مقاله پژوهشی

مدل اعتماد توزیع‌شده رویدادمحور برای شبکه اینترنت اشیا

زهرا هادیان، فضل‌الله ادیب‌نیا و وحید رنجبر

چکیده: چشم‌اندازی از اینترنت آینده به‌گونه‌ای معرفی شده که دستگاه‌های محاسباتی مختلف به یکدیگر متصل می‌شوند تا شبکه‌ای به نام اینترنت اشیا را تشکیل دهند. اینترنت اشیا با ارائه بسیاری از برنامه‌ها و وسایل هوشمند که می‌توان از راه دور کنترل کرد، زندگی انسان را تسهیل می‌کند. امنیت اینترنت اشیا به دلیل ویژگی‌های ذاتی اینترنت اشیا به‌ویژه ناهمگونی گره‌ها از نظر منابع، یک کار چالش‌برانگیز است. مدیریت اعتماد با محاسبه و تجزیه‌وتحلیل اعتماد بین گره‌ها، در برقراری ارتباط بین گره‌ها این امکان را فراهم می‌کند که گره، تصمیم مناسب و قابل اعتمادی بگیرد. هدف طرح‌های مدیریت در یک سیستم توزیع‌شده این است که بر اساس رفتارهای قبلی گره‌ها، رفتارهای آینده آنها را پیش‌بینی کند. در این مقاله یک روش مدیریت اعتماد توزیع‌شده رویدادمحور پیشنهاد شده که به محاسبه اعتماد بین اشیا با استفاده از جمع وزنی می‌پردازد. در این روش، گره‌ها می‌توانند رفتار دیگر گره‌ها را ارزیابی کنند. با توجه به شبیه‌سازی انجام‌شده، روش پیشنهادی در مقایسه با روش DDTMS، سریع‌تر است و در تعداد تراکنش کمتری گره‌های مخرب را شناسایی می‌کند و همچنین در برابر حملات روشن- خاموش و بدگویی مقاوم‌تر است.

کلیدواژه: **اینترنت اشیا، مدیریت اعتماد، مدیریت اعتماد توزیع‌شده، ارزیابی اعتماد.**

۱- مقدمه

اینترنت اشیا (IoT)[1] یک زمینه تحقیقاتی نوظهور در حوزه شبکه است و در کلیه حوزه‌هایی که می‌تواند زندگی افراد را تغییر دهند قابل اعمال است. اینترنت اشیا تعداد زیادی از دستگاه‌های زندگی روزمره را از محیط‌های شبکه ناهمگون ادغام می‌کند و چالش بزرگی را برای مدیریت امنیت پدید می‌آورد. علاوه بر این در برخی موارد استفاده، حجم قابل توجهی از داده‌های حساس تولید می‌شود. تعداد تهدیدات امنیتی مربوط به زیرساخت، بستر و برنامه اینترنت اشیا طی چند سال گذشته، افزایش یافته است [۱]. دستگاه‌های اینترنت اشیا دارای قابلیت‌های محدودی هستند که توانایی اجرای مکانیسم‌های پیچیده امنیت را ندارند که دلیل اصلی آن، محدودیت انرژی و فضای حافظه گره‌های اینترنت اشیا است.

در اینترنت اشیا هر شیء در اینترنت قابل دسترسی و ردیابی است. هدف اینترنت اشیا ایجاد یک شبکه وسیع با میلیاردها شیء است که بتوانند به‌طور یکپارچه داده ایجاد و مبادله کنند و تعاملات هوشمندانه‌ای بین افراد و اشیای اطراف آنها برقرار شود. شبکه‌های اینترنت اشیا از نظر ماهیت باز، ناشناس و پویا هستند که به ناچار مسائل امنیتی، حریم خصوصی و اعتماد[2] شدیدی را ایجاد می‌کنند که مانع از کاربرد گسترده اینترنت اشیا می‌شود [۲].

پروتکل‌های امنیتی مبتنی بر اینترنت سنتی به‌دلیل ناهمگونی دستگاه‌ها و همچنین محدودیت منابع آنها نمی‌توانند در اینترنت اشیا سازگار شوند. در بعضی موارد، گره‌های محدود در شبکه معمولاً برای انجام یک کار خاص نیاز به پشتیبانی از گره‌های دیگر دارند. اگرچه مسائل متعددی وجود دارد که با پیاده‌سازی اینترنت اشیا مرتبط هستند، امنیت به‌دلیل ماهیت خودمختار این فناوری از اهمیت بالایی برخوردار است؛ بنابراین لازم است راهکارهای امنیتی مناسبی که امنیت و محرمانگی داده‌ها را تضمین می‌کند، استفاده شود. مدیریت اعتماد (TM)[3] نقش مهمی در اینترنت اشیا برای تلفیق و استخراج داده‌های قابل اطمینان، خدمات واجد شرایط و افزایش حریم خصوصی کاربر و امنیت اطلاعات ایفا می‌کند. اعتماد می‌تواند به‌عنوان یک ویژگی اصلی برای ایجاد ارتباط قابل اعتماد و یکپارچه بین نهادها و تضمین خدمات و برنامه‌های ایمن در نظر گرفته شود. برای دستیابی به ارتباطات امن و قابل اعتماد، راه‌حل‌های مختلف مبتنی بر اعتماد ارائه شده است [۳].

یک مدل اعتماد قابل اطمینان باید امنیت شبکه و یکپارچگی داده‌ها را تضمین و همچنین به‌عنوان داوری عمل کند که گره‌های قابل اعتماد را شناسایی نماید و به سایر گره‌ها انتشار دهد و هر گونه فعالیت مخرب را شناسایی و مجازات کند. امتیازات اعتماد اختصاص داده شده توسط مدل اعتماد بر اساس سابقه گره‌هاست که می‌تواند به پیش‌بینی رفتارهای آینده گره‌ها کمک کند [۴]. مدل‌های اعتماد جهت شناسایی اشیای مخرب و بهبود قابلیت اطمینان شبکه پیشنهاد شده‌اند. توصیه‌های همسایگان در محاسبه اعتماد، نقش اساسی و مهمی دارند؛ بنابراین مدل‌های اعتماد در برابر حملات مخرب و تبانی، آسیب‌پذیر هستند. همچنین اعتماد یک مانع اساسی است که ممکن است مانع رشد اینترنت اشیا شود و حتی تعدادی از برنامه‌ها را به تأخیر بیندازد [۲].

روش‌های مدیریت اعتماد از نظر انتشار اعتماد به دو دسته متمرکز و توزیع‌شده تقسیم می‌شوند. رویکردهای متمرکز ممکن است برای همه کاربردها مناسب نباشد؛ زیرا مدیریت مرکزی انرژی بیشتری را مصرف می‌کند. در رویکرد متمرکز، هر درخواست و سرویس اعتماد از طریق یک گره مرکزی عبور می‌کند که توسط سایر گره‌های موجود در دامنه وی قابل دسترسی است. گره مرکزی، مسئول ارائه اطلاعات اعتماد ازجمله مذاکره اعتماد، محاسبه و تصمیم‌گیری یا کمک به گره‌ها با تهیه اطلاعات اولیه مورد نیاز برای محاسبه اعتماد خواهد بود. در رویکرد توزیع‌شده، گره‌های اینترنت اشیا به‌طور مستقل اعتماد را محاسبه کرده و جدول

این مقاله در تاریخ ۲۲ شهریور ماه ۱۴۰۱ دریافت و در تاریخ ۹ آذر ماه ۱۴۰۲ بازنگری شد.

زهرا هادیان، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران، (email: zhadian@stu.yazd.ac.ir).

فضل‌الله ادیب‌نیا، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران، (email: fadib@yazd.ac.ir).

وحید رنجبر (نویسنده مسئول)، دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ، ایران، (email: vranjbar@yazd.ac.ir).

1. Internet of Things

2. Trust

3. Trust Management

اعتماد را با گره‌های همسایه بدون دخالت نهاد متمرکز تبادل می‌کنند.

در این مقاله یک روش مدیریت اعتماد توزیع‌شده سبک‌وزن پیشنهاد گردیده که به محاسبه اعتماد بین اشیا با استفاده از جمع وزنی می‌پردازد. در این روش، گره‌ها بعد از انجام تعامل با هم، عملکرد و رفتار گره سرویس‌دهنده را ارزیابی کرده و با توجه به تعداد تراکنش‌های خوب و بد، به گره سرویس‌دهنده پاداش یا مجازات اعطا می‌کنند. گره سرویس‌گیرنده، مقدار اعتماد محاسبه‌شده را در اختیار همسایگان قرار می‌دهد. گره همسایه نیز با توجه به مقایسه مقدار اعتماد پیشنهادی با مقدار اعتمادی که خودش محاسبه کرده، جدول اعتماد خود را به‌روزرسانی می‌کند.

این مقاله در بخش دوم به بررسی کارهای مرتبط در حیطه مدیریت اعتماد در اینترنت اشیا می‌پردازد. در بخش سوم روش مدیریت اعتماد پیشنهادی آمده است. در بخش چهارم نتایج ارزیابی نشان داده شده‌اند و نهایتاً در بخش پنجم به جمع‌بندی و نتیجه‌گیری می‌پردازیم.

۲- کارهای مرتبط

در این بخش ابتدا به بررسی روش‌های متمرکز مدیریت اعتماد که تاکنون توسط محققین ارائه شده است می‌پردازیم. سپس چالش‌های این گونه روش‌ها، بررسی و روش‌های توزیع‌شده ارائه‌شده بیان می‌گردند که سعی در حل چالش‌های روش‌های متمرکز دارند.

عبید و همکارانش یک مدل مدیریت اعتماد متمرکز چندلایه را برای زمان‌بندی کار در محاسبات ابری موبایل (MCC)[1] پیشنهاد کرده‌اند که برای برنامه‌ریزی کارآمد در محیط‌های ابری موبایل قابل پیاده‌سازی است. این رویکرد به دو صورت عمل می‌کند. در این روش ابتدا وظایف قابل اعتماد مورد نیاز برای محاسبات ابری موبایل محاسبه می‌شود. آنها اعتماد را با درنظرگرفتن ویژگی‌هایی مانند صداقت، تأخیر و شایستگی محاسبه می‌کنند. توابع قابل اعتماد باید در لایه ابری توزیع شوند و اهمیت کنترل تمام روش‌های اتوماسیون را ارائه دهند. سپس یک زمان‌بندی کارآمد و پویا را برای بهبود زمان‌بندی کار پس از محاسبه اعتماد با استفاده از روش‌های محاسبه اعتماد اجتماعی و محیطی اضافه می‌کنند و تنها وظایف قابل اعتماد از دستگاه‌ها به سمت ابر منتقل می‌شوند [۵].

کامران احمد و همکارانش یک روش محاسبه اعتماد متمرکز را برای شبکه‌های VANET[2] پیشنهاد داده‌اند. در این مطالعه، یک رویکرد خوشه‌بندی StabTrust برای پرداختن به این مسائل امنیتی پیشنهاد شده است. روش‌های خوشه‌بندی برای محدودکردن ارتباط وسایل نقلیه با زیرساخت‌ها ارائه شده است. در خوشه‌بندی، وسایل نقلیه با هم جمع می‌شوند تا خوشه‌ای را بر اساس قوانین خاصی تنظیم کنند. هر خوشه از تعداد محدودی از وسایل نقلیه/ گره‌ها و یک سرخوشه (CH) تشکیل شده است. StabTrust روشی را برای تدوین خوشه‌های قابل اعتماد و مطمئن ارائه می‌دهد. علاوه بر این از دانش، شهرت و اجزای تجربه اعتماد برای حفظ درجه اعتماد در بین گره‌های یک خوشه استفاده می‌کند. همچنین یک گره با اعتماد عالی به‌عنوان سرخوشه انتخاب می‌شود که اعتماد بین گره‌ها را افزایش می‌دهد تا به اطلاعات تولیدشده توسط یک گره اعتقاد داشته باشند. سرخوشه (CH) می‌تواند مشارکت فعال گره‌های مخرب و در خطر را در داخل ارتباط دستگاه با دستگاه حذف کند. دستاورد این مکانیسم متمرکز، ایجاد پایداری شبکه با افزایش طول عمر شبکه و کاهش سربار محاسبات است و مطمئناً در صورت حجم زیاد داده‌ها و کاربرد حیاتی نمی‌تواند یک رویکرد ایده‌آل باشد؛ زیرا باید مصرف انرژی را نیز در نظر بگیرد [۶].

محمد داهمان و همکارانش یک رویکرد متمرکز برای مدیریت اعتماد در اینترنت اشیا ارائه داده‌اند. آنها برای دستیابی به ارتباط قابل اعتماد بین گره‌ها، پیشنهاد می‌کنند محیط اینترنت اشیا را به خوشه تقسیم کنند. چارچوب کلی آنها شامل یک SN[3] به‌عنوان گره مدیریت اعتماد متمرکز است که ماژول‌های مختلف مربوط به اعتماد را برای ارزیابی اعتماد و نظارت بر دستگاه‌ها نگه می‌دارد. مقادیر اعتماد، گره‌های اصلی خوشه و آدرس گره‌های خوشه را در جدول مسیریابی خود نگه می‌دارد. هر خوشه دارای یک مدیر محلی اعتماد به نام MN[4] است. همچنین در هر خوشه چندین گره سرخوشه CN[5] وجود دارد که تحت نظارت MN با یکدیگر ارتباط برقرار می‌کنند. SN یک حافظه مرکزی برای ذخیره داده‌های اعتماد برای همه MNها و CNها برای کل چارچوب اینترنت اشیا دارد و MNها حافظه محلی دارند که در آنها مقادیر اعتماد برای CNها در هر خوشه ذخیره می‌شود. سیستم مرکزی بر کل شبکه TM-IoT نظارت می‌کند که شامل ارتباط با گره اصلی از برنامه IoT از طریق تماس‌های REST API و ارسال دستورالعمل‌ها به CNها برای دسترسی به داده‌های مخزن است. در شبیه‌سازی این مدل، انعطاف‌پذیری در برابر گره‌های مخرب پیاده‌سازی نشده است [۷].

در مطالعه‌ای که توسط کوتارو و همکاران صورت گرفته است، یک لیست اعتماد در شبکه‌های لبه ارائه گردیده که اطلاعات مربوط به سرویس‌ها و دستگاه‌های معتبر اینترنت اشیا را در بین این دسته از ذی‌نفعان گردش می‌دهد. لیست اعتماد بر جلوگیری از ترافیک ناخواسته از دستگاه‌های اینترنت اشیا مانند حملات DDoS به شبکه‌های لبه، متمرکز است. آنها لیست اعتماد را با استفاده از بلاک‌چین‌های خصوصی و عمومی Ethereum انجام داده‌اند. کنترل‌کننده‌های SDN[6] به‌روزرسانی (آپدیت) از بلاک‌چین را دریافت و بررسی و تعیین می‌کنند که آیا دستگاه به شبکه آنها وصل شود یا خیر. اگر اعتبار دستگاه اینترنت اشیا موفقیت‌آمیز باشد، کنترلر SDN مشخصات دستگاه را در گره بلاک‌چین پیدا می‌کند. اثبات آنها از اجرای مفهوم، ادغام شبکه نرم‌افزارمحور و بلاک‌چین‌ها و نیز برنامه‌های شبه اینترنت اشیا را برای ارزیابی تأیید پوشش داده است. آنها ثابت کرده‌اند که مدیریت ترافیک اینترنت اشیا توسط Trust List که کد مرجع آن به‌عنوان نرم‌افزار منبع باز در دسترس است، به‌درستی انجام می‌شود؛ اما در این روش افزایش اندازه لیست اعتماد به معنای افزایش هزینه تراکنش در بلاک‌چین است و در نتیجه مشکلات مقیاس‌پذیری را افزایش می‌دهد [۸].

امایما و همکارانش یک سیستم مدیریت اعتماد مبتنی بر جوامع مورد علاقه برای اینترنت اجتماعی اشیا (TMCoI-SIOT) را پیشنهاد داده‌اند که ویژگی‌های مختلفی مانند مدل‌سازی اجتماعی اعتماد، اعتماد مستقیم و غیرمستقیم و عوامل معامله را در خود گنجانده است. روش پیشنهادی بر روی اینترنت اجتماعی متمرکز است و چندین پارامتر اعتماد را بر اساس ارزیابی مستقیم و غیرمستقیم ادغام می‌کند. معماری TMCoI-SIOT از مفهوم خوشه‌بندی استفاده می‌کند و گره‌ها را بر اساس علاقه به جوامع تقسیم می‌نماید. در این روش، تشکیل جامعه با تأیید اعتبار گره آغاز

1. Mobile Cloud Computing
2. Vehicle Ad-Hoc Network
3. Super Node
4. Master Node
5. Cluster Node
6. Software-Defined Networking

می‌شود. اگر یک گره بخواهد به SIOT بپیوندد، سرور SIOT آن را تأیید می‌کند. پس از تأیید اعتبار، گره مجاز به پیوستن به جامعه مورد علاقه خود است یا می‌تواند ایجاد جامعه خود را آغاز کند. به‌علاوه، هر جامعه‌ای مدیر اعتماد خاص خود را دارد. انتخاب یک مدیر اعتماد بر اساس مقدار اعتماد است و پارامترهای مورد استفاده برای ارزیابی اعتماد از سطح اعتماد، توانایی و اجتماعی‌بودن یک گره تشکیل شده است. پس از انتخاب مدیر اعتماد، اگر مدیر خراب شود و ارتباط خود را با گره‌ها از دست بدهد، کل جامعه یا یک منطقه مجاز از جامعه خارج می‌شود. مسئولیت‌های مدیر شامل محاسبه و ذخیره‌سازی مقادیر اعتماد است. وقتی یک گره جدید درخواست پیوستن به مدیر را ارسال می‌کند، اعتماد را محاسبه و آن را با مقدار آستانه مقایسه می‌کند. اگر مقدار اعتماد بیشتر از آستانه باشد، مدیر شباهت‌ها و منطقه جغرافیایی گره را بررسی می‌کند تا درخواست پیوستن را بپذیرد. معماری آن مبتنی بر خوشه است و این معماری به کاهش چالش‌های مرتبط با حافظه کمک می‌کند. طرح پیشنهادی در برابر حملات روشن- خاموش[1] ارزیابی شده؛ اما در برابر حملات بددهان[2] مورد ارزیابی قرار نگرفته است [۹].

به‌طور کلی، روش‌های محاسبه و مدیریت اعتماد متمرکز از مشکلاتی مانند تنها یک نقطه شکست دارند، از پیاده‌سازی ساده‌ای برخوردار هستند و مقیاس‌پذیر نیستند و دارای گلوگاه عملکرد هستند، رنج می‌برند؛ به همین دلیل امروزه بیشتر از روش‌های غیرمتمرکز و توزیع‌شده استفاده می‌شود [۱۰].

در مطالعه‌ای که توسط کامران احمد و همکاران صورت گرفت، یک سیستم مدیریت اعتماد توزیع‌شده قدرتمند متقابل دامنه[3] ارائه شده که باعث می‌شود یک وسیله مناسب برای ارزیابی اعتماد به دستگاه‌های مختلف محلی باشد. در این سیستم، اعتماد به سه مؤلفه امنیتی تقسیم می‌شود که به گره‌های اینترنت اشیا کمک می‌کنند تا در برابر دستگاه‌ها و گره‌های مخرب و بدرفتار محکم شوند. مرحله ترکیب اعتماد شامل دانش، شهرت و تجربه است. علاوه بر این، سازوکار پیشنهادی مبتنی بر رویداد است؛ به این معنی که یک گره فقط هنگام وقوع یک رویداد بین دو گره، اعتماد را ارزیابی و به گره‌ها کمک می‌کند تا اعتماد بیشتری را ارزیابی کنند و نیز کارایی سیستم را افزایش دهند. کار پیشنهادی با تمرکز روی ویژگی‌های مختلف مانند امانت، قابلیت استفاده و دقت در بین دیگران با برنامه‌های ارزیابی اعتماد موجود مقایسه می‌شود. RobustTrust توسط شبیه‌سازی‌های گسترده با توجه به عملکرد مطلق اعتماد، صحت تخمین اعتماد و چندین حمله بالقوه تأیید می‌شود؛ اما در این مطالعه میزان مصرف انرژی در مقایسه با کارهای مشابه افزایش یافته و نیز قابلیت سازگاری در مقایسه با کارهای مشابه کمتر است [۱۱].

روپایان و همکارانش با درنظرگرفتن اعتماد به خود (SLT)، اعتماد اجتماعی (ST)، اعتماد سبز (GT) و اعتماد QoS، یک معماری مدیریت اجتماعی مبتنی بر جامعه را پیشنهاد می‌کنند. آنها اعتماد به خود را با استفاده از پارامترهای پردازش داده، حریم خصوصی داده‌های اینترنت اشیا و انتقال داده‌های اینترنت اشیا محاسبه می‌کنند. اعتماد سبز همچنین به‌عنوان اعتماد زیست‌محیطی شناخته می‌شود که با ویژگی‌های شبکه سروکار دارد. دستگاه‌های اینترنت اشیای تازه تأسیس‌شده با رفتار شبکه مقایسه می‌شوند تا بررسی کنند آیا دستگاه‌ها به‌خوبی نصب شده‌اند یا خیر. آنها اعتماد سبز را با پارامترهای طول عمر شبکه و زمان پاسخگویی محاسبه می‌کنند. اعتماد اجتماعی، رفتار گره‌های درون جامعه را نشان می‌دهد. آنها اعتماد اجتماعی را توسط پارامترهای صمیمیت، صداقت و شباهت‌های اجتماعی و همچنین اعتماد QoS را توسط پارامترهای زیادی مانند انطباق پروتکل و انرژی محاسبه می‌کنند. این رویکرد از مقدار انرژی بالایی برای انجام محاسبات استفاده می‌کند [۱۲].

یارا و همکارانش، مدلی را برای مدیریت اعتماد در دستگاه‌ها و سرویس‌های اینترنت اشیا بر اساس تکنیک رتبه‌بندی چند ویژگی ساده (SMART)[4] و الگوریتم حافظه کوتاه‌مدت بلندمدت (LSTM)[5] پیشنهاد پیشنهاد می‌کنند. تکنیک SMART برای محاسبه ارزش اعتماد استفاده می‌شود که ارزش اعتماد را بر اساس اطلاعات گره محاسبه می‌کند که در مرحله قبل (آماده‌سازی داده‌ها) به‌دست آمده است. الگوریتم LSTM برای شناسایی تغییرات در رفتار بر اساس آستانه اعتماد استفاده می‌شود. روش آنها با استفاده از دقت، نرخ تلفات، صحت، فراخوانی و اندازه‌گیری F[6] بر روی نمونه‌های داده‌های مختلف با اندازه‌های مختلف ارزیابی می‌شود؛ اما این مطالعه در برابر حملات مورد ارزیابی قرار نگرفته است [۱۳].

در کارهای مطالعه‌شده در مدیریت اعتماد متمرکز با روش‌هایی مانند خوشه‌بندی [۶] و [۹]، یک سرور یا مدیریت‌های چندسطحی [۷]، چند سرور را به‌عنوان سرور مرکزی در نظر می‌گیرند. در اینترنت اشیا، انتخاب یک سرور به‌عنوان سرور مرکزی که مسئولیت محاسبه مقدار اعتماد برای همه گره‌ها را به عهده دارد، معایب زیادی دارد و یکی از مهم‌ترین آنها این است که اگر مرجع مرکزی به خطر بیفتد، هیچ ابزار جایگزینی برای مدیریت یا کنترل مقدار اعتماد وجود ندارد. در مدیریت اعتماد توزیع‌شده چون هر گره خودش ارزش اعتماد را محاسبه می‌کند، هر گره به مصرف انرژی و حافظه بیشتری نسبت به رویکرد متمرکز نیاز دارد. یکی از معایب مهمی که در اکثر رویکردهای توزیع‌شده [۱۱] و [۱۲] مطرح گردیده است، مصرف انرژی و حافظه گره‌هاست. خلاصه‌ای از مطالعات پیشین در این حوزه در جدول ۱ آمده است.

در این مقاله با توجه به ماهیت اینترنت اشیا، یک مدیریت اعتماد توزیع‌شده مطرح گردیده که علاوه بر سبکی و راحتی، ارزش اعتماد را در زمان سریع‌تر و تعداد تراکنش کمتر محاسبه می‌کند و نیز در برابر حملات روشن- خاموش و بددهان مقاوم است.

۳- روش پیشنهادی

در اینترنت اشیا، دستگاه‌های ناهمگون زیادی به هم متصل هستند که در هر زمان و مکان به شبکه سراسری اینترنت متصل می‌شوند و امکان دسترسی به اطلاعاتی زیاد را فراهم می‌کنند. این اشیای هوشمند، توانایی انجام کارهای روزمره را با کمترین دخالت انسان دارند. این دستگاه‌ها در اینترنت اشیا اغلب در معرض استفاده عمومی قرار می‌گیرند و از طریق کانال‌های بی‌سیم با هم ارتباط برقرار می‌کنند؛ بنابراین در برابر حملات مخرب آسیب‌پذیر هستند. ایده اصلی مدیریت اعتماد، ایجاد اعتماد بین دو گره منفرد است. مدیریت اعتماد مکانیسمی است که امکان شناسایی گره‌های مخرب، خودخواه و در معرض خطر را نیز فراهم می‌کند.

بر اساس مطالعه انجام‌شده در [۸] مدل‌های محاسبه اعتماد موجود در

1. On-Off Attacks
2. Bad-Mouthing Attacks
3. RobustTrust
4. Simple Multi-Attribute Rating Technique
5. Long Short-Term Memory
6. F-Measure

جدول ۱: خلاصه کارهای پیشین.

رویکرد	سال/ مرجع	تمرکز تحقیق	معایب تحقیق
متمرکز	۲۰۲۱ [۵]	یک رویکرد افزایش اعتماد چندسطحی را برای برنامه‌ریزی کارآمد در محیط‌های ابری موبایل پیشنهاد می‌کند.	در برابر حملات مورد ارزیابی قرار نگرفته است.
	۲۰۱۷ [۶]	اعتماد متمرکز را با استفاده از رویکرد خوشه‌بندی ارائه می‌دهد و به‌صورت رویدادمحور به‌روزرسانی می‌شود.	برتری آن نسبت به تکنیک‌های موجود مبهم است؛ زیرا با سایر طرح‌ها ارزیابی و مقایسه نمی‌شود.
	۲۰۱۹ [۷]	مدیریت اعتماد متمرکز را در سه سطح ارائه داده‌اند و اشیا را بر اساس علایق و شباهت به جوامع مختلف تقسیم کردند. فرایند به‌روزرسانی در سطح پایین به‌صورت رویدادمحور است و در سطح بالا به‌صورت زمان‌محور است.	به صدور گواهینامه‌ها متکی است؛ بنابراین مقیاس‌پذیری سیستم تضمین نمی‌شود.
	۲۰۱۷ [۹]	اعتماد اجتماعی متمرکز را با استفاده از رویکرد خوشه‌بندی ارائه داده‌اند و در پیش‌بینی اعتماد از تکنیک فیلتر کالمن برای تخمین گره‌ها استفاده می‌کند.	در برابر حملات بددهان مورد ارزیابی قرار نگرفته است.
توزیع‌شده	۲۰۱۹ [۱۱]	مدیریت اعتماد توزیع‌شده را ارائه داده‌اند و با استفاده از پارامترهای دانش، شهرت و تجربه اعتماد را محاسبه کرده‌اند. به‌صورت رویدادمحور به‌روزرسانی می‌شود.	میزان مصرف انرژی در مقایسه با کارهای مشابه افزایش یافته و نیز قابلیت سازگاری در مقایسه با کارهای مشابه کمتر است.
	۲۰۱۸ [۱۲]	با درنظرگرفتن اعتمادبه‌نفس (SLT)، اعتماد اجتماعی (ST)، اعتماد سبز (GT) و اعتماد QoS، یک معماری مدیریت اجتماعی مبتنی بر جامعه را پیشنهاد می‌کند.	مقدار انرژی بالایی برای انجام محاسبات استفاده می‌کند.
	۲۰۲۲ [۱۳]	مدلی را برای مدیریت اعتماد بر اساس تکنیک رتبه‌بندی چند ویژگی ساده (SMART) و الگوریتم حافظه کوتاه‌مدت بلندمدت (LSTM) پیشنهاد می‌کند.	در برابر حملات مورد ارزیابی قرار نگرفته است.

سیستم‌های اینترنت اشیا بر اساس پنج بعد اساسی برای یک مدل محاسبه اعتماد طراحی می‌شوند که شامل ترکیب اعتماد، انتشار اعتماد، تجمیع اعتماد، به‌روزرسانی اعتماد و شکل‌گیری اعتماد است. هر یک از ابعاد طراحی را به‌صورت مختصر بیان می‌کنیم. ترکیب اعتماد به‌مواردی گفته می‌شود که در محاسبه اعتماد در نظر می‌گیرند و شامل اعتماد به کیفیت سرویس‌ها (QoS)[1] و اعتماد اجتماعی است. انتشار اعتماد به چگونگی انتشار شواهد اعتماد به همسایگان اشاره دارد. به‌طور کلی، دو طرح انتشار اعتماد وجود دارد؛ توزیع‌شده و متمرکز. جمع‌آوری اعتماد به جمع‌آوری شواهد اعتماد از طریق مشاهدات مستقیم خود یا بازخورد از همسایگان اشاره دارد. تکنیک‌های عمده تجمع اعتماد شامل مجموع وزنی، نظریه اعتقاد، استنباط بیزی، منطق فازی و تحلیل رگرسیون است. هنگام به‌روزرسانی اعتماد، نگرانی‌های به‌روزرسانی اعتماد وجود دارد و به‌طور کلی، دو رویکرد وجود دارد: رویدادمحور و زمان‌محور. شکل‌گیری اعتماد به چگونگی شکل‌گیری اعتماد کلی از چندین ویژگی اعتماد اشاره دارد و از جنبه اعتماد منفرد یا اعتماد چندگانه در نظر گرفته شده است.

با توجه به ابعاد محاسبه اعتماد در ادامه هر یک از ابعاد طرح پیشنهادی را بیان می‌کنیم.

۳-۱ جمع‌آوری اعتماد

در روش پیشنهادی بعد از انجام هر معامله بین دو گره، اگر معامله موفق باشد پاداشی برای گره در نظر گرفته می‌شود و اگر معامله ناموفق باشد مجازاتی برای آن گره در نظر گرفته می‌شود و سپس مقدار اعتماد از مجموع پاداش و مجازات در نظر گرفته‌شده، محاسبه و به‌عنوان مقدار اعتماد جدید در جدول اعتماد ذخیره می‌شود. بعد از انجام هر معامله اگر معامله موفقیت‌آمیز باشد مقدار پاداش از فرمول زیر به‌دست می‌آید

$$Success = Success + ۱ \quad (۱)$$

$$R_s = \frac{Success}{Total} \times \beta^{\Delta t} \quad (۲)$$

$$N_j = R_s \times W_{sj} \quad (۳)$$

که $Success$ تعداد معاملات موفقی که با این گره داشته و $Total$ تعداد کل معاملاتی که با این گره داشته و R_s پاداشی که بعد از انجام معامله موفق به گره همسایه می‌دهد، است. W_{sj} وزن سرویس است و برای هر کدام از سرویس‌ها با توجه به انرژی، حافظه و پردازش، وزن‌های متفاوتی در نظر گرفته شده است. N_j مقدار پاداشی است که برای این سرویس گره مورد نظر محاسبه شده است.

اگر معامله ناموفق باشد مقدار اعتماد از (۴) تا (۷) به‌دست می‌آید

$$Failure = Failure + ۱ \quad (۴)$$

$$onoff = onoff + ۱ \quad (۵)$$

$$P_s = -\log(۲ \times (\frac{Failure}{Total} + onoff) \times FailedRepeated) \times \beta^{\Delta t} \quad (۶)$$

$$N_j = P_s \times W_{sj} \quad (۷)$$

که $Failure$ تعداد تعاملات ناموفقی که با این گره داشته و $Total$ تعداد کل معاملاتی که با این گره داشته، است. $onoff$ پارامتری است که برای تشخیص حملات روشن- خاموش در نظر گرفته شده است. هر وقت معامله‌ای ناموفق و معامله قبلی آن موفق باشد، مقدار متغیر $onoff$ افزایش می‌یابد. اگر تعداد معاملات ناموفق مکرر افزایش یابد، مقدار اعتماد باید بسیار کاهش یابد؛ بنابراین متغیر $FailedRepeated$ در نظر گرفته شده که اگر معامله‌ای ناموفق و معامله قبلی نیز ناموفق باشد مقدار این متغیر افزایش می‌یابد. P_s مجازاتی است که بعد از انجام معامله ناموفق به گره همسایه اختصاص می‌دهد و N_j مقدار اعتمادی است که برای این سرویس محاسبه شده است. بعد از محاسبه پاداش و مجازات مقدار اعتماد از مجموع آنها محاسبه می‌شود.

مقدار اعتماد هر گره با گذشت زمان تغییر می‌کند. اگر دو گره در مدت زمان طولانی با هم تراکنش نداشته باشند، مقدار اعتماد محاسبه‌شده در مراحل قبل اهمیت خود را از دست می‌دهد. دلیل این امر آن است که گره مطمئن نیست آیا گره سرویس‌دهنده هنوز قابل اطمینان است یا خیر و در نتیجه باعث می‌شود گره سرویس‌گیرنده را در محاسبه اعتماد دچار اشتباه کند. در روش پیشنهادی برای اینکه فاصله زمانی بین تراکنش‌ها نیز در

1. Quality of Service

نظر گرفته شود، بعد از محاسبه پاداش و مجازات هر گره، مقدار اعتماد به‌دست‌آمده را در مقدار $\beta^{\Delta t}$ ضرب می‌کنیم که β در اینجا عددی بین ۰ و ۱ و Δt اختلاف زمانی تراکنش‌های انجام‌شده بین دو گره است. هرچه اختلاف زمانی بیشتر باشد، مقدار اعتماد کمتر تغییر می‌کند. مقدار β هرچه کمتر باشد تأثیر گذشت زمان را بیشتر خواهد کرد و میزان اهمیت پاداش یا مجازات کمتر می‌شود.

۳-۲ به‌روزرسانی اعتماد

ارزیابی اعتماد غیرمستقیم در محاسبه اعتماد، جنبه قابل توجهی دارد؛ زیرا وقتی یک گره اطلاعات لازم را برای محاسبه اعتماد به یک گره خاص در اختیار ندارد، آن گره از گره‌های همسایه درخواست می‌کند تا تجربه خود را در مورد یک گره خاص به اشتراک بگذارند [۱۴].

در روش پیشنهادی برای بالابردن کارایی سیستم، اعتماد به‌صورت رویدادمحور به‌روزرسانی می‌شود. هر گره بعد از انجام هر تراکنش و محاسبه اعتماد، مقدار اعتماد محاسبه‌شده را در اختیار همسایگان خود قرار می‌دهد. برای کاهش حجم ترافیک به‌جای ارسال کل جدول اعتماد، فقط اعتماد گرهی را که با آن تراکنش داشته و مقدار آن را محاسبه کرده است ارسال می‌کند. گره برای اینکه تشخیص بدهد توصیه‌ای که گره همسایه ارسال کرده یک توصیه خوب است یا نه، از روش زیر استفاده می‌کند

$$\theta = \left| RecommenderTrust - OldTrust \right| \qquad (۸)$$

در (۸) $RecommenderTrust$ مقدار اعتماد توصیه‌شده گره همسایه و $OldTrust$ مقدار اعتماد محاسبه‌شده از معامله قبلی است که در جدولش ذخیره کرده است. اگر اختلاف این دو مقدار بیشتر از Qr شد، گره نتیجه می‌گیرد که این توصیه، یک توصیه بد است و جدولش را به‌روزرسانی نمی‌کند و اگر اختلاف کم بود، مقدار اعتماد جدول خود را به‌روزرسانی می‌کند و به این طریق از حملات بددهان جلوگیری می‌شود. گره با استفاده از فرمول زیر مقدار اعتماد خود را به‌روزرسانی می‌کند

$$NewTrust = \alpha \times OldTrust + (۱-\alpha) \times RecommenderTrust \qquad (۹)$$

با استفاده از (۹) ضریب اعتماد توصیه‌شده را مدیریت می‌کنیم؛ به این صورت که در این فرمول تأثیر اعتماد توصیه‌شده کمتر در نظر گرفته شده تا از حملات بددهان جلوگیری شود.

برای جلوگیری از حملات هوشمندانه که گره‌های مخرب، پیشنهادهای بد را با اختلاف کم ولی تعداد زیاد ارسال کنند، هر گره تعداد محدودی پیشنهاد را قبول می‌کند. گره بعد از این که تعداد محدودی پیشنهاد خوب را در مورد یک گره قبول کرد، دیگر تا وقتی که دوباره خودش با گره مورد نظر تراکنش نداشته باشد پیشنهادی قبول نمی‌کند.

یک سیستم اینترنت اشیا با پیوستن گره‌های جدید و خروج گره‌های موجود تکامل می‌یابد. یک پروتکل مدیریت اعتماد باید به این موضوع بپردازد تا به گره‌های جدید که به شبکه می‌پیوندند اجازه دهد تا سریعاً و با درجه‌ای از دقت معقول اعتماد را به‌دست آورد [۱۵]. در روش پیشنهادی، وقتی گره جدیدی وارد شبکه می‌شود تا قبل از اینکه با گرهی تبادل داشته باشد تعداد محدودی پیشنهاد را پذیرفته و مقدار اعتماد خود را آپدیت می‌کند؛ بنابراین گرهی که جدید وارد شبکه می‌شود سریع‌تر مقدار اعتماد را محاسبه می‌کند. وقتی گره جدیدی وارد سیستم می‌شود، مقدار اعتماد تمام گره‌ها را صفر در نظر گرفته است؛ بنابراین اختلاف اعتمادش با مقدار پیشنهادی بیشتر از Qr می‌شود و اعتماد را آپدیت نمی‌کند؛ به همین دلیل ما برای گره‌هایی که هنوز هیچ تراکنشی نداشته‌اند Qr را چک نمی‌کنیم. گره تازه‌وارد تا قبل از آنکه خودش با گره مورد نظر تراکنش داشته باشد، فقط تعداد محدودی پیشنهاد را قبول می‌کند و حتی اگر پیشنهاد مخربی به گره تازه‌وارد شود، بعد از آن که گره تازه‌وارد با گره مورد نظر تراکنش داشته باشد، مقدار اعتماد به‌درستی محاسبه می‌شود و مورد حمله قرار نمی‌گیرد. اگر پیشنهادهای مخربی به گره تازه‌وارد فرستاده شود مقدار اعتماد را دیرتر محاسبه می‌کند؛ ولی از آنجا که تعداد گره‌های مخرب کمتر از گره‌های خوب است و گره میانگین ۳ پیشنهاد را محاسبه می‌کند، در بیشتر مواقع گره تازه‌وارد، اعتماد را سریع‌تر محاسبه می‌کند.

۳-۳ انتشار اعتماد

در روش پیشنهادی انتشار اعتماد به‌صورت توزیع‌شده است و گره‌ها بدون نیاز به نهاد مرکزی و به‌طور مستقل، اعتماد همسایگان خود را محاسبه می‌کنند. اهمیت عمده اعتماد توزیع‌شده این است که گره‌ها لازم نیست به هیچ مرجع متمرکزی اعتماد کنند. در روش پیشنهادی هر گره، خودش مقدار اعتماد گره‌هایی را که با آنها تعامل داشته محاسبه می‌کند. هر گره شامل یک جدول اعتماد است که به تعداد همسایگان گره، رکورد دارد و اطلاعاتی مانند شناسه گره همسایه، مقدار اعتماد محاسبه‌شده، تعداد تراکنش‌های خوب و تعداد تراکنش‌های بد را ذخیره می‌کند.

۳-٤ ترکیب اعتماد

در روش پیشنهادی، اعتماد یک گره با استفاده از زمان پاسخگویی که یکی از معیارهای کیفیت سرویس (QoS) است و توصیه‌های همسایگان محاسبه می‌شود. در اینترنت اشیا یک گره ممکن است بعد از یک دوره زمانی یا بعد از چند تراکنش خوب به‌عنوان یک گره مخرب عمل کند؛ پس در روش پیشنهادی، اعتماد هر گره را با توجه به تراکنشی که الآن با آن گره داشته و سابقه گره و توصیه‌های همسایگان محاسبه می‌کنیم. در این روش هر گره با توجه به زمان پاسخگویی گره مقابل و سابقه آن، مقدار اعتماد آن گره را محاسبه می‌کند. همچنین هر گره می‌تواند چندین سرویس را ارائه دهد و برای هر کدام از سرویس‌ها با توجه به انرژی، حافظه و پردازش، وزن‌های متفاوتی (W_{sj}) در نظر گرفته شده است. وزن هر سرویس را با توجه به رابطه زیر محاسبه می‌کنیم

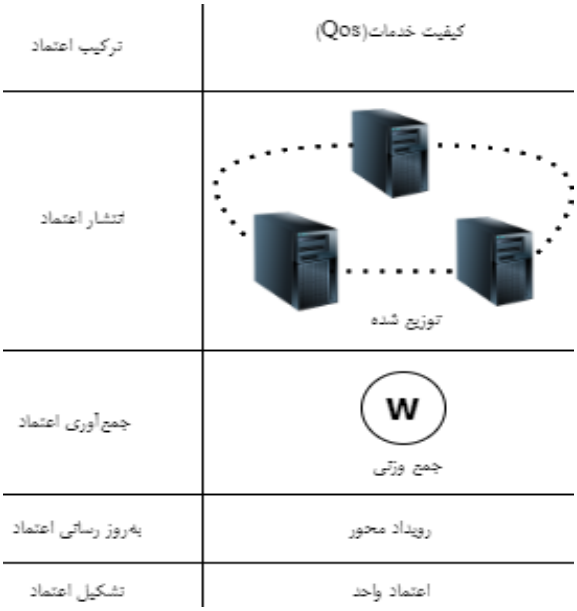
$$W_{sj} = S_j \times \sigma \qquad (۱۰)$$

در (۱۰)، σ مقداری بین صفر و یک دارد و برای به‌هنجارکردن W استفاده می‌شود. S_j مقداری است که با توجه به انرژی، حافظه و پردازش به هر سرویس اختصاص می‌دهیم و سرویس‌هایی که حساسیت بیشتری دارند و یا به ظرفیت پردازش بیشتری نیاز دارند دارای S_j بالاتری هستند و سرویس‌هایی که به منابع زیادی احتیاج ندارند، S_j کمتری دارند. هرچه مقدار S_j بزرگ‌تر باشد مقدار اعتماد سریع‌تر همگرا می‌شود.

۳-۵ شکل‌گیری اعتماد

در روش پیشنهادی، شکل‌گیری اعتماد به‌صورت اعتماد منفرد به‌کار گرفته شده و فقط یک ویژگی اعتماد در پروتکل اعتماد در نظر گرفته شده است. در این روش ما از زمان پاسخگویی استفاده کرده‌ایم که یکی از معیارهای کیفیت سرویس است و مهم‌ترین معیار در سیستم‌های اینترنت اشیای سرویس‌گرا محسوب می‌شود.

همان طور که در شکل ۱ آمده است در طراحی روش پیشنهادی برای ترکیب اعتماد از کیفیت خدمات، برای انتشار اعتماد از روش توزیع‌شده، برای جمع‌آوری اعتماد از روش جمع وزنی با مشاهدات مستقیم و غیرمستقیم، برای به‌روزرسانی اعتماد از روش رویدادمحور و برای تشکیل



شکل ۱: روش پیشنهادی.

اعتماد از اعتماد واحد استفاده شده است.

به‌طور کلی در روش پیشنهادی با توجه به تراکنش‌های گذشته و تراکنش فعلی بین دو گره، مقدار اعتماد محاسبه شده و در جدول اعتماد گره ذخیره می‌شود. سپس گره مورد نظر، مقدار اعتماد محاسبه‌شده را در اختیار همسایگان خود قرار می‌دهد. گره همسایه با توجه به مقدار اعتمادی که خودش قبلاً محاسبه کرده و مقدار اعتماد پیشنهادشده با استفاده از روش جمع وزنی، مقدار اعتماد خود را به‌روزرسانی می‌کند.

٤- نتایج شبیه‌سازی

در این مقاله روش پیشنهادی با روش DDTMS [۱۶] مقایسه گردیده است. در روش DDTMS رفتار گره را با توجه به ارائه یا رد سرویس‌های درخواستی، ارزیابی و اعتماد را محاسبه می‌کنند. در روش DDTMS هنگامی که یک گره به‌عنوان گره مخرب شناسایی می‌شود، گره تعاملات آینده خود را با آن متوقف می‌کند و به سایر گره‌های همسایه نیز اطلاع می‌دهد. DDTMS تنها حمله روشن- خاموش یک گره مخرب را شناسایی می‌کند. شبکه شبیه‌سازی‌شده هر کدام از روش‌ها شامل ۵۰ گره Tmote Sky است که از این ۵۰ گره، ۱۰ گره به‌عنوان گره مخرب شبیه‌سازی شده‌اند و گره‌ها به‌طور تصادفی توزیع شده است. مقدار W_{sj} برای گره‌ها در هر دو شبیه‌سازی (روش پیشنهادی و روش DDTMS) ۰/۱ در نظر گرفته شده است. همچنین شبیه‌سازی هر دو روش در ۵ مرحله و شرایط یکسان انجام گردیده و نمودار میانگین نتایج، رسم و در جدول ۲ مقدار متغیرها بیان شده است.

٤-۱ محیط شبیه‌سازی

شبیه‌سازی در محیط COOJA موجود در سیستم‌عامل Contiki انجام شده است. شبیه‌ساز کوجا محیطی برای شبیه‌سازی اینترنت اشیاست که در سیستم عامل Contiki قرار دارد. Contiki یک سیستم‌عامل متن‌باز برای سیستم‌های تحت شبکه با حافظه محدود است. تمرکز سیستم‌عامل Contiki بر روی وسیله‌های اینترنت اشیای بی‌سیم با انرژی محدود و شبیه‌سازی اپلیکیشن‌های اینترنت اشیاست. از مزایای قابل توجه کوجا می‌توان به محیط گرافیکی و کاربردی آن اشاره کرد که شبیه‌سازی را بسیار آسان‌تر می‌کند. نصب و اجرای کوجا نیز پیچیدگی زیادی ندارد.

جدول ۲: مقدار متغیرها.

متغیر	مقدار
اختلاف اعتماد محاسبه‌شده و اعتماد پیشنهادی (Qr)	۰/۲
وزن سرویس (W_{sj})	۰/۱
تعداد پیشنهادها (x)	۳
ضریب جمع وزنی (α)	۰/۳۳

جدول ۳: پارامترهای شبیه‌سازی.

پارامتر	مقدار
شبیه‌ساز	Cooja under Contiki ۳.۰ OS
محیط رادیویی	Unit disk graph medium (UDGM)
محدوده تحت پوشش هر گره	۵۰ متر
نوع گره‌ها	Sky mote
تعداد گره‌ها	۵۰ گره
لایه فیزیکی	IEEE ۸۰۲.۱۵.۴
لایه MAC	IPv۶
لایه شبکه	RPL
لایه انتقال	UDP
مدت‌زمان شبیه‌سازی	یک ساعت
نرخ ارسال بسته	۱ بسته در هر ۲۰ تا ۶۰ ثانیه

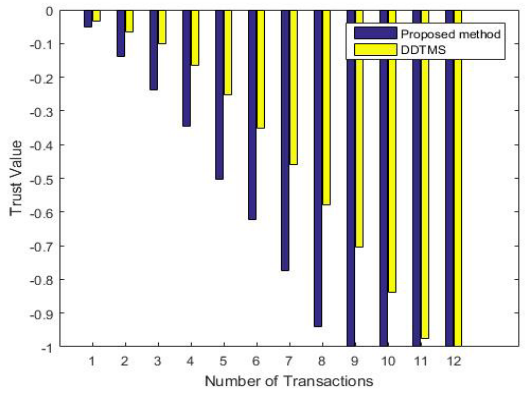
همچنین بسیاری از پروتکل‌ها و استانداردهای رایج و مرسوم اینترنت اشیا و شبکه‌های بی‌سیم به‌صورت پیش‌فرض تعبیه شده‌اند. کوجا شبیه‌سازی سطح متقابل را امکان‌پذیر و شبیه‌سازی سطح پایین سخت‌افزار و شبیه‌سازی سطح بالا را در یک شبیه‌سازی واحد ترکیب می‌کند. از این جهت انعطاف‌پذیر و توسعه‌پذیر است که تمام سطوح سیستم را می‌توان تغییر داد یا جایگزین کرد. شبیه‌ساز کوجا در جاوا پیاده‌سازی شده و این باعث می‌شود که به‌راحتی برای کاربران گسترش یابد؛ اما اجازه می‌دهد تا نرم‌افزار گره با استفاده از رابط محلی جاوا به زبان C یا C++ نوشته شود [۱۷].

ما یک شبکه حسگر بی‌سیم را شبیه‌سازی کردیم که دما را اندازه‌گیری و اطلاعات را با یکدیگر تبادل می‌کند. ابعاد محیط شبیه‌ساز را ۶۰۰ متر در ۶۰۰ متر در نظر گرفتیم و بنابراین ۵۰ گره در این محیط قرار داده‌ایم که از نوع Sky mote هستند؛ زیرا این نوع، گره‌های حسگر بی‌سیم را شبیه‌سازی می‌کند و تا فاصله ۵۰ متری قابلیت ارتباط با گره‌های دیگر را دارد. از استاندارد IEEE ۸۰۲.۱۵.۴ برای لایه فیزیکی استفاده شده که برای انتقال داده‌های حسگر بی‌سیم استفاده می‌شود. از پروتکل IPv۶ در لایه MAC استفاده شده تا هر گره، آدرس دستگاه‌های دیگر را بشناسد. همچنین از پروتکل RPL برای لایه شبکه استفاده می‌شود تا مسیریابی کم‌مصرف با امکان از دست دادن بسته‌ها فراهم شود و از پروتکل UDP برای انتقال داده‌ها در لایه انتقال استفاده می‌شود. مدت زمان شبیه‌سازی یک ساعت در نظر گرفته شده است. با توجه به حساسیت دما هر حسگر هر ۲۰ تا ۶۰ ثانیه یک بسته داده را به گره‌های دیگر ارسال می‌کند. در این شبیه‌سازی، هر گره حسگر بی‌سیم، دما را اندازه‌گیری و اطلاعات آن را به گره‌های دیگر ارسال می‌کند. پارامترهای شبیه‌سازی در جدول ۳ قابل مشاهده است

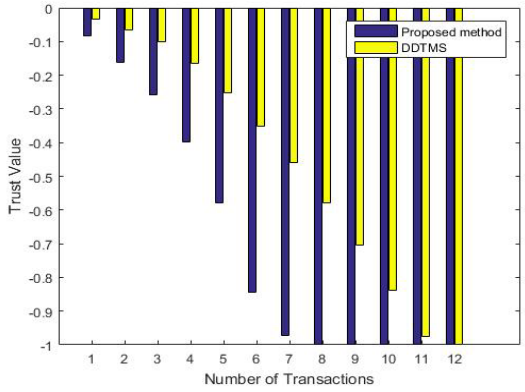
٤-۲ نتایج ارزیابی

٤-۲-۱ محاسبه اعتماد گره مخرب

در روش‌های مدیریت اعتماد، تشخیص گره مخرب از اهمیت زیادی



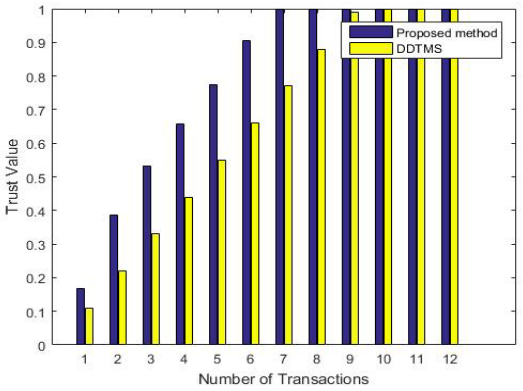
شکل ۲: مقایسه اعتماد محاسبه‌شده گره مخرب در طول زمان در هر دو روش با محدودیت تعداد پیشنهادها.



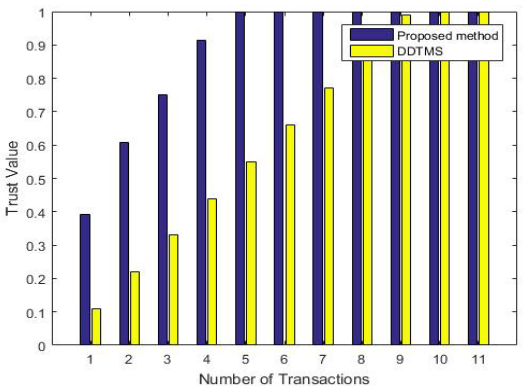
شکل ۳: مقایسه اعتماد محاسبه‌شده گره مخرب در طول زمان در هر دو روش بدون محدودیت تعداد پیشنهادها.

برخوردار است. برای ارزیابی اعتماد گره‌های مخرب، ۵۰ گره به‌طور تصادفی در شبکه توزیع شده‌اند که از این ۵۰ گره، ۱۰ گره به‌عنوان گره مخرب هستند. منظور از گره مخرب گرهی است که بیشتر مواقع درخواست‌ها را پاسخ نمی‌دهد. مقدار اعتماد محاسبه‌شده گره مخرب که توسط یکی از گره‌ها محاسبه شده است، در شکل ۲ آمده و مقدار اعتماد گره مخرب در دو روش با هم مقایسه شده است. همان طور که دیده می‌شود در مدل مدیریت اعتماد پیشنهادی در مقایسه با روش DDTMS، هم در زمان زودتر و هم در تعداد تراکنش کمتر، مقدار اعتماد گره مخرب به سمت کمینه رفته است. زیرا در روش پیشنهادی هر گره بعد از هر بار تراکنش، اعتماد را محاسبه کرده و اطلاعات خود را در اختیار همسایگان قرار می‌دهد. هر گره هنگامی که ارزش اعتمادی به آن پیشنهاد شود بر اساس حداکثر ۳ پیشنهاد جدول اعتماد خود را به‌روزرسانی می‌کند؛ به همین دلیل گره‌های همسایه، قبل از تراکنش بعدی مقدار اعتماد خود را با توجه به مشاهدات غیرمستیم، به‌روزرسانی می‌کنند و بنابراین شناسایی گره‌های مخرب در زمان کمتر و تعداد تراکنش کمتر انجام می‌شود؛ اما در روش DDTMS پیشنهادهای همسایگان و مشاهدات غیرمستقیم وجود ندارد و مقدار اعتماد فقط بعد از هر بار تراکنش به‌روزرسانی می‌شود.

ما برای محاسبه اعتماد گره مخرب، حالتی را در نظر گرفتیم که گره مورد نظر تمام پیشنهادهای همسایگان را قبول کند و محدودیتی در تعداد پیشنهادها نگذاشتیم. همان طور که در شکل ۳ مشاهده می‌کنید مقدار اعتماد نسبت به حالتی که فقط ۳ پیشنهاد را قبول می‌کند در زمان زودتر و تعداد تراکنش کمتر محاسبه شده است؛ اما ریسک حملات هوشمندانه را دارد. در این حالت هرچه تعداد همسایگان گره بیشتر باشد، مقدار اعتماد سریع‌تر محاسبه می‌شود؛ زیرا تعداد پیشنهادها، بیشتر و مقدار اعتماد، سریع‌تر همگرا می‌شود.



شکل ۴: مقایسه اعتماد محاسبه‌شده گره درستکار در طول زمان در هر دو روش با محدودیت تعداد پیشنهادها.



شکل ۵: مقایسه اعتماد محاسبه‌شده گره درستکار در طول زمان در هر دو روش بدون محدودیت تعداد پیشنهادها.

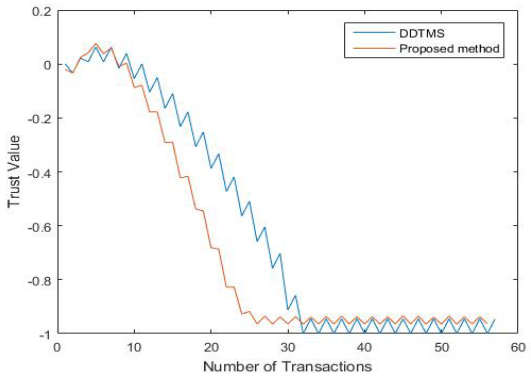
٤-۲-۲ محاسبه اعتماد گره درستکار

با توجه به این که در یک مدل مدیریت اعتماد، علاوه بر تشخیص گره‌های مخرب، شناسایی گره‌های درستکار در زمان مناسب نیز اهمیت دارد، در شکل ۴ اعتماد محاسبه‌شده گره‌های درستکار در دو روش با هم مقایسه شده است. در این سناریو تمام ۵۰ گره، گره‌های درستکار هستند. منظور از گره درستکار، گرهی است که درخواست‌های سرویس‌گیرنده را جواب می‌دهد. در شبیه‌سازی گره‌های درستکار نیز مقدار W_{sj} برای گره‌های درستکار در هر دو روش ۰/۱ در نظر گرفته شده و مقدار اعتماد محاسبه‌شده یکی از گره‌ها در هر دو روش رسم شده است. همان طور که می‌بینیم روش پیشنهادی در گره‌های درستکار، هم در زمان خیلی کمتر و هم تعداد تراکنش‌های کمتر، مقدار اعتماد را محاسبه کرده است.

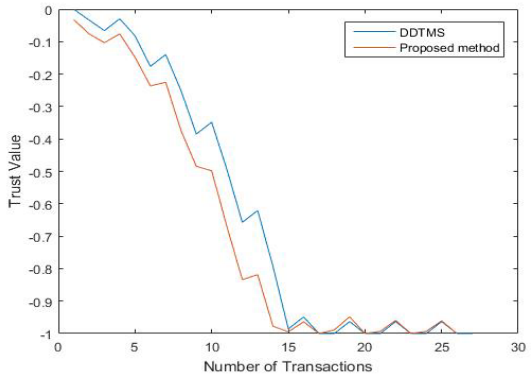
در محاسبه گره درستکار همچنین ما حالتی را در نظر گرفتیم که تمام پیشنهادها را قبول کند و محدودیتی در قبول پیشنهادها نداشته باشد. همان طور که در شکل ۵ مشاهده می‌کنید در این حالت، خیلی سریع‌تر و در تعداد تراکنش کمتر، مقدار اعتماد محاسبه شده است.

٤-۲-۳ تشخیص حمله روشن- خاموش

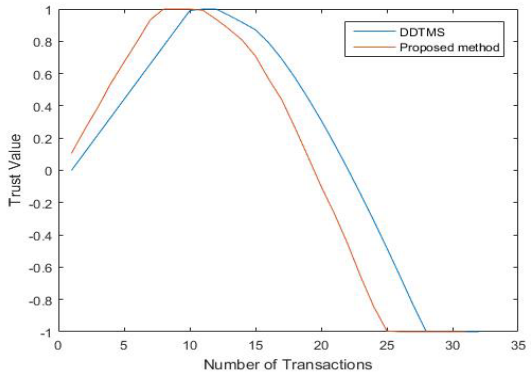
در روش پیشنهادی برای تشخیص حمله روشن- خاموش از پارامتر *onoff* استفاده شده و اگر تراکنشی ناموفق و تراکنش قبلی آن موفق باشد، مقدار آن را افزایش می‌دهیم. برای ارزیابی تشخیص حمله روشن- خاموش ما سه سناریو را شبیه‌سازی کرده‌ایم. در سناریوی اول، گرهی را شبیه‌سازی کردیم که از هر ۲ درخواست، یکی را پاسخ می‌دهد و سپس مقدار اعتماد آن گره را محاسبه و دو روش را با هم مقایسه کرده‌ایم. همان طور که در شکل ۶ می‌بینید، هر دو روش گره مخرب را به‌درستی



شکل ۶: تشخیص موفق حمله روشن‌خاموش در هر دو روش در سناریوی از هر ۲ درخواست یکی پاسخ داده شود.



شکل ۷: تشخیص موفق حمله روشن‌خاموش در هر دو روش در سناریوی از هر ۳ درخواست یکی پاسخ داده شود.

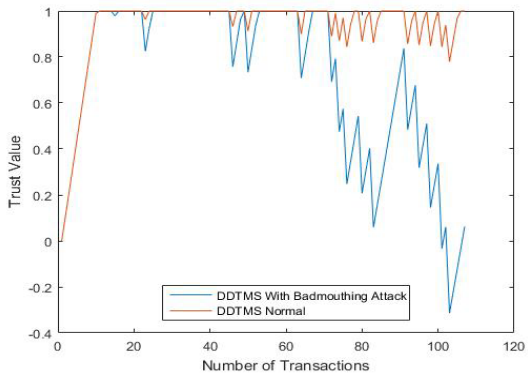


شکل ۸: تشخیص موفق حمله روشن‌خاموش در هر دو روش در سناریوی بعد از مدتی پاسخ ندهد.

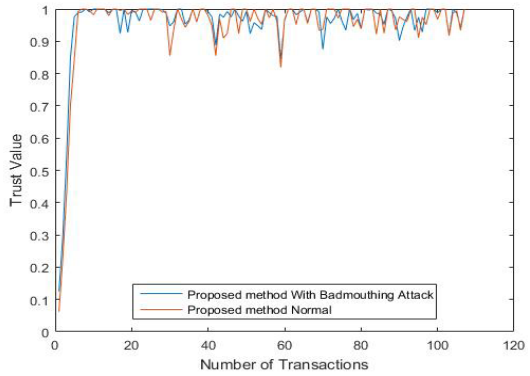
تشخیص داده‌اند؛ اما در روش پیشنهادی چون مقدار اعتماد محاسبه‌شده را با همسایگان به اشتراک می‌گذاریم، گره‌ها حمله روشن- خاموش را در زمان زودتر و تعداد تراکنش کمتر تشخیص داده‌اند. همچنین مقدار اعتماد محاسبه‌شده در روش پیشنهادشده، حتی کمتر از مقدار اعتماد روش DDTMS است.

در سناریوی بعدی ما گرهی را شبیه‌سازی کرده‌ایم که از هر ۳ درخواست، یکی را پاسخ می‌دهد و سپس مقدار اعتماد این گره را محاسبه و نمودار دو روش را رسم کرده‌ایم. همان طور که در شکل ۷ دیده می‌شود هر دو روش، حمله را به‌درستی تشخیص داده‌اند و مقدار اعتماد را ۱- محاسبه کرده‌اند.

در سناریوی آخر برای تشخیص حمله روشن- خاموش، ما گرهی را در نظر گرفتیم که چند دقیقه اول تمام درخواست‌ها را پاسخ می‌دهد و بعد از مدتی درخواست‌ها را پاسخ نمی‌دهد و نمودار محاسبه اعتماد آن گره در



شکل ۹: تشخیص ناموفق حمله بددهان در روش DDTMS.



شکل ۱۰: تشخیص موفق حمله بددهان در روش پیشنهادی. (در متن ارجاع ندارد)

هر دو روش رسم شده است. در این سناریو هم همان طور که در شکل ۸ مشاهده می‌شود، هر دو روش حمله را به‌درستی تشخیص داده و مقدار اعتماد گره را ۱- محاسبه کرده‌اند.

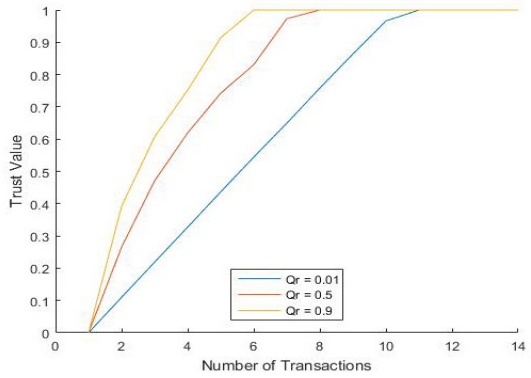
٤-۲-٤ تشخیص حمله بددهان

در مطالعه انجام‌شده علاوه بر حمله روشن- خاموش، حمله بددهان نیز مورد ارزیابی قرار گرفته است. در روش پیشنهادی، گره‌ها وقتی مقدار اعتمادی را به آنها پیشنهاد می‌دهند با مقدار اعتماد خود مقایسه می‌کنند و اگر اختلاف مقدارها زیاد نبود، اعتماد خود را به روش جمع وزنی آپدیت کرده و به همین دلیل مورد حمله بددهان واقع نمی‌شوند. برای ارزیابی حمله بددهان، گره بدگویی را شبیه‌سازی کرده‌ایم که مدام اعتماد گره‌های دیگر را عدد ۱- گذاشته و برای گره‌های همسایه ارسال می‌کند. همچنین گرهی را شبیه‌سازی کرده‌ایم که ۸۰ درصد مواقع، پاسخ درخواست‌ها را می‌دهد و مقدار اعتماد آن را محاسبه کرده‌ایم. مقدار اعتماد گره را یک بار با وجود گره بددهان و یک بار بدون گره بددهان محاسبه کرده و نمودار مقدار اعتماد به‌دست‌آمده را رسم کرده‌ایم.

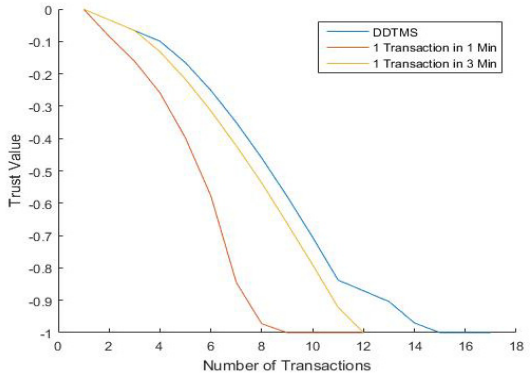
همان طور که در شکل ۹ دیده می‌شود، در روش DDTMS به‌راحتی مورد حمله بددهان قرار گرفته و مقدار اعتماد یک گره خوب را که باید مقدار اعتماد محاسبه‌شده بالای ۰٫۸ باشد، حتی در بعضی مواقع تا ۰٫۳- نیز محاسبه کرده است. اما در روش پیشنهادی چون مقدار اعتماد پیشنهادشده را با مقدار اعتمادی که خودش محاسبه کرده، مقایسه می‌کند، مورد حمله بددهان قرار نگرفته و همان طور که در شکل ۱۰ مشاهده می‌کنید، مقدار اعتماد با وجود گره بددهان و بدون گره بددهان، تقریباً نزدیک به هم محاسبه شده است.

٤-۲-٥ اهمیت انتخاب Qr

در روش پیشنهادی برای جلوگیری از حملات بددهان، ما مقدار اعتماد پیشنهادی را با مقدار اعتمادی که خود گره محاسبه کرده است مقایسه



شکل ۱۱: نمودار مقایسه مقدار Qr در روش پیشنهادی.



شکل ۱۲: مقایسه اعتماد گره مخرب در تراکنش‌هایی با فاصله زمانی مختلف.

می‌نماییم و اگر اختلاف این دو مقدار کمتر از Qr بود، مقدار اعتماد را به‌روزرسانی می‌کنیم. در این قسمت برای نشان‌دادن اهمیت انتخاب Qr، نمودار مقدار اعتماد محاسبه‌شده گره درستکار را با Qrهای متفاوت رسم کردیم. در شکل ۱۱ نمودار محاسبه اعتماد گره درستکار را با Qrهای ۰/۰۱، ۰/۵ و ۰/۹ رسم کرده‌ایم. همان طور که مشاهده می‌کنید هرچه مقدار Qr کوچک‌تر باشد، گره مقدار اعتماد را به‌روزرسانی نمی‌کند و بنابراین مقدار اعتماد در زمان دیرتر و تعداد تراکنش بیشتر به حالت پایدار می‌رسد و هرچه مقدار Qr بزرگ‌تر باشد، گره با پیشنهادهای بیشتری مقدار اعتماد را به‌روزرسانی می‌کند و در زمان سریع‌تر و تعداد تراکنش کمتر مقدار اعتماد را تشخیص می‌دهد. اما اگر Qr مقدار بالایی داشته باشد احتمال تشخیص حملات بدگویی سخت‌تر می‌شود و بنابراین در انتخاب Qr باید دقت داشت و آن را مناسب انتخاب کرد. ما در این روش برای جلوگیری از حملات بددهان مقدار Qr را ۰/۲ قرار داده‌ایم.

٤-٢-٦ اهمیت زمان در محاسبه اعتماد

هنگامی که دو گره در مدت زمان طولانی با هم تراکنش نداشته‌اند، مقدار اعتمادی که گره قبلاً محاسبه کرده است باید ارزش کمتری داشته باشد؛ زیرا ممکن است گره در این فاصله زمانی رفتار متفاوتی داشته باشد. برای نشان‌دادن اهمیت زمان در محاسبه اعتماد، گره‌های مخربی را شبیه‌سازی کردیم که در فاصله زمانی ۳ تا ۴ دقیقه با هم تراکنش داشته باشند و بعد مقدار اعتماد را با حالتی که ۲۰ تا ۶۰ ثانیه‌ای یک بار تراکنش داشته باشند مقایسه انجام شده است. همان طور که در شکل ۱۲ مشاهده می‌کنید هرچه فاصله زمانی دو تراکنش بیشتر باشد، مقدار اعتماد در زمان دیرتر و تعداد تراکنش بیشتر محاسبه می‌شود. نمودار این دو حالت را با روش DDTMS که تراکنش‌ها در همان فاصله ۲۰ تا ۶۰ ثانیه، انجام شده نیز مقایسه کرده‌ایم. مشاهده می‌کنید در حالتی که فاصله تراکنش‌ها سه برابر شده است، همچنان از روش DDTMS، سریع‌تر اعتماد را محاسبه می‌کند.

نتایج ارزیابی نشان می‌دهند روش پیشنهادی در زمان سریع‌تر و تعداد تراکنش کمتر مقدار اعتماد را محاسبه کرده و در برابر حملات روشن- خاموش و بددهان مقاوم است.

۵- نتیجه‌گیری

اینترنت اشیا دنیایی را ایجاد می‌کند که در آن اشیا فیزیکی به‌طور یکپارچه در شبکه‌های اطلاعاتی ترکیب می‌شوند تا سرویس‌های پیشرفته و هوشمندی برای انسان‌ها ارائه کنند. مدیریت اعتماد، نقش مهمی در اینترنت اشیا برای تلفیق و استخراج داده‌های قابل اعتماد، خدمات واجد شرایط و افزایش حریم خصوصی کاربر و امنیت اطلاعات ایفا می‌کند.

در این مقاله مدل مدیریت اعتماد توزیع‌شده برای اینترنت اشیا معرفی شده که با استفاده از تراکنش مستقیم بین دو گره و توصیه‌های همسایگان بعد از هر تراکنش، مقدار اعتماد را محاسبه می‌کند. در روش پیشنهادی در هنگام به‌روزرسانی اعتماد با مقایسه مقدار اعتماد پیشنهادی و محدودکردن تعداد پیشنهادها، علاوه بر حملات روشن- خاموش از حملات بددهان نیز جلوگیری شده و نیز مقدار اعتماد خیلی سریع‌تر و در تعداد تراکنش کمتر از DDTMS محاسبه شده است. روش DDTMS چون فقط اطلاعات گره‌های مخرب را در اختیار همسایگان قرار می‌دهد به‌راحتی می‌تواند مورد حملات بددهان قرار گیرد.

در روش پیشنهادی هرچه تعداد همسایگان درستکار گره بیشتر باشد که اطلاعات درستی در اختیار دیگر گره‌ها قرار دهد، گره مقدار اعتماد را در زمان سریع‌تری محاسبه کرده و همچنین گره‌هایی که جدید وارد شبکه می‌شوند با پیشنهادهایی که از همسایگان درستکار می‌گیرند خیلی سریع‌تر اعتماد را محاسبه می‌کنند. همچنین در این روش با توجه به اینکه برای هر سرویس یک ضریب در نظر گرفتیم در سیستم‌های دارای چند سرویس قابل استفاده و پیاده‌سازی است و با توجه به اینکه در این روش، هر گره فقط با همسایگان خود در ارتباط است و همچنین محاسبات به‌صورت توزیع‌شده انجام شده است، مقیاس‌پذیری بیشتری دارد و برای سیستم‌های بزرگ نیز قابل پیاده‌سازی و اعمال است. اما این روش در سیستم‌های با تحرک زیاد سازگار نیست؛ زیرا گره‌ها با توجه به تراکنش‌های قبلی و تراکنش اکنون اعتماد را محاسبه می‌کنند و وقتی گره دارای تحرک باشد، مدام با همسایگان جدید مواجه می‌شود و هر بار برای گره‌های جدید باید اعتماد را محاسبه کند. بنابراین سرعت محاسبه اعتماد در سیستم‌های با تحرک زیاد پایین می‌آید و همچنین به‌دلیل استفاده از مشاهدات غیرمستقیم سربار ارتباطی بیشتری دارد.

مراجع

[1] R. Thirukkumaran and P. Muthu Kannan, "Survey: security and trust management in Internet of Things," in *Proc. IEEE Global Conf. on Wireless Computing and Networking, GCWCN'18*, pp. 131-134, Lonavala, India, 23-24 Nov. 2018.

[2] L. Yijia, J. Wang, Z. Yan, Z. Wan, and R. Jäntti, "A survey on blockchain-based trust management for Internet of Things," *IEEE Internet of Things J.*, vol. 10, no. 7, pp. 5898-5922, 1 Apr. 2023.

[3] U. Din, M. Guizani, B. S. Kim, S. Hassan, and M. Khurram Khan, "Trust management techniques for the Internet of Things: a survey," *IEEE Access*, vol. 7, pp. 29763-29787, 2019.

[4] S. Dhelim, *et al.*, "Trust2Vec: large-scale IoT trust management system based on signed network embeddings," *IEEE Internet of Things J.*, vol. 10, no. 1, pp. 553-562, 1 Jan. 2022.

[5] A. Ali, *et al.*, "Multilevel central trust management approach for task scheduling on IoT-based mobile cloud computing," *Sensors*, vol. 22, no. 1, Article ID: 108, Jan. 2022.

[6] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, and S. Khan, "StabTrust-a stable and centralized trust-based clustering mechanism for IoT enabled vehicular Ad-Hoc networks," *IEEE Access*, vol. 8, pp. 21159-21177, 2020.

[7] M. D. Alshehri and F. K. Hussain, "A centralized trust management mechanism for the Internet of Things (CTM-IoT)," in *Proc. of 12th Int. Conf.on Broad-Band Wireless Computing, Communication and Applications, BWCCA'18,* pp. 533-543, Barcelona, Spain, 8-10 Nov. 2018.

[8] J. Guo, *Trust-Based Service Management of Internet of Things Systems and Its Applications*, Apr. 2018, Accessed: Jul. 25, 2021. [Online]. Available: https://vtechworks.lib.vt.edu/handle/10919/82854

[9] O. Ben Abderrahim, M. H. Elhdhili, and L. Saidane, "TMCoI-SIOT: a trust management system based on communities of interest for the social Internet of Things," in *Proc. 13th Int. Wireless Communications and Mobile Computing Conf., IWCMC'17*, pp. 747-752, Valencia, Spain , 26-30 Jun. 2017.

[10] Q. Arshad, W. Zada Khan, F. Azam, M. K. Khan, H. Yu, and Y. B. Zikria, "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges," *Complex & Intelligent Systems*, vol. 9, no. 6, pp. 6155-6176, 2023.

[11] K. A. Awan, *et al.*, "RobustTrust-a pro-privacy robust distributed trust management mechanism for Internet of Things," *IEEE Access*, vol. 7, pp. 62095-62106, 2019.

[12] R. Das, M. Singh, and K. Majumder, "SGSQoT: a community-based trust management scheme in Internet of Things," in *Proc. of Int. Ethical Hacking Conf., EHaCON'18*, pp. 209-222, Kolkata, India, 2019.

[13] Y. Alghofaili and M. A. Rassam, "A trust management model for IoT devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique," *Sensors*, vol. 22, no. 2, Article ID: 834, Jan. 2022.

[14] A. Adewuyi, H. Cheng, Q. Shi, J. Cao, Á. MacDermott, and X. Wang, "CTRUST: a dynamic trust model for collaborative applications in the Internet of Things," *IEEE Internet of Things J.*, vol. 6, no. 3, pp. 5432-5445, Jun. 2019.

[15] P. Massa and P. Avesani, "Trust-aware recommender systems," in *Proc. ACM Recommender Systems Conf., RecSys'07*, pp. 17-24, Minneapolis, MN, USA, 19-20 Oct. 2007.

[16] S. W. A. Hamdani, *et al.*, "Dynamic distributed trust management scheme for the Internet of Things," *Turk J. Elec Eng & Comp Sci*, vol. 29, no. 2, pp. 796-815, Mar. 2021.

[17] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne, and T. Voigt, "Cross-level sensor network simulation with COOJA," in *Proc. 31st IEEE Conf. on Local Computer Networks*, pp. 641-648, Tampa, FL, USA, 16-18 Nov. 2006.

زهرا هادیان تحصیلات خود را در مقاطع کارشناسی مهندسی کامپیوتر در سال ۱۳۸۷ در دانشگاه شهید باهنر کرمان به پایان رسانده است، سپس در سال ۱۴۰۰ کارشناسی ارشد خود را در رشته مهندسی کامپیوتر- شبکه‌های کامپیوتری از دانشگاه یزد دریافت کرد. از جمله زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: امنیت شبکه های کامپیوتری، یادگیری ماشین و اینترنت اشیا.

فضل‌الله ادیب‌نیا تحصیلات خود را در مقطع کارشناسی رشته مهندسی کامپیوتر در سال ۱۳۶۵ در دانشگاه صنعتی اصفهان و مقاطع کارشناسی ارشد مهندسی کامپیوتر را در سال ۱۳۶۸ در دانشگاه صنعتی شریف به پایان رسانده است وی همچنین دکتری تخصصی در رشته مهندسی کامپیوتر را در دانشگاه برمن آلمان در سال ۱۳۷۸ به پایان رساند. هم اکنون دانشیار دانشکده مهندسی کامپیوتر دانشگاه یزد می‌باشد. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: رایانش مه و ابری، امنیت شبکه، شبکه‌های بی‌سیم و سیار.

وحید رنجبر تحصیلات کارشناسی خود را در دانشگاه صنعتی شیراز در رشته مهندسی فناوری اطلاعات در سال ۱۳۹۰ گذراند و مقطع کارشناسی ارشد فناوری اطلاعات خود را در دانشگاه صنعتی شریف در سال ۱۳۹۲ به پایان رساند، سپس در سال ۱۳۹۷ دکتری فناوری اطلاعات خود را از دانشگاه تهران دریافت کرد. وی هم‌اکنون استادیار دانشکده مهندسی کامپیوتر دانشگاه یزد است و زمینه های تحقیقاتی مورد علاقه ایشان امنیت اطلاعات و شبکه، تحلیل شبکه‌های اطلاعاتی و اینترنت اشیا است.

.