مدل اعتماد توزیع‌شده رویداد محور برای شبکه اینترنت اشیا

زهرا هادیان، فضل‌الله ادیب‌نیا و وحید رنجبر*

چکیده - چشم‌اندازی از اینترنت آینده به‌گونه‌ای معرفی‌شده است 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 ازنظر 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 قابل‌اعتمادی را 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 رویداد محور پیشنهاد شده است 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 روشن‌خاموش و بدگویی مقاوم‌تر است.

***کلید واژه*- اینترنت اشیا، مدیریت اعتماد، مدیریت اعتماد توزیع‌شده، ارزیابی اعتماد.**

۱- مقدمه

اینترنت اشیا[1] یک زمینه تحقیقاتی نوظهور در حوزه شبکه است و در کلیه حوزه‌هایی که می‌تواند زندگی افراد را تغییر دهند قابل‌اعمال 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 قابل‌توجهی از داده‌های حساس تولید می‌شود. تعداد تهدیدات امنیتی مربوط به زیرساخت، بستر و برنامه اینترنت اشیا طی چند سال گذشته، افزایش‌یافته 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 حافظه‌ی گره‌های اینترنت اشیا است.

در اینترنت اشیا هر شیء در اینترنت قابل‌دسترسی و ردیابی است. هدف اینترنت اشیا ایجاد یک شبکه وسیع با میلیاردها شیء است که بتوانند به طور یکپارچه داده ایجاد و مبادله کنند و تعاملات هوشمندانه‌ای بین افراد و اشیاء اطراف آنها برقرار شود. شبکه‌های اینترنت اشیا ازنظر ماهیت باز، ناشناس و پویا هستند، که به ناچار مسائل امنیتی، حریم خصوصی و اعتماد شدیدی را ایجاد می کند که مانع از کاربرد گسترده اینترنت اشیا می شود [۲].

پروتکل‌های امنیتی مبتنی بر اینترنت سنتی به دلیل 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، اما امنیت به دلیل 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[2] نقش مهمی در اینترنت اشیا برای تلفیق و استخراج داده‌های قابل‌اطمینان، خدمات واجد شرایط و افزایش حریم خصوصی کاربر و امنیت اطلاعات ایفا می‌کند. اعتماد[3] می‌تواند به‌عنوان یک ویژگی اصلی برای ایجاد ارتباط قابل‌اعتماد و یکپارچه بین نهادها و تضمین خدمات و برنامه‌های ایمن در نظر گرفته شود. برای دستیابی به ارتباطات امن و قابل‌اعتماد، راه‌حل‌های مختلف مبتنی بر اعتماد ارائه‌شده است [۳].

یک مدل اعتماد قابل اطمینان باید امنیت شبکه و یکپارچگی داده‌ها را تضمین کند و همچنین به عنوان داوری عمل کند که گره‌های قابل اعتماد را شناسایی کند و به سایر گره‌ها انتشار دهد و هرگونه فعالیت مخرب را شناسایی و مجازات کند. امتیازات اعتماد اختصاص داده شده توسط مدل اعتماد بر اساس سابقه گره‌ها است، که می‌تواند به پیش بینی رفتارهای آینده گره‌ها کمک کند [۴]. مدل‌های اعتماد جهت شناسایی اشیا مخرب و بهبود قابلیت اطمینان شبکه پیشنهاد شده‌اند. توصیه‌های

مقاله در تاریخ ..... ارسال شد. این پژوهش به عنوان پایان نامه کارشناسی ارشد مهندسی کامپیوتر در گرایش شبکه های کامپیوتری در دانشگاه یزد پذیرفته شده است .

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

[1] IoT

[2] Trust management (TM)

[3] Trust

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 ازنظر انتشار اعتماد به دودسته 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 قابل‌دسترسی است. گره مرکزی مسئول ارائه اطلاعات اعتماد ازجمله مذاکره اعتماد، محاسبه و تصمیم‌گیری و یا کمک به گره‌ها با تهیه اطلاعات اولیه موردنیاز برای محاسبه اعتماد خواهد بود. در رویکرد توزیع‌شده گره‌های اینترنت اشیا به‌طور مستقل اعتماد را محاسبه کرده و جدول اعتماد را با گره‌های همسایه بدون دخالت نهاد متمرکز تبادل می‌کنند.

در این مقاله یک روش مدیریت اعتماد توزیع‌شده سبک وزن پیشنهاد شده است 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 مقایسه‌ی مقدار اعتماد پیشنهادی با مقدار اعتمادی که خودش محاسبه کرده، جدول اعتماد خود را به‌روزرسانی می‌کند.

در این مقاله در بخش دوم به بررسی کارهای مرتبط در حیطه‌ی مدیریت اعتماد در اینترنت اشیا پرداخته‌شده است. در بخش سوم روش مدیریت اعتماد پیشنهادی ارائه‌شده است. در بخش چهارم نتایج ارزیابی نشان داده‌شده‌اند و درنهایت 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 خواهیم پرداخت و سپس چالش‌های این گونه روش‌ها بررسی شده است و روش‌های توزیع شده ارائه شده که سعی در حل چالش‌های روش‌های متمرکز دارد بیان می‌شود.

عبید و همکارانش یک مدل مدیریت اعتماد متمرکز چندلایه برای زمان‌بندی کار در محاسبات ابری موبایل (MCC[4]) 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 قابل‌اعتماد موردنیاز برای محاسبات ابری موبایل را محاسبه می‌شود. آنها اعتماد را با در نظر گرفتن ویژگی‌هایی مانند صداقت، تأخیر و شایستگی محاسبه می‌کنند. توابع قابل‌اعتماد باید در لایه ابری توزیع شوند و اهمیت کنترل تمام روش‌های اتوماسیون را ارائه دهند. سپس، یک زمان‌بندی کارآمد و پویا برای بهبود زمان‌بندی کار پس از محاسبه اعتماد با استفاده از روش‌های محاسبه اعتماد اجتماعی و محیطی اضافه می‌کنند و تنها وظایف قابل‌اعتماد از دستگاه‌ها به سمت ابر منتقل می‌شوند [۵].

کامران احمد و همکارانش یک روش محاسبه اعتماد متمرکز را برای شبکه‌های VANET[5] پیشنهاد داده‌اند. در این مطالعه یک رویکرد خوشه‌بندی StabTrust برای پرداختن به این مسائل امنیتی پیشنهادشده است. روش‌های خوشه‌بندی برای محدود کردن ارتباط وسایل نقلیه با زیرساخت‌ها ارائه‌شده است. در خوشه‌بندی، وسایل نقلیه باهم جمع می‌شوند تا خوشه‌ای را براساس قوانین خاصی تنظیم کنند. هر خوشه از تعداد محدودی از وسایل نقلیه/گره‌ها و یک سرخوشه (CH) تشکیل‌شده است. StabTrust روشی را برای تدوین خوشه‌های قابل‌اعتماد 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 درخطر 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 قابل‌اعتماد بین گره‌ها، پیشنهاد می‌کنند محیط اینترنت اشیا را به خوشه تقسیم کنند. چارچوب کلی آن‌ها شامل یک Super Node (SN) 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 Master Node (MN) است. همچنین در هر خوشه چندین گره سرخوشه Cluster Node (CN) وجود دارد که تحت نظارت MN با یکدیگر ارتباط برقرار می‌کنند. SN یک حافظه مرکزی برای ذخیره داده‌های اعتماد برای همه MNها و CN ها برای کل چارچوب اینترنت اشیا دارد و MN ها حافظه محلی دارند که در آن‌ها مقادیر اعتماد برای CN ها در هر خوشه

[4] Mobile cloud computing

[5] Vehicle ad-hoc network

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 CN ها 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 داده‌اند که اطلاعات مربوط به سرویس‌ها و دستگاه‌های معتبر اینترنت اشیا را در بین این دسته از ذی‌نفعان گردش می‌کند. لیست اعتماد بر جلوگیری از ترافیک ناخواسته از دستگاه‌های اینترنت اشیا ازجمله 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 شده‌ای) از بلاک چین را دریافت می‌کنند 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 نرم‌افزار محور و بلاک‌چین‌ها و همچنین 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 درنتیجه مشکلات مقیاس‌پذیری را افزایش می‌دهد [۸].

امایما و همکارانش یک سیستم مدیریت اعتماد مبتنی بر جوامع موردعلاقه برای اینترنت اجتماعی اشیا (TMCoI-SIOT) پیشنهاد داده‌اند که ویژگی‌های مختلفی ازجمله 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 براساس ارزیابی مستقیم و غیرمستقیم ادغام می‌کند. معماری TMCoI-SIOT از مفهوم خوشه‌بندی استفاده می‌کند و گره‌ها را براساس علاقه به جوامع تقسیم می‌کند. در این روش تشکیل جامعه با تأیید اعتبار گره آغاز می‌شود. اگر یک گره بخواهد به SIOT بپیوندد، سرور SIOT آن را تأیید می‌کند. پس از تأیید اعتبار، گره مجاز به پیوستن به جامعه موردعلاقه خود است یا می‌تواند ایجاد جامعه خود را آغاز کند. بعلاوه، هر جامعه‌ای مدیر اعتماد خاص خود را دارد. انتخاب یک مدیر اعتماد براساس مقدار اعتماد است و پارامترهای مورداستفاده برای ارزیابی اعتماد از سطح اعتماد، توانایی و اجتماعی بودن یک گره تشکیل‌شده 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 شود. مسئولیت‌های مدیر شامل محاسبه و ذخیره‌سازی مقادیر اعتماد است. وقتی یک گره جدید درخواست پیوستن به مدیر را ارسال می‌کند، اعتماد را محاسبه می‌کند 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 روشن‌خاموش[7] ارزیابی‌شده، اما در برابر حملات بددهان[8] مورد ارزیابی قرار نگرفته است [۹].

به‌طورکلی، روش‌های محاسبه و مدیریت اعتماد متمرکز از مشکلاتی مانند تنها یک نقطه شکست دارند و از پیاده‌سازی ساده‌ای برخوردار هستند و مقیاس‌پذیر نیستند و دارای گلوگاه عملکردهستند 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 (RobustTrust) ارائه‌شده است 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 گره‌ها مخرب و بدرفتار محکم شوند. مرحله ترکیب اعتماد شامل دانش، شهرت و تجربه است. علاوه بر این، سازوکار پیشنهادی مبتنی بر رویداد است؛ به‌این معنی که یک گره فقط هنگام وقوع یک رویداد بین دو گره، اعتماد را ارزیابی می‌کند و به گره‌ها کمک می‌کند تا اعتماد بیشتری را ارزیابی کنند و همچنین 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 افزایش‌یافته است و همچنین قابلیت سازگاری در مقایسه باکارهای مشابه کم‌تر است [۱۱].

روپایان و همکارانش با در نظر گرفتن اعتماد به‌خود (SLT)، اعتماد اجتماعی (ST)، اعتماد سبز (GT) و اعتماد QoS، یک معماری مدیریت اجتماعی مبتنی بر جامعه را پیشنهاد می‌کنند. آن‌ها اعتماد به‌خود 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 اشیا تازه تأسیس‌شده با رفتار شبکه مقایسه می‌شوند تا بررسی کنند آیا دستگاه‌ها به‌خوبی نصب‌شده‌اند یا خیر. آن‌ها اعتماد سبز را با پارامترهای طول عمر شبکه و زمان پاسخگویی

[6] Software-defined networking

[7] On-off attacks

[8] Bad-mouthing attacks

محاسبه می‌کنند. اعتماد اجتماعی رفتار گره‌های درون جامعه را نشان می‌دهد. آن‌ها اعتماد اجتماعی را توسط پارامترهای صمیمیت، صداقت و شباهت‌های اجتماعی محاسبه می‌کنند. آن‌ها 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].

یاراو همکارانش یک مدلی را برای مدیریت اعتماد در دستگاه‌ها و سرویس‌های اینترنت اشیا، بر اساس تکنیک رتبه‌بندی چند ویژگی ساده (SMART[9]) و الگوریتم حافظه کوتاه‌مدت بلندمدت (LSTM[10]) پیشنهاد می‌کنند. تکنیک SMART برای محاسبه ارزش اعتماد استفاده می شود که ارزش اعتماد را بر اساس اطلاعات گره که در مرحله قبل (آماده سازی داده ها) به‌دست آمده، محاسبه می کند. الگوریتم LSTM برای شناسایی تغییرات در رفتار بر اساس آستانه اعتماد استفاده می شود. روش آن‌ها با استفاده از دقت، نرخ تلفات، صحت، فراخوانی و اندازه گیری F (F-Measure) بر روی نمونه های داده های مختلف با اندازه های مختلف ارزیابی می شود 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 چند سطحی [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 به محاسبه می‌کند؛ بنابراین 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] مطرح‌شده است، مصرف انرژی و حافظه گره‌ها است.

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 می‌کنند.	در برابر حملات مورد ارزیابی قرار نگرفته است.
	۲۰۱۷ [۶]	اعتماد متمرکز را با استفاده از رویکرد خوشه‌بندی ارائه می‌دهد و به‌صورت رویداد محور 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 را ارائه داده‌اند و اشیا را براساس علایق و شباهت به جوامع مختلف تقسیم کردند. فرآیند به‌روزرسانی در سطح پایین به‌صورت رویداد محور است و در سطح بالا به‌صورت زمان محور 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.
توزیع شده	۲۰۱۹ [۱۱]	مدیریت اعتماد توزیع‌شده ارائه داده‌اند و با استفاده از پارامترهای دانش، شهرت و تجربه اعتماد را محاسبه کرده‌اند. به‌صورت رویداد محور به‌روزرسانی می‌شود.	میزان مصرف انرژی در مقایسه باکارهای مشابه افزایش‌یافته است و همچنین قابلیت سازگاری در مقایسه باکارهای مشابه کم‌تر است.
	۲۰۱۸ [۱۲]	با در نظر گرفتن اعتمادبه‌نفس (SLT)، اعتماد اجتماعی (ST)، اعتماد سبز (GT) و اعتماد QoS، یک معماری مدیریت اجتماعی مبتنی بر جامعه را پیشنهاد می‌کنند.	مقدار انرژی بالایی برای انجام محاسبات استفاده می‌کند.
	۲۰۲۲ [۱۳]	یک مدلی را برای مدیریت اعتماد، بر اساس تکنیک رتبه‌بندی چند ویژگی ساده (SMART) و الگوریتم حافظه کوتاه‌مدت بلندمدت (LSTM) پیشنهاد می‌کنند.	در برابر حملات مورد ارزیابی قرار نگرفته است.

در این مقاله، با توجه به ماهیت اینترنت اشیا، یک مدیریت اعتماد توزیع‌شده مطرح‌شده است که علاوه بر سبک و راحت بودن، ارزش اعتماد را در زمان سریع‌تر و تعداد تراکنش کم‌تر محاسبه می‌کند؛ و همچنین در

[9] Simple multi-attribute rating technique
[10] Long short-term memory

برابر حملات روشن‌خاموش و بددهان نیز مقاوم است.

۳- روش پیشنهادی

اگر در اینترنت اشیا، دستگاه‌های ناهمگون زیادی به هم متصل هستند که در هر زمان و هر مکان به شبکه سراسری اینترنت متصل می‌شوند و امکان دسترسی به اطلاعات زیادی را فراهم می‌کند. این اشیا 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 باهم ارتباط برقرار می‌کنند، بنابراین در برابر حملات مخرب آسیب‌پذیر هستند. ایده اصلی مدیریت اعتماد ایجاد اعتماد بین دو گره منفرد است. مدیریت اعتماد مکانیزمی است که امکان شناسایی گره‌های مخرب، خودخواه و در معرض خطر را نیز فراهم می‌کند. براساس مطالعه انجام شده در [۸] مدل‌های محاسبه اعتماد موجود در سیستم‌های اینترنت اشیا براساس 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[11]) و اعتماد اجتماعی است. انتشار اعتماد به چگونگی انتشار شواهد اعتماد به همسایگان اشاره دارد. به‌طورکلی، دو طرح انتشار اعتماد وجود دارد، یعنی 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 به‌طورکلی، دو رویکرد وجود دارد: رویکرد رویداد محور و رویکرد زمان محور. شکل‌گیری اعتماد به چگونگی شکل‌گیری اعتماد کلی از چندین ویژگی اعتماد اشاره دارد. شکل‌گیری اعتماد از جنبه اعتماد منفرد یا اعتماد چندگانه در نظر گرفته‌شده 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 می‌شود و به‌عنوان مقدار اعتماد جدید در جدول اعتماد ذخیره می‌شود. بعد از انجام هر معامله اگر معامله موفقیت‌آمیز باشد مقدار پاداش از فرمول زیر به دست می‌آید:

$$Success = Success + 1 \quad (۱)$$

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

$$N_j = R_s * W_{sj} \quad (۳)$$

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

اگر معامله ناموفق باشد مقدار اعتماد از فرمول‌های (۴) الی (۷) به‌دست می‌آید:

$$Failure = Failure + 1 \quad (۴)$$

$$onoff = onoff + 1 \quad (۵)$$

(۶)

$$P_s = -\log(2*(\frac{Failure}{Total} + onoff) * Failed\,\mathrm{Re}\,peated) * \beta^{\Delta t}$$

$$N_j = P_s * W_{sj} \quad (۷)$$

که در اینجا Failure تعداد تعاملات ناموفقی است که با این گره داشته و Total تعداد کل معاملاتی که با این گره داشته. onoff پارامتری است که برای تشخیص حملات روشن‌خاموش در نظر گرفته‌شده است. هر وقت معامله‌ای ناموفق باشد 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 گرفته‌شده است که اگر معامله‌ای ناموفق باشد 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 که برای این سرویس محاسبه‌شده است. بعد از محاسبه پاداش و مجازات مقدار اعتماد از مجموع آن‌ها محاسبه می‌شود.

مقدار اعتماد هر گره باگذشت زمان تغییر می‌کند. اگر دو گره در مدت‌زمان طولانی باهم تراکنش نداشته باشند مقدار اعتماد محاسبه‌شده در مراحل قبل اهمیت خود را از دست می‌دهد، دلیل این امر این است که گره مطمئن نیست آیا گره سرویس‌دهنده هنوز قابل‌اطمینان است یا خیر، درنتیجه باعث می‌شود گره سرویس‌گیرنده را در محاسبه اعتماد دچار اشتباه کند. در روش پیشنهادی به‌منظور اینکه فاصله زمانی بین تراکنش‌ها نیز در 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 تا ۱ است و Δt اختلاف‌زمانی تراکنش‌های انجام‌شده بین دو گره است و هر چه اختلاف‌زمانی بیشتر باشد مقدار اعتماد کم‌تر تغییر می‌کند. مقدار β هرچقدر کم‌تر باشد تأثیر گذشت زمان را بیشتر خواهد کرد و میزان اهمیت پاداش یا مجازات کم‌تر خواهد شد.

[11] Quality of service

۳-۲- به‌روزرسانی اعتماد

ارزیابی اعتماد غیرمستقیم در محاسبه اعتماد، جنبه قابل‌توجهی دارد زیرا وقتی یک گره اطلاعات لازم را برای محاسبه اعتماد به یک گره خاص را 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 بالا بردن کارایی سیستم اعتماد به‌صورت رویداد محور 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 گره‌ای که با آن تراکنش داشته و مقدار آن را محاسبه کرده است را ارسال می‌کند. گره برای اینکه تشخیص بدهد توصیه‌ای که گره همسایه ارسال کرده یک توصیه خوب است یا نه از روش زیر استفاده می‌کند:

$$\theta = |\,\mathrm{Re}commenderTrrust - OldTrust\,| \qquad (۸)$$

در فرمول (۸) RecommenderTrust مقدار اعتماد توصیه‌شده گره همسایه است و OldTrust مقدار اعتماد محاسبه‌شده از معامله قبلی 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:

$$NewTrust = \alpha * OldTrust + (1-\alpha) * \mathrm{Re}commenderTrust \qquad (۹)$$

با استفاده از فرمول (۹) ضریب اعتماد توصیه‌شده را مدیریت می‌کنیم به این صورت که در این فرمول تأثیر اعتماد توصیه‌شده کم‌تر در نظر گرفته‌شده است 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 بعدازاینکه تعداد محدودی پیشنهاد خوب را در مورد یک گره قبول کرد، دیگر تا وقتی‌که دوباره خودش با گره موردنظر تراکنش نداشته باشد پیشنهادی قبول نمی‌کند.

یک سیستم اینترنت اشیا با پیوستن گره‌های جدید و خارج شدن گره‌های موجود تکامل می‌یابد. یک پروتکل مدیریت اعتماد باید به این موضوع بپردازد تا به گره‌های جدید که به شبکه می‌پیوندند اجازه دهد تا به‌سرعت و با درجه‌ای از دقت معقول اعتماد را به دست آورد [۱۵]. در روش پیشنهادی وقتی گره جدیدی وارد شبکه می‌شود تا قبل از اینکه با گره‌ای تبادل داشته باشد تعداد محدودی پیشنهاد را پذیرفته و مقدار اعتماد خود را آپدیت می‌کند؛ بنابراین گره‌ای که جدید وارد شبکه می‌شود سریع‌تر مقدار اعتماد را محاسبه می‌کند. وقتی گره جدید که 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 اینکه خودش با گره موردنظر تراکنش داشته باشد، فقط تعداد محدودی پیشنهاد را قبول می‌کنند و حتی اگر پیشنهاد مخربی به گره تازه‌وارد شود بعد از اینکه گره تازه‌وارد با گره موردنظر تراکنش داشته باشد، مقدار اعتماد به‌درستی محاسبه می‌شود و موردحمله قرار نمی‌گیرد. اگر پیشنهادهای مخربی به گره تازه‌وارد فرستاده شود مقدار اعتماد را دیرتر محاسبه می‌کند ولی ازآنجایی‌که 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 که با آن‌ها تعامل داشته را 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.

۳-۴- 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، بنابراین در روش پیشنهادی اعتماد هر گره را با توجه به تراکنشی که الآن با آن گره داشته و سابقه‌ی گره و توصیه‌های همسایگان محاسبه می‌کنیم. در این روش هر گره با توجه به زمان پاسخگویی گره مقابل و سابقه‌ی آن، مقدار اعتماد آن گره را محاسبه می‌کند. همچنین هر گره می‌تواند چندین سرویس را ارائه دهد و برای هرکدام از سرویس‌ها با توجه به انرژی، حافظه و پردازش وزن‌های متفاوتی (W_{sj}) در نظر گرفته‌شده است. وزن هر سرویس را با توجه رابطه زیر محاسبه می‌کنیم:

$$W_{sj} = S_j * \sigma \qquad (۱۰)$$

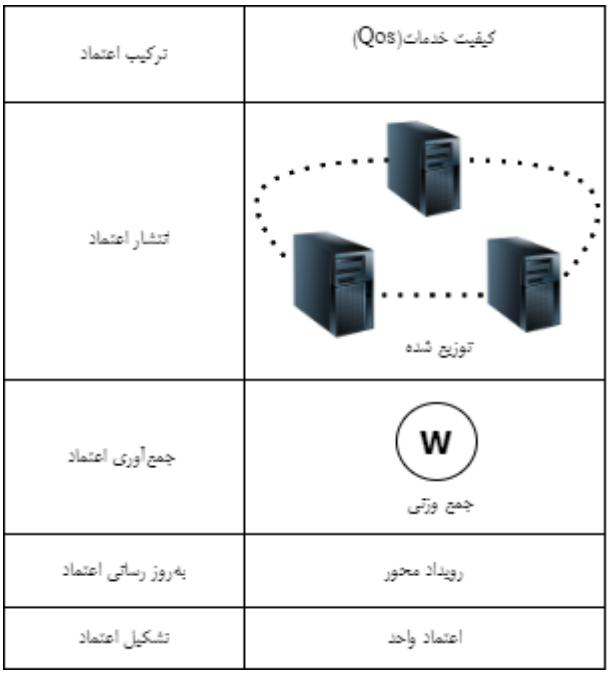
در رابطه (۱۰) σ مقداری بین صفر و یک دارد و برای بهنجار کردن W استفاده می‌شود، S_j مقداری است که با توجه به انرژی، حافظه و پردازش به هر سرویس اختصاص می‌دهیم و سرویس‌هایی که حساسیت بیشتری دارند و یا به ظرفیت پردازش بیشتری نیاز دارند دارای S_j بالاتری هستند و سرویس‌هایی که به منابع زیادی احتیاج ندارند دارای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

۳-۵- شکل‌گیری اعتماد

در روش پیشنهادی شکل‌گیری اعتماد به‌صورت اعتماد منفرد بکار گرفته‌شده است و فقط یک ویژگی اعتماد در پروتکل اعتماد در نظر گرفته‌شده است. در این روش ما از زمان پاسخگویی که یکی از معیارهای

کیفیت سرویس است و مهم‌ترین معیار در سیستم‌های اینترنت اشیا سرویس‌گرا محسوب می‌شود استفاده کرده‌ایم.

همان‌طور که در شکل ۱ نشان داده‌شده 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 رویداد محور و برای تشکیل اعتماد از اعتماد واحد استفاده‌شده است.



شکل ۱ : روش پیشنهادی

به‌طورکلی در روش پیشنهادی، با توجه به تراکنش‌های گذشته و تراکنش فعلی بین دو گره، مقدار اعتماد محاسبه‌شده و در جدول اعتماد گره ذخیره می‌شود، سپس گره موردنظر مقدار اعتماد محاسبه‌شده را در اختیار همسایگان خود قرار داده. گره همسایه، با توجه به مقدار اعتمادی که خودش قبلاً محاسبه کرده است 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 می‌کنند و اعتماد را محاسبه می‌کند. در روش DDTMS هنگامی که یک گره به عنوان گره مخرب شناسایی می شود، گره تعاملات آینده خود را با آن متوقف می کند و به سایر گره های همسایه نیز اطلاع می دهد. DDTMS تنها حمله روشن-خاموش یک گره مخرب را شناسایی می‌کند. شبکه شبیه‌سازی‌شده‌ی هرکدام از روش‌ها شامل ۵۰ گره Tmote Sky است که از این ۵۰ گره ۱۰ گره به‌عنوان گره مخرب شبیه‌سازی شده‌اند و گره‌ها به‌طور تصادفی توزیع‌شده است. مقدار Wsj برای گره‌ها در هر دو شبیه‌سازی (روش پیشنهادی و روش DDTMS) ۰.۱ در نظر گرفته‌شده است. همچنین شبیه‌سازی هر دو روش در ۵ مرحله و شرایط یکسان انجام‌شده است و نمودار میانگین نتایج رسم شده است. در **Error! Reference source not found.** مقدار متغیرها بیان‌شده است.

جدول ۲: مقدار متغیرها

متغیرها	مقدار متغیرها
مقدار اختلاف اعتماد محاسبه‌شده و اعتماد پیشنهادی (Qr)	۰.۲
وزن سرویس (Wsj)	۰.۱
تعداد پیشنهادها (x)	۳
ضریب جمع وزنی (α)	$\frac{1}{3}$

۴-۱- محیط شبیه‌سازی

شبیه‌سازی در محیط COOJA موجود در سیستم‌عامل Contiki انجام‌شده است. شبیه‌سازکوجا یک محیطی برای شبیه‌سازی اینترنت اشیا است 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 اشیا بی‌سیم باانرژی محدود و شبیه‌سازی اپلیکیشن‌های اینترنت اشیا است. از مزایای قابل‌توجه کوجا می‌توان به محیط گرافیکی و کاربردی آن اشاره کرد که شبیه‌سازی را بسیار آسان‌تر می‌کند. نصب و اجرای کوجا نیز پیچیدگی زیادی ندارد. همچنین بسیاری از پروتکل‌ها و استانداردهای رایج و مرسوم اینترنت اشیا و شبکه‌های بی‌سیم به‌صورت پیش‌فرض تعبیه‌شده‌اند. کوجا، شبیه‌سازی سطح متقابل را امکان‌پذیر می‌کند، شبیه‌سازی سطح پایین سخت‌افزار و شبیه‌سازی سطح بالا را در یک شبیه‌سازی واحد ترکیب می‌کند. ازاین‌جهت انعطاف‌پذیر و توسعه‌پذیر است که تمام سطوح سیستم را می‌توان تغییر داد یا جایگزین کرد. شبیه‌ساز کوجا در جاوا پیاده‌سازی شده است و این باعث می‌شود که شبیه‌ساز 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 نمودیم که دما را اندازه‌گیری و اطلاعات را با یکدیگر تبادل می‌کنند. ابعاد محیط شبیه‌ساز را ۶۰۰ متر در ۶۰۰ متر در نظر گرفتیم بنابراین ۵۰ گره در این محیط قرار داده‌ایم که از نوع Sky mote هستند زیرا این نوع، گره‌های حسگر بی‌سیم را شبیه‌سازی می‌کند.گره‌های Sky mote تا فاصله ۵۰ متری قابلیت ارتباط با گره‌های دیگر را دارند. از استاندارد IEEE 802.15.4 برای لایه فیزیکی استفاده شده که برای انتقال داده‌های حسگر بی‌سیم استفاده می‌شود. از پروتکل IPv6 در لایه MAC استفاده شده تا هر گره آدرس دستگاه‌های دیگر را بشناسد همچنین از پروتکل RPL برای لایه شبکه

استفاده می‌شود تا مسیریابی کم مصرف با امکان از دست دادن بسته‌ها فراهم شود و از پروتکل UDP برای انتقال داده‌ها در لایه انتقال استفاده می‌شود. مدت‌زمان 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 کرده و اطلاعات آن را به گره‌های دیگر ارسال می‌کند.

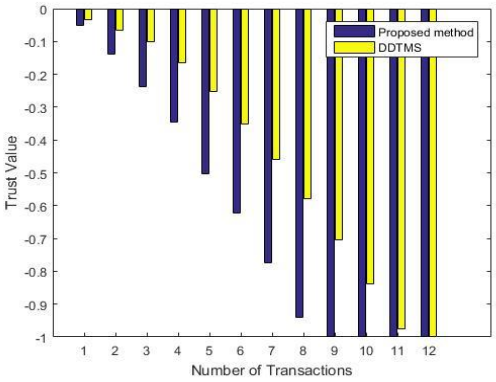
جدول ۳: پارامترهای شبیه‌سازی

پارامترها	مقدار پارامترها
شبیه‌ساز	Cooja under Contiki 3.0 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 802.15.4
لایهMAC	IPv6
لایه شبکه	RPL
لایه انتقال	UDP
مدت‌زمان شبیه‌سازی	یک ساعت
نرخ ارسال بسته	۱ بسته در هر ۲۰ تا ۶۰ ثانیه

۴-۲- نتایج ارزیابی

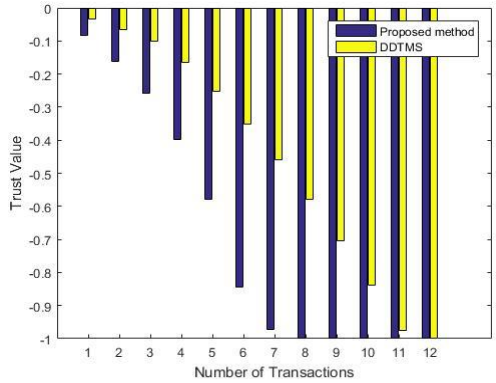
۴-۲-۱- محاسبه اعتماد گره مخرب

در روش‌های مدیریت اعتماد تشخیص گره مخرب از اهمیت زیادی برخوردار است. برای ارزیابی اعتماد گره‌های مخرب، ۵۰ گره به‌طور تصادفی در شبکه توزیع‌شده‌اند که از این ۵۰ گره ۱۰ گره به‌عنوان گره مخرب هستند. منظور از گره مخرب گره‌ای است که بیشتر مواقع درخواست‌ها را پاسخ نمی‌دهد. مقدار اعتماد محاسبه‌شده‌ی گره مخرب که توسط یکی از گره‌ها محاسبه شده است، در شکل ۲ رسم شده است و مقدار اعتماد گره مخرب در دو روش با هم مقایسه شده است. همان‌طور که دیده می‌شود 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 هنگامی‌که 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 کرده، بنابراین شناسایی گره‌های مخرب در زمان کم‌تر و تعداد تراکنش کم‌تر انجام می‌شود؛ اما در روش DDTMS پیشنهادات همسایگان و مشاهدات غیرمستقیم وجود ندارد و مقدار اعتماد فقط بعد از هر بار تراکنش به‌روزرسانی می‌شود.



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

ما برای محاسبه اعتماد گره مخرب حالتی را در نظر گرفتیم که گره موردنظر تمام پیشنهادهای همسایگان را قبول کند و محدودیتی در تعداد پیشنهادها نگذاشتیم. همان‌طور 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 محاسبه‌شده است، اما ریسک حملات هوشمندانه را دارد. در این حالت هر چه تعداد همسایگان گره بیشتر باشد، مقدار اعتماد سریع‌تر محاسبه می‌شود زیرا تعداد پیشنهادها بیشتر می‌شود و مقدار اعتماد سریع‌تر همگرا می‌شود.

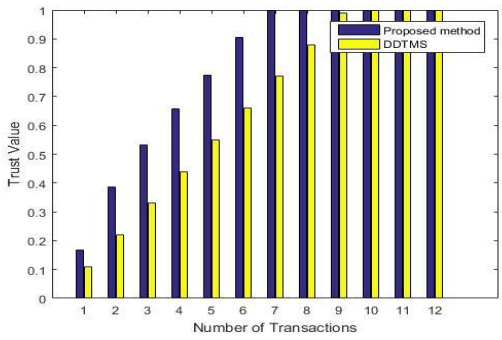


شکل ۳: مقایسه اعتماد محاسبه‌شده گره مخرب در طول زمان در هر دو روش بدون محدودیت تعداد پیشنهادها

۴-۲-۲- محاسبه اعتماد گره درستکار

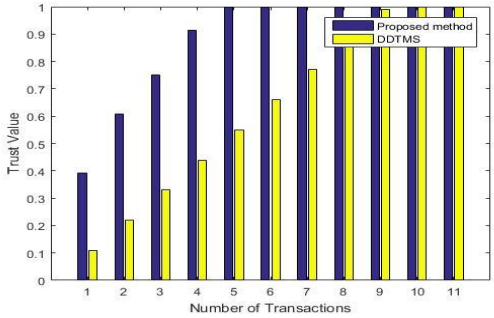
با توجه به این‌که در یک مدل مدیریت اعتماد علاوه بر تشخیص گره‌های مخرب شناسایی گره‌های درستکار در زمان مناسب نیز اهمیت دارد، در شکل ۴ اعتماد محاسبه‌شده گره‌های درستکار در دو روش باهم مقایسه شده است. در این سناریو تمام ۵۰ گره، گره‌های درستکار هستند. منظور از

گره درستکار، گره‌ای است که درخواست‌های سرویس‌گیرنده را جواب می‌دهند. در شبیه‌سازی گره‌های درستکار نیز مقدار Wsj برای گره‌های درستکار در هر دو روش ۰.۱ در نظر گرفته‌شده است. مقدار اعتماد محاسبه‌شده یکی از گره‌ها در هر دو روش رسم شده است. همان‌طور که می‌بینیم روش پیشنهادی در گره‌های درستکار هم در زمان خیلی کم‌تر و همچنین تعداد تراکنش‌های کم‌تر مقدار اعتماد را محاسبه کرده است.



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

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

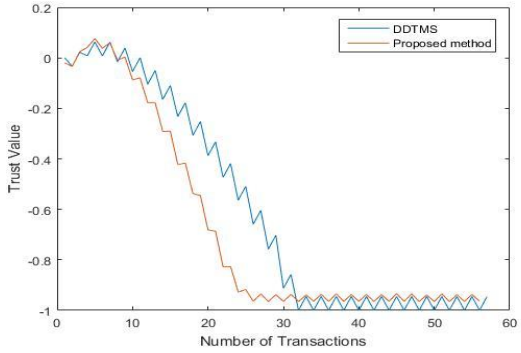


شکل ۵: مقایسه اعتماد محاسبه‌شده گره درستکار در طول زمان در هر دو روش بدون محدودیت تعداد پیشنهادها

۴-۲-۳- تشخیص حمله روشن‌خاموش

در روش پیشنهادی برای تشخیص حمله روشن‌خاموش از پارامتر onoff استفاده‌شده است و اگر تراکنشی ناموفق باشد و تراکنش قبلی آن موفق بوده است مقدار آن را افزایش می‌دهیم. برای ارزیابی تشخیص حمله روشن‌خاموش ما سه سناریو را شبیه‌سازی انجام داده‌ایم. در سناریو اول گره‌ای را شبیه‌سازی کردیم که از هر ۲ درخواست یکی را پاسخ می‌دهد و سپس مقدار اعتماد آن گره را محاسبه کرده و دو روش را باهم مقایسه انجام داده‌ایم. همان‌طور که در شکل ۶ می‌بینید هر دو روش گره مخرب را به‌درستی تشخیص داده، اما در روش پیشنهادی چون مقدار اعتماد محاسبه‌شده را با همسایگان به اشتراک می‌گذاریم گره‌ها حمله روشن‌خاموش را در زمان زودتر و تعداد تراکنش کم‌تر تشخیص داده است.

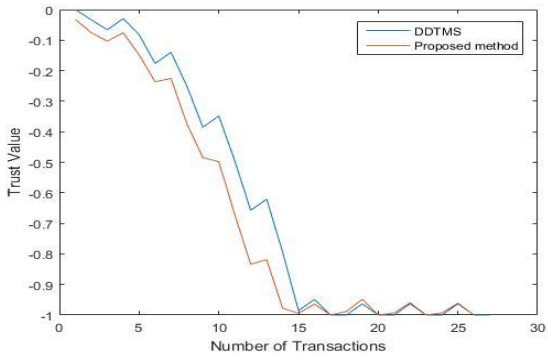
همچنین مقدار اعتماد محاسبه‌شده در روش پیشنهادی حتی کم‌تر از مقدار اعتماد روش DDTMS است.



.

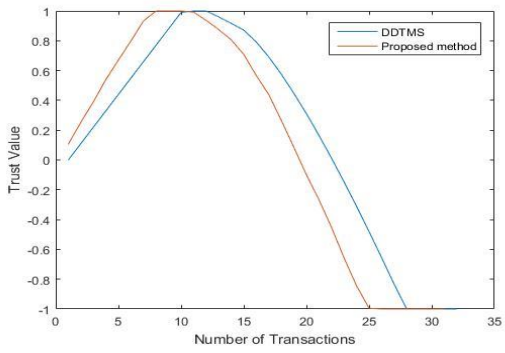
شکل ۶: تشخیص موفق حمله روشن‌خاموش در هر دو روش در سناریو از هر ۲ درخواست یکی پاسخ داده شود

در سناریو بعدی ما گره‌ای را شبیه‌سازی کرده‌ایم که از هر ۳ درخواست یکی را پاسخ می‌دهد و سپس مقدار اعتماد این گره را محاسبه کرده و نمودار دو روش را رسم کرده‌ایم. همان‌طور که در شکل ۷ می‌بینید هر دو روش حمله را به‌درستی تشخیص داده‌اند و مقدار اعتماد را ۱- محاسبه کرده‌اند.



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

در سناریو آخر برای تشخیص حمله روشن‌خاموش ما گره‌ای 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 هر دو روش رسم شده است. در این سناریو هم همان‌طور که در شکل ۸ مشاهده می‌شود، هر دو روش حمله را به‌درستی تشخیص داده و مقدار اعتماد گره را ۱- محاسبه کرده‌اند.

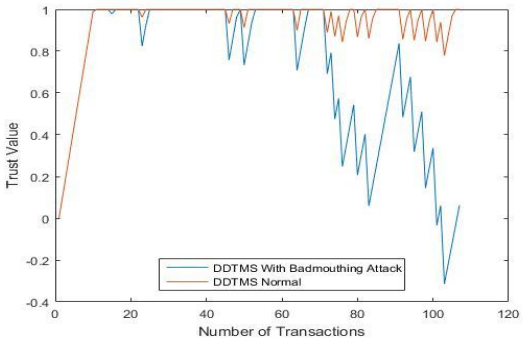


شکل ۸: تشخیص موفق حمله روشن‌خاموش در هر دو روش در سناریو بعد از مدتی پاسخ ندهد

۴-۲-۴- تشخیص حمله بددهان

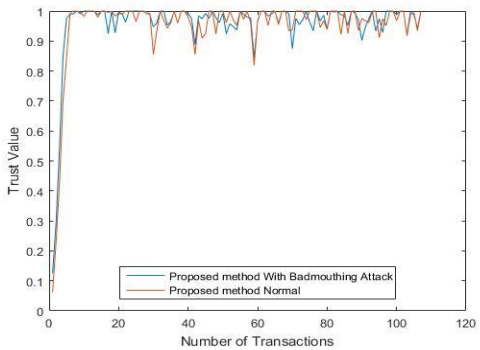
در مطالعه انجام‌شده علاوه بر حمله روشن‌خاموش حمله بددهان را نیز مورد ارزیابی قرارگرفته است. در روش پیشنهادی گره‌ها وقتی مقدار اعتمادی را به آن‌ها پیشنهاد می‌دهند با مقدار اعتماد خود مقایسه می‌کنند و اگر اختلاف مقدارها زیاد نبود اعتماد خود را به روش جمع وزنی آپدیت کرده به همین دلیل موردحمله بددهان واقع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

همان‌طور که در شکل ۹ می‌بینید در روش DDTMS به‌راحتی موردحمله بددهان قرارگرفته است و مقدار اعتماد یک گره خوب که باید مقدار اعتماد محاسبه‌شده بالای ۰.۸ باشد را حتی در بعضی مواقع تا ۰.۳- نیز محاسبه کرده است.



شکل ۹: تشخیص ناموفق حمله بددهان در روش DDTMS

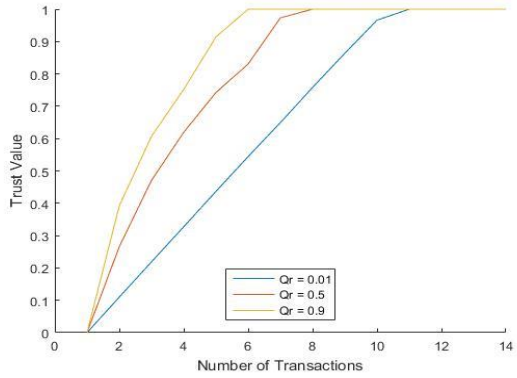
اما در روش پیشنهادی چون مقدار اعتماد پیشنهادشده را با مقدار اعتمادی که خودش محاسبه کرده، مقایسه می‌کند، موردحمله بددهان قرار نگرفته است و همان‌طور که در مشاهده می‌کنید مقدار اعتماد محاسبه‌شده، باوجود گره بددهان و بدون گره بددهان، تقریباً نزدیک به هم محاسبه‌شده است.



شکل ۱۰: تشخیص موفق حمله بددهان در روش پیشنهادی

۴-۲-۵- اهمیت انتخاب Qr

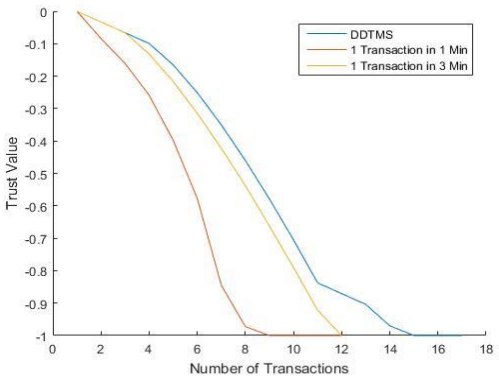
در روش پیشنهادی برای جلوگیری از حملات بددهان ما مقدار اعتماد پیشنهادی را با مقدار اعتمادی که خود گره محاسبه کرده است مقایسه می‌کنیم و اگر اختلاف این دو مقدار کم‌تر از Qr بود، مقدار اعتماد را به‌روزرسانی می‌کنیم. در این قسمت برای نشان دادن اهمیت انتخاب Qr نمودار مقدار اعتماد محاسبه‌شده گره درستکار را با Qr های متفاوت رسم کردیم. در **شکل ۱۱** نمودار محاسبه اعتماد گره درستکار را با Qr =0.01 و Qr =0.5 و Qr =0.9رسم کرده‌ایم همان‌طور که مشاهده می‌کنید هر چه مقدار Qr کوچک‌تر باشد، گره مقدار اعتماد را به‌روزرسانی نمی‌کند، بنابراین مقدار اعتماد در زمان دیرتر و تعداد تراکنش بیشتر به حالت پایدار می‌رسد و هر چه مقدار Qr بزرگ‌تر باشد، گره با پیشنهادهای بیشتری مقدار اعتماد را به‌روزرسانی می‌کند 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، بنابراین در انتخاب Qr باید دقت داشت و آن را مناسب انتخاب کرد. ما در این روش برای جلوگیری از حملات بددهان مقدار Qr = 0.2 قرار داده‌ایم.



شکل ۱۱: نمودار مقایسه مقدار Qr در روش پیشنهادی

۴-۲-۶- اهمیت زمان در محاسبه اعتماد

هنگامی‌که دو گره در مدت‌زمان طولانی باهم تراکنش نداشته‌اند مقدار اعتمادی که گره قبلاً محاسبه کرده است باید ارزش کم‌تری داشته باشد، زیرا ممکن است در این فاصله زمانی گره رفتار متفاوتی داشته باشد. برای نشان دادن اهمیت زمان در محاسبه اعتماد، گره‌های مخربی را شبیه‌سازی کردیم که در فاصله‌ی زمانی ۳ تا ۴ دقیقه باهم تراکنش داشته باشند و بعد مقدار اعتماد را باحالتی که ۲۰ تا ۶۰ ثانیه‌ای یک‌بار تراکنش داشته باشند مقایسه انجام‌شده است. همان‌طور که در شکل ۱۲ مشاهده می‌کنید هر چه 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 می‌شود، نیز مقایسه کرده‌ایم. مشاهده می‌کنید که در حالتی که فاصله تراکنش‌ها سه برابر شده است، همچنان از روش DDTMS، سریع‌تر اعتماد را محاسبه می‌کند.



شکل ۱۲: مقایسه اعتماد گره مخرب در تراکنش‌هایی بافاصله زمانی مختلف

نتایج ارزیابی نشان می‌دهد که روش پیشنهادی در زمان سریع‌تر و تعداد تراکنش کم‌تر مقدار اعتماد را محاسبه کرده و در برابر حملات روشن‌خاموش و بددهان مقاوم است.

۵- نتیجه گیری

اینترنت اشیا (IoT) 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 قابل‌اعتماد، خدمات واجد شرایط و افزایش حریم خصوصی کاربر و امنیت اطلاعات ایفا می‌کند.

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

در روش پیشنهادی هر چه 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 می‌گیرد 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 قابل‌استفاده و پیاده‌سازی است؛ و با توجه به اینکه، در این روش هر گره فقط با همسایگان خود در ارتباط است، و همچنین محاسبات به‌صورت توزیع شده 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 می‌کند 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 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Nov. 2018, pp. 131–134. doi: 10.1109/GCWCN.2018.8668640.

[2] Liu, Yijia, Jie Wang, Zheng Yan, Zhiguo Wan, and Riku Jäntti. "A survey on blockchain-based trust management for Internet of Things." IEEE Internet of Things Journal 10, no. 7 (2023): 5898-5922.

[3] Ud 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, doi: 10.1109/ACCESS.2018.2880838.

[4] S. Dhelim, N. Aung, T. Kechadi, H. Ning, L. Chen and A. Lakas, "Trust2Vec: Large-Scale IoT Trust Management System based on Signed Network Embeddings," in IEEE Internet of Things Journal, 2022, doi: 10.1109/JIOT.2022.3201772.

[5] A. Ali *et al.*, “Multilevel Central Trust Management Approach for Task Scheduling on IoT-Based Mobile Cloud Computing,” *Sensors*, vol. 22, no. 1, Art. no. 1, Jan. 2022, doi: 10.3390/s22010108.

[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, doi: 10.1109/ACCESS.2020.2968948.

[7] M. D. Alshehri and F. K. Hussain, “A Centralized Trust Management Mechanism for the Internet of Things (CTM-IoT),” in Advances on Broad-Band Wireless Computing, Communication and Applications, Cham, 2018, pp. 533–543. doi: 10.1007/978-3-319-69811-3_48.

[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 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Jun. 2017, pp. 747–752. doi: 10.1109/IWCMC.2017.7986378.

[10] Arshad, Qurat-ul-Ain, Wazir Zada Khan, Faisal Azam, Muhammad Khurram Khan, Heejung Yu, and Yousaf Bin Zikria. "Blockchain-based decentralized trust management in IoT: systems, requirements and challenges." Complex & Intelligent Systems (2023): 1-22.

[11] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani, A. Altameem, and S. U. Jadoon, “RobustTrust – A Pro-Privacy Robust Distributed Trust Management Mechanism for Internet of Things,” IEEE Access, vol. 7, pp. 62095–62106, 2019, doi: 10.1109/ACCESS.2019.2916340.

[12] R. Das, M. Singh, and K. Majumder, “SGSQoT: A Community-Based Trust Management Scheme in Internet of Things,” in Proceedings of International Ethical Hacking Conference 2018, Singapore, 2019, pp. 209–222, doi: 10.1007/978-981-13-1544-2_18.

[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, Art. no. 2, Jan. 2022, doi: 10.3390/s22020634.

[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 Journal, vol. 6, no. 3, pp. 5432–5445, Jun. 2019, doi: 10.1109/JIoT.2019.2902022.

[15] P. Massa, and P. Avesani, “Trust-aware Recommender Systems,” ACM Recommender Systems Conference, Minneapolis, Minnesota, USA, Oct.2007.
[16] S. W. A. Hamdani, A. W. Khan, N. Iltaf, J. I. Bangash, Y. A. Bangash, and A. Khan, “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 Proceedings. 2006 31st IEEE Conference on Local Computer Networks, Nov. 2006, pp. 641–648. doi: 10.1109/LCN.2006.322172.