دهد، بدست می‌آورد.

ب– الگوریتم محاسبه‌ی میزان مشارکت گره (NAC)

اگر تعداد بسته‌های ارسالی از گره‌ای مانند A بیشتر یا برابر با $Percent_{packet\_sent}$ درصد تعداد همسایگانش باشد و میزان مشارکت یک همسایه‌ی خاص مثل B ، در کمتر از $Percent_{association}$ درصد از تعاملات گره A وجود داشته باشد، آنگاه گره B، به عنوان گره مظنون شناخته شده، از فرصت استفاده می‌کند و مورد نظارت قرارخواهد گرفت.

۴-۱ نظارت گره‌ها بر یکدیگر

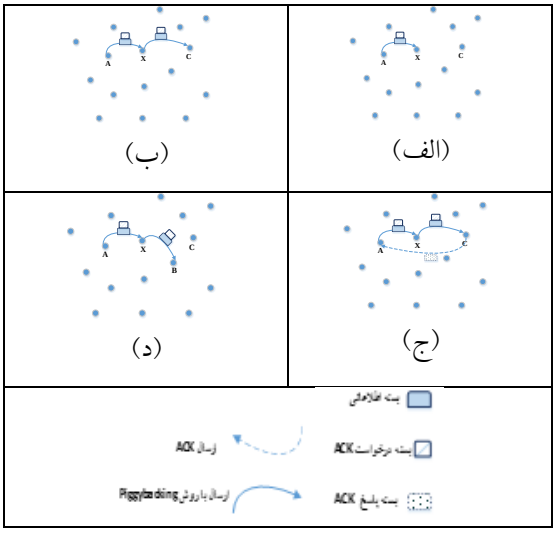
سناریوی نظارت گره‌ها بر همدیگر بدین صورت مطرح می‌شود:

هنگامی که گره‌ای تشخیص داد گره‌ای دیگر (مثل گره X) مخرب شده است، با ارسال بسته‌ای به همسایگان آن گره، آنان را از مخرب بودن گره X مطلع می‌گرداند. هر گره‌ای که از مخرب و یا مظنون بودن همسایه‌اش مطلع شد، پس از گذشت زمان $t_{det\_mal}$ از هنگامی که گره X مخرب یا مظنون تشخیص داده شده است، در یک بازه‌ی زمانی گره X را تحت نظارت خود قرارمی‌دهد. بدین‌صورت که:

۲-۱- چنانچه A و C همسایه‌های گره X بوده و به عنوان گره ناظر برای X درنظرگرفته شده باشند، هنگامی‌که گره A قصد ارسال اطلاعات (شامل درخواست ارسال Acknowledge) به مقصد گره C داشته‌باشد، اطلاعات خود را از طریق گره X به C ارسال کرده و به مدت $t_{wait}$ منتظر پیغام ACK از سوی گره C می‌ماند (شکل ۲- الف).

۲-۲- در این حالت، فرض می‌شود که گره X بسته‌ی دریافتی را به مقصد C ارسال می‌کند (شکل ۲ – ب). ازطرفی، گره C که از مخرب بودن X آگاه است، به فرستنده‌ی هر بسته‌ی دریافت‌شده از X یک پیام ACK ارسال کرده (شکل ۲-ج) و سپس بسته‌ی دریافتی را به همراه اطلاعات گره X به روش ارسال Piggybacking به مقصد گره مابعد خود می‌فرستد.

۲-۳- چنانچه بعد از گذشت زمان $t_{wait}$ ، گره A پیام ACK از سوی گره C دریافت نکرد، به معنی آن خواهد بود که گره X مسیریابی بسته را به‌درستی انجام نداده و بسته را به گره دلخواه خود (گره دیگری مثل B) فرستاده است (شکل ۲-د). در این‌صورت گره A مجدداً اقدام به ارسال داده‌ی خود و همینطور اطلاعات گره X، به روش Piggybacking، از مسیری دیگر می‌نماید.




شکل ۲- مراحل اجرای فاز نظارت. الف- گره A، بسته‌ی خود را از طریق گره X به گره C ارسال می‌کند. ب- گره X بسته‌ی گره A را به گره C ارسال می‌کند. ج – گره C با دریافت بسته‌ی گره A، پیغام ACK را به گره A می‌فرستد. د – گره X، بسته‌ی گره A را به مقصد نمی‌فرستد.

حال می‌توان شـــرایطی را درنظر گرفت که گره مظنون یا مخرب X، خود اقدام به تولید ACK جعلی نموده و با انجام این عمل و با هدف فریب گره فرسـتنده، این گره را از رسـیدن اطلاعاتش به گره C مطمئن سازد. بنابراین برای حصول اطمینان تقریبی از رسـیدن بسـته‌ی اطلاعات به مقصـد واقعی، هرگاه که گره A با هدف نظارت بر گره مظنون یا مخرب X، قصـد ارسـال اطلاعات به گره X را داشـته، همسـایگان گره X را نیز مطلع می‌کند. گره‌های همسـایه نیز، رسـیدن یا عدم رسـیدن بسته‌ی اطلاعاتی گره A به مقصد گره C را از طریق استراق سمع، کنترل می‌کنند. آنگاه گره A پس از دریافت پاسخ ACK، واقعی و یا جعلی بودن پیام ACK را با رأی‌گیری از نتایج گزارش شده از گره‌های همسایه، معین می‌سازد.

۴-۲ توزیع اطلاعات گره بدخواه بین گره‌ها و ایستگاه مرکزی

پیشنهاد توزیع اطلاعات گره‌های بدخواه، براساس این روش خواهد بود که هر گره، در تعاملات و ارسالاتی که طی زمان‌های مختلف انجام می‌دهد، مقدار اعتماد گره‌ای که آن را بدخواه تشخیص داده است را به روش Piggybacking به مقصد خود که ایستگاه مرکزی می‌باشد، ارسال می‌کند. ایستگاه مرکزی نیز در بازه‌های زمانی معین‌شده‌ای، مقادیر دریافتی را به همسایگان گره مزبور اعلام می‌کند.

۴-۳ روش تعامل با گره جدید و مقداردهی اولیه‌ی اعتماد

پیشـنهاد روش برخورد با گره‌ای که سـابقه‌ای از تعامل آن گره ثبت نشـده، بدین صورت خواهد بود که با استناد به مدارکی چون باقیمانده‌ی انرژی، مقدار موقتی اعتماد برای وی منظورمی‌شود. این مقدار موقتی، همان مقدار اولیه‌ی اعتماد برای هرگره در آغاز شـروع به‌کار شـبکه خواهد بود. آنگاه گره موردنظر، مورد تسـت راسـتی‌آزمایی قرارمی‌گیرد، چنانچه نتیجه‌ی تست مثبت باشد، تعامل با آن گره آغاز می‌شود درغیر اینصورت سابقه‌ی ارزیابی گره، به عنوان مقدار اعتماد آن گره، ذخیره شده و توسط همسایگانش موردنظارت قرارمی‌گیرد.

۴-۴ تصمیم‌گیری و محاسبه‌ی اعتماد براساس مدل منطق ذهنی

یک گره، مقدار اعتماد همسایگان خود را به این روش محاسبه می‌کند که ابتدا شماره شناسایی (ID) گره object را در لیست اطلاعاتی که نزد خود دارد، جستجو می‌نماید. چنانچه جستجو موفقیت‌آمیز بود، زمان آخرین اعتماد مقدار ثبت شده در پنجره‌ی لغزان را با زمان فعلی مقایسه کرده و اگر در بازه‌ی حد آستانه‌ای که بدین منظور تعیین شده، قرار داشته باشد، تصمیم‌گیری خود را برمبنای همان مقدار اعتماد بازیابی شده قرار می‌دهد و در غیراینصورت، مقدار جدید اعتماد را محاسبه می‌کند. لازم به ذکر است که درنظر گرفتن این حالت، این مزیت مهم را دارد که باعث افزایش سرعت مسیریابی خواهدشد.

جهت محاسبه‌ی مقدار اعتماد، با توجه به میزان تعاملات موفق ($N_S$) و ناموفق ($N_{US}$)، مقدار انرژی باقی‌مانده($E_{rem}$)، تعداد دفعات مظنون شناخته‌شدن از سوی گره ارزیابی کننده ($N_{sus}$)، تعداد دفعاتی که به‌دلیل مخرب شناخته شدن از سوی گره‌های همسایه، مورد نظارت قرارگرفته ($N_{mal}$)، فاصله‌ی زمانی دریافت و ارسال بسته توسط آن گره ($t_{sr}$) ،گره درخواست‌کننده، اقدام به ارزیابی اعتماد گره موردنظر می‌نماید.

برای به‌کارگیری هرکدام از این پارامترها، ابتدا میزان تأثیر هر پارامتر به‌صورت مستقل بررسی شده و در نهایت، برآیند همه‌ی رابطه‌های بدست‌آمده، به عنوان اعتماد ارزیابی شده‌ی نهایی، معرفی می‌شود. در ادامه، مقدار اعتماد در حوزه‌های انرژی، رفتار و ارسال مورد محاسبه قرار می‌گیرند. با استفاده از رابطه۴، مقدار اعتماد انرژی محاسبه می‌شود.

$$Tr_{energy} = \frac{E_{rem}}{E_{ini}} \qquad (۴)$$

در این‌جا، $E_{ini}$ مقدار انرژی اولیه‌ی هرگره و $Tr_{energy}$ اعتماد از دیدگاه انرژی می‌باشد.

برای محاسبه‌ی اعتماد در حوزه‌ی رفتار گره، تأثیر دو پارامتر $N_{sus}$ و $N_{mal}$ بر مقدار اعتماد، در یک رابطه گنجانده می‌شود. با توجه به رابطه ۵ :

$$Tr_{behaviour} = \left(1 - \frac{N_{sus}}{N_{max-sus}}\right) * \left(1 - \frac{N_{mal}}{N_{max-mal}}\right) \qquad (۵)$$

که در آن، $N_{max-sus}$ حداکثر تعداد دفعاتی که گره می‌تواند به عنوان گره مظنون، مورد نظارت قرارگیرد و $N_{max-mal}$ حداکثر تعداد دفعاتی است که گره می‌تواند به عنوان گره مخرب، مورد نظارت قرارگیرد. $Tr_{behavior}$ اعتماد از دیدگاه رفتار گره‌ها می‌باشد.

با استناد به رابطه ۵، می‌توان چنین استدلال نمود که اگر حاصل کسر $\frac{N_{sus}}{N_{det-sus}}$ و یا $\frac{N_{mal}}{N_{det-mal}}$ صفر شود، به معنی اعتماد کامل در همان حوزه است (کسر اول نشان‌دهنده‌ی میزان مظنون بودن و کسر دوم بیان‌کننده‌ی میزان مخرب بودن می‌باشد) و بالعکس چنانچه مقدار یک یا نزدیک به یک داشته باشند، به معنی کسر همان مقدار از اعتماد در همان حوزه می‌باشد. حاصل‌ضرب این دو پرانتز نیز گویای این نکته است که چنانچه گره‌ای مخرب شناخته شد (یعنی: $1 - \frac{N_{mal}}{N_{det-mal}} = 0$ یا $1 - \frac{N_{sus}}{N_{det-sus}} = 0$)، با صفر شدن یکی از پرانتزها، دیگری نیز از ارزش خواهد افتاد؛ چرا که فرصت آن گره یا برای

مظنون بودن و یا برای مخرب بودن، به اتمام رسیده و در هرکدام یک از این حالات، مخرب بودن آن گره محرز اعلام شده است.

جهت تصمیم‌گیری برای موفقیت یا عدم موفقیت ارسال یک بسته، می‌بایست اختلاف زمان ارسال و دریافت یک بسته را محاسبه کرد. اما از آنجاییکه، امکان از بین رفتن بسته (Packet Discard) در شبکه‌ها، امری اجتناب‌ناپذیر است، جهت درنظرگرفتن اثرات ناشی از آن، با استفاده از محاسبات انجام گرفته توسط Faridi و همکارانش در [۱۹] ابتدا احتمال از بین رفتن بسته، در محاسبه‌ی RTT به شرح ذیل، درنظر گرفته می‌شود:

هنگامی‌که گره‌ای قصد ارسال بسته‌ای را داشته و همزمان گره یا گره‌های مجاور آن نیز بسته‌ای ارسال می‌کنند، امکان ایجاد تصادم (Collision) رخ می‌دهد. در این حالت یک یا همه‌ی بسته‌ها از بین می‌روند و فرستنده می‌بایست، بسته‌ی خود را مجدداً ارسال کند. آنچه که در یک انتقال اطلاعات می‌تواند رخ دهد، شکست (Failure) در دسترسی به کانال، تصادم بسته‌های اطلاعاتی و یا موفقیت در ارسال بسته‌ها می‌باشد. در [۱۹] دو حالت برای از بین رفتن بسته درنظرگرفته شده است، یکی حالت شکست و دیگری تصادم. براساس نتایج حاصل از [۱۹] محاسبه‌ی احتمال اینکه سرانجامِ یک بسته به یکی از دو حالت شکست یا تصادم ختم شود، با استناد به رابطه‌های ۶ و ۷، بدست می‌آید.

$$P_{FAIL} = \prod_{i=0}^{M}(1 - y_i) \qquad (۶)$$

که در آن y احتمال دسترسی به کانال، M تعداد حالات تشخیص کانال (CCA - Clear Channel Assessment) و $P_{FAIL}$ احتمال شکست در دسترسی به کانال می‌باشد.

$$P_{COL} = P_{co} \times (1 - P_{FAIL}) \qquad (۷)$$

که در آن، $P_{co}$، احتمال تصادم هر گره و $P_{COL}$ احتمال تصادم شبکه می‌باشد.

بنابراین، با اعمال تأثیر رویداد تصادم، جهت بدست آوردن نتیجه‌ی موفقیت‌آمیز بودن و یا حصول عدم موفقیت در یک تعامل خاص، می‌توان از شبه‌کد شکل ۳ استفاده کرد:

```
1 | If (RTT <= Tmax)
2 |     Status<- Successful
3 | Else
4 |         Status<- Unsuccessful
```

شکل ۳- شبه کد نتیجه‌ی موفقیت‌آمیز بودن یا عدم موفقیت یک ارسال

که در این‌جا، RTT زمان رفت (ارسال بسته) و برگشت (دریافت پاسخ Ack) و $T_{max}$ مقدار حد آستانه‌ی زمان رفت و برگشت می‌باشد که مقدار آن به ازای هر گره، از رابطه ۸ بدست می‌آید:

$$T_{max}(i) = Threshold_{RTT} + P_{Col}(i) \qquad (۸)$$

با محاسبه‌ی هرکدام از پارامترهای رابطه منطق ذهنی، اعتماد ارزیابی شده‌ی مبتنی‌بر این رابطه، محاسبه می‌گردد. (رابطه‌های ۹ و ۱۰ و ۱۱)

$$b = \left(\frac{S}{S+F+1}\right) \quad (۹)$$

$$d = \left(\frac{F}{S+F+1}\right) \quad (۱۰)$$

$$u = \left(\frac{1}{S+F+1}\right) \quad (۱۱)$$

که در آن S، F، b، d و u به‌ترتیب، بیان کننده‌ی موفقیت، عدم موفقیت، اعتقاد، عدم اعتقاد و عدم قطعیت می‌باشند.

شایان ذکر است که مقدار بدست‌آمده از پارامتر u، همان مقدار اطمینان می‌باشد که نشان‌دهنده‌ی میزان صحت اعتماد است و برای اعمال تأثیر آن در مقدار اعتماد، از رابطه مدل منطقی استفاده می‌شود.

با درنظرگرفتن پارامتر a ($0 \leq a < 1$) به عنوان نرخ پایه‌ی تعریف‌شده در مدل منطق ذهنی، امید ریاضی اعتماد ارسال با توجه به رابطه۱۲ بدست می‌آید:

$$Tr_{packet} = b + au \quad (۱۲)$$

که پارامتر a معمولاً ۰,۵ درنظرگرفته می‌شود و $Tr_{packet}$ امید ریاضی اعتماد ارسال می‌باشد.

حال، با داشتن مقادیر اعتماد بدست‌آمده از هر پارامتر (یعنی رابطه‌های ۴، ۵ و ۱۱)، اعتماد نهایی یک گره با توجه به رابطه ۱۳، از حاصل‌جمع ضرب وزنی آن‌ها بدست می‌آید:

$$Tr_{new} = \alpha * Tr_{packet} + \beta * Tr_{energy} + \gamma * Tr_{behaviour} \quad (۱۳)$$
$$Where \quad \alpha + \beta + \gamma = 1$$

که مقدار ضرایب α، β و γ متغیر بوده و میزان تأثیر هرکدام از اعتمادهای بدست‌آمده را معین می‌سازند. $Tr_{new}$ جدیدترین مقدار اعتماد محاسبه شده‌ی یک گره خاص است.

طریقه‌ی ورود و خروج مقادیر اعتماد در پنجره‌ی لغزان و محاسبه‌ی ضریب تأثیر سابقه در آن نیز، می‌تواند طبق تعریف رابطه ۱۴ محاسبه می‌شود:

$$w_i = \rho^{\varepsilon \Delta T_i} \quad (۱۴)$$

و در نهایت، برآیند میزان سابقه، با استناد به رابطه ۱۵، محاسبه می‌شود.

$$Tr_{last} = W_3 * Tr_3 + W_4 * Tr_4 + W_5 * Tr_5 \quad (۱۵)$$

در این رابطه، $Tr_{last}$ مقدار برآیند اعتماد در سه تعامل گذشته می‌باشد.

برای ذخیره کردن اعتماد جدید در پنجره‌ی لغزان، با اعمال وزن‌دهی، مقدار جدید آخرین اعتماد، (رابطه ۱۶)، بدست می‌آیند:

$$Tr_{final} = W_{last} * Tr_{last} + W_{new} * Tr_{new} \qquad (۱۶)$$

۵. نتایج شبیه‌سازی

شبکه‌ی حسگر بی‌سیم پیاده‌سازی شده، دارای تعداد ۲۰۰ گره بوده، که در فضایی به ابعاد ۴۰ ×۴۰ متر مربع، مستقر شده‌اند. مهمترین پارامترهای این شبکه و مقادیر مربوط به محاسبه‌ی اعتماد در جدول ۱، مشاهده می‌شود.

۵-۱ ارزیابی مقایسه‌ای پیشنهاد حاضر با پژوهش EDTM

در این بخش، نتایج حاصل از مقایسه‌ی مقدار انرژی باقیمانده و درصد تشخیص گره‌های مخرب در طرح پیشنهادی، نسبت به پژوهش [۱۲] با نام EDTM (Efficient Distributed Trust Model)، مورد تحلیل و بررسی قرارمی‌گیرد.

جدول ۱- پارامترهای به‌کار رفته در شبیه‌سازی

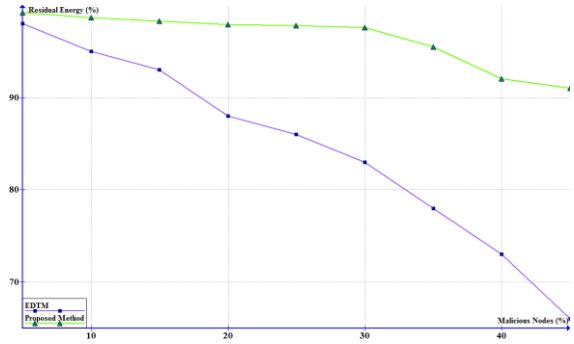
| نام پارامتر | مقدار پارامتر | شرح |
|---|---|---|
| BaseRateSL | ۰,۵ | نرخ پایه در رابطه مدل منطق ذهنی |
| α | ۰,۲۵ | ضریب امید ریاضی ارسال بسته در محاسبه‌ی مقدار جدید اعتماد |
| β | ۰,۵۵ | ضریب اعتماد در حوزه‌ی انرژی در محاسبه‌ی مقدار جدید اعتماد |
| γ | ۰,۲ | ضریب اعتماد در حوزه‌ی رفتار در محاسبه‌ی مقدار جدید اعتماد |
| θ | ۰,۷ | وزن مقدار جدید اعتماد در حالت $TR_{new} >= TR_{last} * 0.9$ |
| ω | ۰,۳ | وزن مقدار جدید اعتماد در حالت $TR_{new} < TR_{last} * 0.9$ |

| | | |
|---|---|---|
| TrustThreshold | ۰,۴ | حد آستانه‌ی قابل قبول برای مقدار اعتماد |
| RTTThreshold | ۵ | حد آستانه‌ی قابل قبول برای RTT |

۵-۲ ارزیابی و تحلیل انرژی باقیمانده‌ی کل شبکه

برای بدست‌آوردن انرژی باقیمانده‌ی کل شبکه، در انتهای یک شبیه‌سازی، مجموع انرژی‌های باقیمانده‌ی تک‌تک گره‌ها محاسبه می‌شود. نتایج حاصل از شبیه‌سازی با انرژی باقیمانده‌ی کل شبکه در EDTM، مورد مقایسه قرارگرفته است که در نمودار شکل ۴، قابل مشاهده می‌باشد.

در نمودارهای شکل‌های ۴ تا ۵، علامت مثلث (نمودار سبز رنگ)، نشان‌دهنده‌ی نتیجه‌ی طرح پیشنهادی است و علامت مربع (نمودار آبی رنگ)، نتیجه‌ی اجرای EDTM، می‌باشد.

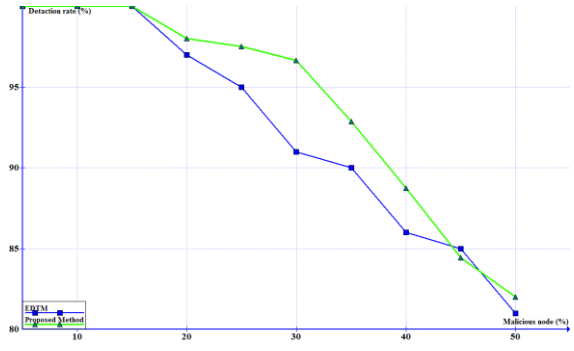



شکل ۴- مقایسه‌ی انرژی باقیمانده

همانطورکه مشاهده می‌شود، طرح پیشنهادی، با داشتن ۱۱,۹۹٪ افزایش نسبت به EDTM، توانسته است انرژی باقیمانده‌ی شبکه با مقدار نهایی انرژی ۸۶۷,۹ میلی ژول، بیشتر حفظ کند. درحالیکه انرژی باقیمانده‌ی شبکه در EDTM، به اندازه‌ی ۷۶۰ میلی ژول می‌باشد. این تفاوت به‌دلیل ذخیره‌ی انرژی گره‌های حسگر در عدم ارسال بسته به گره‌های بدخواهی که در همسایگی‌شان وجود دارد، رخ می‌دهد. چرا که بعد از اجرای الگوریتم‌های شناسایی گره بدخواه، هر گره‌ای که در نتیجه‌ی تعامل با گره بدخواه مزبور، این شناخت را پیدا کرده باشد از تعامل با وی خودداری نموده و از طرفی به‌دلیل گزارش گره تشخیص‌دهنده به ایستگاه مرکزی، گره‌های مجاور گره بدخواه نیز از طریق اعلام ایستگاه مرکزی و بدون صرف انرژی، زمان و ارتباط، از تعامل با گره بدخواه معرفی‌شده، خودداری خواهند نمود. این خودداری در ایجاد تعامل، به‌هنگام همه‌پخشی یک بسته توسط گره به همسایگانش، مفید می‌باشد، چرا که گره بدخواه در لیست گره‌های مخرب مربوط به گره فرستنده قرار دارد و از این‌رو، پیام و بسته‌ای برای آن گره ارسال نمی‌شود. بنابراین انرژی باقیمانده‌ی گره فرستنده، به مقدار بیشتری ذخیره خواهد شد. همچنین، استفاده از پنجره‌ی لغزان بهبودیافته به‌همراه ضریب تأثیر سابقه، کمک خواهد کرد تا هر گره به‌جای ایجاد تعامل جدید و بررسی میزان اعتماد گره مورد نظرش، از آخرین مقادیر اعتماد موجود در ساختار پنجره‌ی لغزان، استفاده کرده و از فعالیت‌های قبلی در شناخت و ارزیابی آن گره، بهره ببرد، بدون آنکه نیاز به صرف مجدد انرژی داشته باشد.

۳-۵ ارزیابی و تحلیل نرخ تشخیص گره‌های مخرب

در این شبیه‌سازی، پارامتر درصد گره‌های بدخواه از مقدار ۵٪ شروع و با افزایش ۵٪ به مقدار ۵۰٪ می‌رسد، که در هر بار افزایش تعداد گره‌های بدخواه، یک بار شبیه‌سازی انجام گرفته و میزان تشخیص تعداد گره‌های بدخواه مورد ارزیابی قرار می‌گیرد. نتیجه‌ی این ارزیابی که در نمودار شکل ۵، قابل ملاحظه می‌باشد، نشان‌دهنده‌ی افزایش دقت تشخیص نسبت به مدل EDTM می‌باشد.




شکل ۵- مقایسه‌ی نرخ تشخیص گره‌های بدخواه

این مقایسه، نشان می‌دهد طرح پیشنهادی با افزایش ۱٫۵۲٪ نسبت به طرح EDTM، قابلیت شناسایی گره‌های بدخواه را به ۹۴٫۰۲٪ ارتقاء داده است. این درحالی است که دقت تشخیص مدل EDTM به اندازه‌ی ۹۲٫۵٪ می‌باشد. اما همانطور که از نمودار شکل فوق برمی‌آید، در طرح پیشنهادی، میزان دقت تشخیص از ۳۰٪ خرابی به بعد، با ضریب بیشتری نسبت به مدل EDTM افت پیدا می‌کند. این موضوع به این دلیل است که در حین شبیه‌سازی و با اجرای طرح پیشنهادی و بالأخص با فعالیت الگوریتم‌های تشخیص گره بدخواه و اینکه در این میان، برخی گره‌ها به‌دلیل قرارگرفتن در کنار تعداد بیشتری همسایه‌ی بدخواه، مجبور به استفاده از گره‌های همسایه‌ی باقیمانده در ارسال بسته‌های خود شده و برخی از آن گره‌های همسایه نیز بعد از طی زمانی، انرژی کافی برای ارسال نخواهند داشت و به تدریج به عنوان گره مخرب شناخته می‌شوند، لذا چنانچه گره‌های واقعاً مخرب و یا بدخواهی در نزدیکی این گره‌های همسایه بوده و فقط از طریق آن‌ها قابل شناسایی باشند، همچنان مخفی می‌مانند. این موضوع را می‌توان با بیان مثبت یا منفی کاذب، به‌صورت روشن‌تری توضیح داد که شرح آن در ادامه خواهد آمد.

۶. تحلیل کارآیی راهکار پیشنهادی

۶-۱ ارزیابی تأثیر ضرایب محاسبه اعتماد بر کارکرد شبکه

منظور از ضرایب محاسبه‌ی اعتماد، ضرایب به‌کاررفته در رابطه **Error! Reference source not found.** می‌باشد که در شبیه‌سازی با نام‌های $\alpha$ ، $\beta$ و $\gamma$ شناخته شده‌اند. باتوجه به جدول ۱، این ضرایب به‌ترتیب دارای مقادیر ۰٫۲۵ ، ۰٫۵۵ و ۰٫۲ می‌باشند. مقدار بدست‌آمده برای ضریب $\beta$، مؤید این واقعیت است که میزان انرژی باقیمانده‌ی یک گره حسگر، در قابلیت اعتماد آن گره، از اهمیت بالاتری نسبت به رفتار و نحوه‌ی تعامل گره در ارسال اطلاعات همسایگان، برخوردار است.

چنانکه، هر گره حسگر برای اثبات قابلیت اعتماد خود، نیاز به انرژی داشته و بدون داشتن انرژی کافی، قادر به انجام وظایف خود نخواهد بود.

براین اساس، جهت ارائه‌ی میزان سرعت دستیابی به تشخیص گره‌های بدخواه، که یکی از اهداف تحقیق حاضر می‌باشد، به ازای مقادیر مختلف این ضرایب و درصد خرابی برابر با ۵٪ ، نمودارهای شکل ۶ که بیان‌کننده‌ی میزان سرعت تشخیص گره‌های بدخواه براساس مقادیر مختلف ضرایب $\alpha$ ، $\beta$ و $\gamma$ است، بدست می‌آید. در همه‌ی این نمودارها، مقدار عددی زمان پاسخ‌دهی نقاط بدست‌آمده در هر بار تغییر مقدار $\alpha$، $\beta$ و $\gamma$، حاصل از میانگین نتیجه‌ی سه بار اجرای شبیه‌سازی می‌باشد. بقیه‌ی پارامترها طبق جدول ۱، مقداردهی می‌شوند. نمودار آبی در شکل ۶ مقدار بهینه‌ی $\alpha$ و زمان پاسخ‌دهی آن را بررسی می‌کند که ضریب $TR_{packet}$ می‌باشد. در این نمودار، حالت‌های ذیل برای ضرایب $\alpha$، $\beta$ و $\gamma$ درنظرگرفته شده است:

$\alpha > bata, \gamma$

$\beta = \gamma$

جدول ۲ مقادیر $\alpha$، $\beta$ و $\gamma$ در بررسی مقدار بهینه‌ی $\alpha$

| مختصات نقطه | $\alpha$ | $\beta$ | $\gamma$ | زمان پاسخ‌دهی |
|---|---|---|---|---|
| (۷۴۰۲ و ۰,۰۵) | ۰,۰۵ | ۰,۴۷۵ | ۰,۴۷۵ | ۷۴۰۲ |
| (۵۹۰۷ و ۰,۱) | ۰,۱ | ۰,۴۵ | ۰,۴۵ | ۵۹۰۷ |
| (۴۶۷۵ و ۰,۱۵) | ۰,۱۵ | ۰,۴۲۵ | ۰,۴۲۵ | ۴۶۷۵ |
| (۴۷۷۵ و ۰,۲) | ۰,۲ | ۰,۴ | ۰,۴ | ۴۷۷۵ |
| (۵۳۵۶ و ۰,۲۵) | ۰,۲۵ | ۰,۳۷۵ | ۰,۳۷۵ | ۵۳۵۶ |
| (۵۶۰۰ و ۰,۳) | ۰,۳ | ۰,۳۵ | ۰,۳۵ | ۵۶۰۰ |
| (۵۶۷۷ و ۰,۳۵) | ۰,۳۵ | ۰,۳۲۵ | ۰,۳۲۵ | ۵۶۷۷ |
| (۶۲۵۰ و ۰,۴) | ۰,۴ | ۰,۳ | ۰,۳ | ۶۲۵۰ |
| (۶۸۰۶ و ۰,۴۵) | ۰,۴۵ | ۰,۲۷۵ | ۰,۲۷۵ | ۶۸۰۶ |
| (۷۴۲۴ و ۰,۵) | ۰,۵ | ۰,۲۵ | ۰,۲۵ | ۷۴۲۴ |
| (۷۹۴۶ و ۰,۵۵) | ۰,۵۵ | ۰,۲۲۵ | ۰,۲۲۵ | ۷۹۴۶ |
| (۸۰۵۲ و ۰,۶) | ۰,۶ | ۰,۱۵ | ۰,۱۵ | ۸۰۵۲ |

از نمودارشکل ۶ و جدول ۲، برمی‌آید که مقدار بهینه برای ضریب $\alpha$ در بازه‌ی (۰,۲۵ تا ۰,۱۵) قرار دارد. این نقطه‌ی بهینه، بیانگر این موضوع است که افزایش مقدار ضریب امید ریاضی ارسال بسته، از خارج از این بازه، باعث افزایش زمان پاسخ‌دهی شده و این نتیجه، تأکیدی بر اهمیت تأثیر مقدار دو ضریب $\beta$ و $\gamma$ نیز می‌باشد.

همین روند برای ضرایب $\beta$ و $\gamma$ در نمودارهای شکل ۶و مقادیری نظیر جدول ۲، اجرا می‌شود.

حالات ضرایب در شکل ۶، برای مقدار α (نمودار آبی) به شرح ذیل

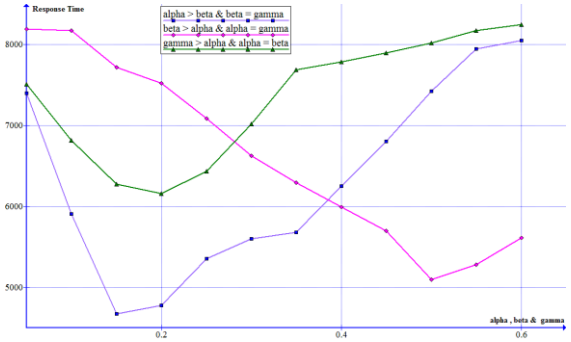
$\beta > \alpha , \gamma$
$\alpha = \gamma$

و برای مقدار β (نمودار صورتی) بدین صورت می‌باشد:

$\gamma > \alpha , \beta$
$\alpha = \beta$

نمودار صورتی در شکل ۶، مقدار بهینه‌ی β و زمان پاسخ‌دهی را بررسی می‌کند که ضریب $TR_{energy}$ محسوب می‌شود. همانطور که در شکل ۶مشاهده می‌شود، مقدار بهینه‌ی β در بازه‌ی (۰,۵۵ تا ۰,۴۵) قراردارد. این نمودار نشان می‌دهد گرچه با افزایش مقدار ضریب اعتماد انرژی تا ۰,۵، زمان پاسخ‌دهی کاهش می‌یابد، اما بعد از این مقدار و با افزایش مجدد ضریب اعتماد انرژی، زمان پاسخ‌دهی، روبه افزایش خواهد بود. این بدان معنی است که گرچه میزان انرژی باقیمانده، عاملی بسیار موثر در زمان پاسخ‌دهی می‌باشد، اما در کنار آن، میزان اعتماد در ارسال بسته و چگونگی رفتار گره در تعامل با همسایگان نیز، از ارزشی درخور خود، برخوردار است.

در ادامه، نمودار سبز شکل ۶، نیز بررسی γ، ضریب $TR_{behavior}$ را نشان می‌دهد. در این نمودار نیز، در بازه‌ی (۰,۲۵ تا ۰,۱۵)، مقدار γ، مقدار بهینه‌ای نشان داده می‌شود.




شکل ۶- مقایسه‌ی زمان‌های پاسخ‌دهی در α، β و γ

براساس این نمودار، می‌توان گفت با توجه به اثبات اهمیت و تأثیر میزان انرژی در کاهش زمان پاسخ‌دهی، ملاک انتخاب مقادیر α، β و γ برمبنای اولویت‌های انرژی، امید ریاضی ارسال بسته و نحوه‌ی رفتار گره، درنظرگرفته می‌شوند. بنابراین مقدار ۰,۵۵ برای β، ۰,۲۵ برای α و ۰,۲ برای γ انتخاب می‌شوند.

همچنین، براساس این نمودار و با مقایسه‌ی نقطه‌ی کمینه در هر سه نمودار، درمورد نمودار γ که دارای نقطه‌ی کمینه‌ی بالاتری نسبت به نمودارهای α و β می‌باشد، می‌توان گفت میزان تأثیر رفتار گره در مدل پیشنهادی، نسبت به تأثیر میزان انرژی و امید ریاضی ارسال بسته، کمتر بوده و به بیانی دیگر، نشان‌دهنده‌ی اهمیت بالای انرژی و امید ریاضی ارسال بسته در مسیریابی می‌باشد.

### ۶-۲ ارزیابی میزان دقت مدل پیشنهادی

در این بخش با استناد به معیار Precision، Recall و $F_1$-measure ، دقت مدل پیشنهادی مورد ارزیابی قرار می‌گیرد.

معیار Precision که از رابطه ۱۷، بدست می‌آید، بیانگر میزان دقت مدل در میان داده‌های پیش‌بینی‌شده می‌باشد.

$$Precision = \frac{TP}{TP + FP} \quad (۱۷)$$

معیـار Recall بـا استـفاده از رابطه **Error! Reference source not found.** بدسـت می‌آید و نسبت داده‌های پیش‌بینی شده به تعداد کل داده‌های مورد انتظار برای پیش‌بینی را نشان می‌دهد.

$$Recall = \frac{TP}{TP + FN} \quad (۱۸)$$

همچنین معیار$F_1$-measure ، که از رابطه **Error! Reference source not found.**، قابل محاسـبه اسـت، نوعی میانگین وزنی بین Precision و Recall می‌باشد که بالاترین مقدار آن ۱ و پایین‌ترین مقدار آن ۰ است.

$$F_1 = 2 * \frac{Precision * Recall}{Precision + Recall} \quad (۱۹)$$

بنابراین، می‌توان جدول ۳ را که مقدار Precision ، Recall و F1-Measure را در تشـخیص گره‌های بدخواه به ازای درصدهای مختلف گره‌های مخرب نشان می‌دهد، ترسیم نمود.

جدول ۳ – دقت مدل پیشنهادی در میان داده‌های پیش‌بینی‌شده.

| MaliciousPercent | Precision | Recall | $F_1$-measure |
|---|---|---|---|
| ٪۱۰ | ۱ | ۱ | ۱ |
| ٪۲۰ | ۰,۸۴ | ۰,۹۷ | ۰,۹ |
| ٪۳۰ | ۰,۸ | ۰,۹۶ | ۰,۸۷ |
| ٪۴۰ | ۰,۷۸ | ۰,۸۸ | ۰,۸۲ |
| ٪۵۰ | ۰,۷۴ | ۰,۸۲ | ۰,۷۷ |

با توجه به مقادیر Precision در جدول ۳، که معرف میزان دقت بدسـت‌آمده می‌باشد، مشاهده می‌شود که گرچه با افزایش نرخ خرابی گره‌ها، دقت تشـخیص، روندی نزولی دارد، اما بدسـت‌آمدن مقادیر بیشـتر از ۰,۷، حاکی از تشـخیصـی با دقت مناسب دارد. همچنین، نسبت داده‌های پیش‌بینی شده به کل داده‌های مورد انتظار که با Recall بیان شده است، بیان کننده‌ی این مطلب اسـت که حتی با افزایش درصـد خرابی گره‌های مخرب، روش ارائه شـده، توانایی بسـیار خوبی برای تشـخیص گره‌هـای واقعـاً مخرب داشـــتـه اســـت. به‌همین ترتیب، معیار$F_1$-measure که معرف میانگین وزنی بین Precision و Recall است، بر تأیید و صحت مقادیر بدست‌آمده از این دو معیار، تأکید دارد.

## ۷. نتیجه‌گیری و پیشنهادها

نتایج حاصل از این طرح تحقیق، نشان داده است که با بکارگیری روش پیشنهادی می‌توان تا حد بسیار قابل توجهی در میزان مصـرف انرژی صـرفه‌جویی به‌عمل آورده و در عین حال، افزایش دقت تشـخیص گره‌های مخرب را نیز به دسـتاورد قبلی افزود. افزایش دقت در تشـخیص گره‌های مخرب، خود عاملی برای رشـد سرعت مسیریابی محسوب می‌شود، چراکه هرچه دقت تشـخیص بالاتر باشـد، میزان شرکت گره‌های بدخواه و یا مخرب در انتخاب شدن و شامل شدن در مسیر ارسال بسته، کاهش یافته و بسته‌ها زودتر و با امنیت بالاتری به مقصد خواهند رسید.

به عنوان پیشـنهادهایی برای ادامه کار در آینده می‌توان فاکتور فرصـت برای هر گره را براسـاس تابعی از نظرات همسـایگان تنظیم کرد تا تعداد فرصـت برای گره‌ای که اعتماد بیشـتری از دیدگاه همسـایگان دارد، نسـبت به گره‌ای که از این مزیت برخوردار نیسـت، بیشـتر باشـد، چراکه این فاکتور از عوامل مهم در به تعویق افتادن شناسایی یک گره به عنوان گره بدخواه می‌باشد.

## مراجع


1. Ishmanov, F., S.W. Kim, and S.Y. Nam, *A robust trust establishment scheme for wireless sensor networks.* Sensors, 2015. **15**(3): p. 7040-7061.
2. Jøsang, A., E. Gray, and M. Kinateder, *Simplification and analysis of transitive trust networks.* Web Intelligence and Agent Systems: An International Journal, 2006. **4**(2): p. 139-161.
3. Feng, R., et al., *A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory.* Sensors, 2011. **11**(2): p. 1345-1360.
4. Bao, F., et al ,.*Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection.* IEEE transactions on network and service management, 2012. **9**(2): p. 169-183.
5. Li, X., F. Zhou, and J. Du, *LDTS: A lightweight and dependable trust system for clustered wireless sensor networks.* IEEE transactions on information forensics and security, 2013. **8**(6): p. 924-935.
6. Geetha, V. and K. Chandrasekaran, *A distributed trust based secure communication framework for wireless sensor network.* Wireless Sensor Network, 2014. **6**(09): p. 173.
7. Zhang, B., Z. Huang, and Y. Xiang, *A novel multiple-level trust management framework for wireless sensor networks.* Computer Networks, 2014. **72**: p. 45-61.
8. Ahmed, A., et al., *A trust aware routing protocol for energy constrained wireless sensor network.* Telecommunication Systems, 2016. **61**(1): p. 123-140.
9- Fang, W., et al., *BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks.* Journal of Network and Computer Applications, 2016. **59**: p. 88-94.
10. Singh, M., et al. *Lightweight trust model for clustered WSN*. in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*. 2015. Springer.

11. Jadidoleslamy, H., M.R. Aref, and H. Bahramgiri, *A fuzzy fully distributed trust management system in wireless sensor networks.* AEU-International Journal of Electronics and Communications, 2016. **70**(1): p. 40-49.
12. Jiang, J., et al., *An efficient distributed trust model for wireless sensor networks.* IEEE transactions on parallel and distributed systems, 2014. **26**(5): p. 1228-1237.
13. Devanagavi, G.D., N. Nalini, and R.C. Biradar, *Secured routing in wireless sensor networks using fault-free and trusted nodes.* International Journal of Communication Systems, 2016. **29**(1): p. 170-193.
14. Yang, T., et al., *A secure routing of wireless sensor networks based on trust evaluation model.* Procedia computer science, 2018. **131**: p. 1156-1163.
15. Khalid, N.A., Q. Bai, and A. Al-Anbuky, *Adaptive trust-based routing protocol for large scale WSNs.* IEEE Access, 2019. **7**: p. 143539-143549.
16. Shende, D.K. and S. Sonavane, *CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications.* Wireless Networks, 2020. **26**(6): p. 4011-4029.
17. Fang, W., et al., *Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks.* Digital Communications and Networks, 2021. **7**(4): p. 470-478.
18. Abualkishik, A.Z. and A.A. Alwan, *Trust aware aquila optimizer based secure data transmission for information management in wireless sensor networks.* Journal of Cybersecurity and Information Management, 2022. **9**(1): p. 40-51.
19. Faridi, A., et al., *Comprehensive evaluation of the IEEE 802.15. 4 MAC layer performance with retransmissions.* IEEE Transactions on Vehicular Technology, 2010. **59**(8): p. 3917-3932.