Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 12, Number 4, Winter 2024, pp. 1-11
Received: 07/08/2023, Revised: 12/07/2023, Accepted: 02/16/2024

A Blockchain-Based Trust Management Mechanism for IoT

Zahra Jafari[1], Vahid Ranjbar [2*] and Seyed akbar Mostafavi [3]
1- Department of Computer Engineering, Yazd University, Yazd , Iran.
2*- Department of Computer Engineering, Yazd University, Yazd, Iran.
3- Department of Computer Engineering, Yazd University, Yazd , Iran.
[1]Zahrajafari@stu.yazd.ac.ir, [2*] vranjbar@yazd.ac.ir, and [3]a.mostafavi@yazd.ac.ir

Corresponding author's address: Vahid Ranjbar, Department of Computer Engineering, Yazd University, Yazd, Iran.

Abstract- The increasing use of connected objects in Internet of Things systems leads to the production of a large amount of data, which creates many challenges and security issues and prevents the widespread use of Internet of Things. Trust management is a well-known solution to improve security in the Internet of Things, in which malicious attacks are detected by evaluating user behavior and calculating the level of trust in them. Traditional methods of distributed trust management do not meet the scalability requirements and resource limitations of IoT devices. Blockchain is used to solve the challenges of trust management in the Internet of Things due to its lack of centralization and immutability. In this article, a blockchain-based trust management method is presented, in which each object evaluates the level of trust of the service providers it has interacted with using the service quality criterion and publishes it in the blockchain. In this method, the nodes are leveled based on the level of trust and after analyzing the behavior, they are punished and rewarded. The evaluation of the proposed method show that the proposed method has a good performance in detecting malicious nodes and dealing with bad-mouthing, self-promotion**,** On-Off and voting attacks.

Keywords- Blockchain, Distributed Trust Management, Internet of Things (IoT), Reward and Punishment Mechanism

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۲، شماره ۴، زمستان ۱۴۰۲ ، صفحه ۱-۱۱
دریافت: ۱۴۰۲/۰۴/۱۷، بازنگری: ۱۴۰۲/۰۹/۲۶، پذیرش: ۱۴۰۲/۱۱/۲۷

ارائه یک سازوکار مدیریت اعتماد مبتنی بر بلاک‌چین برای اینترنت اشیاء

زهرا جعفری[۱]، وحید رنجبر*[۲]، سید اکبر مصطفوی[۳]
۱- دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.
*۲- دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.
۳- دانشکده مهندسی کامپیوتر، دانشگاه یزد، یزد، ایران.
[1] Zahrajafari@stu.yazd.ac.ir, [2*] vranjbar @yazd.ac.ir, [3] a.mostafavi@yazd.ac.ir

* نشانی نویسنده مسئول: وحید رنجبر، یزد، دانشگاه یزد، دانشکده مهندسی کامپیوتر.

چکیده- استفاده روزافزون از اشیاء متصل در سیستم‌های اینترنت اشیاء منجر به تولید حجم زیادی از داده‌ها می‌شود که این امر، چالش‌ها و مسائل امنیتی متعددی را ایجاد کرده و مانع از کاربرد گسترده اینترنت اشیاء می‌شود. مدیریت اعتماد یک راهکار شناخته شده برای بهبود امنیت در اینترنت اشیاء است که در آن با ارزیابی رفتار کاربران و محاسبه میزان اعتماد به آنها، حملات مخرب شناسایی می‌شوند. روش‌های سنتی مدیریت اعتماد متمرکز، الزامات مقیاس‌پذیری و محدودیت منابع دستگاه‌های اینترنت اشیاء را برآورده نمی‌کنند. بلاک‌چین به دلیل ویژگی عدم تمرکز و تغییرناپذیری برای رفع چالش‌های مدیریت اعتماد در اینترنت اشیاء استفاده می‌شود. در این مقاله یک روش مدیریت اعتماد مبتنی بر بلاک‌چین ارائه می‌شود که در آن هر شیء، میزان اعتماد ارائه‌دهندگان خدمات که با آن‌ها در تعامل بوده است را با استفاده از معیار کیفیت خدمات ارزیابی کرده و در بلاک‌چین منتشر می‌کند. در این روش، گره‌ها بر اساس میزان اعتماد سطح‌بندی شده و پس از تحلیل رفتار، شامل مجازات و پاداش می‌شوند. نتایج ارزیابی روش پیشنهادی نشان می‌دهد که روش پیشنهادی عملکرد مناسبی در تشخیص گره‌های مخرب و مقابله با حملات بدگویی، خودتبلیغی، خاموش-روشن و رأی‌گیری دارد.

واژه‌های کلیدی: اینترنت اشیاء، بلاک‌چین، مدیریت اعتماد توزیع شده، مکانیسم پاداش و مجازات.

۱- مقدمه

اطمینان از اعتماد بین دستگاه‌های اینترنت اشیاء (IoT[1]) برای اطمینان از کیفیت و عملکرد سیستم بسیار مهم است. مفهوم اعتماد و امنیت زمانی اهمیت بیشتری پیدا می‌کند که دستگاه‌های هوشمند مجبور به انتقال اطلاعات مهم برای برخی موقعیت‌های بحرانی هستند که در آن تصمیم باید به موقع و دقیق گرفته شود. مدیریت اعتماد به عنوان یک جنبه مهم از امنیت، نقش حیاتی در تضمین تبادل اطلاعات به شیوه‌ای امن و حفظ قابلیت اطمینان یک سیستم با اندازه گیری میزان اعتماد در دستگاه‌های اینترنت اشیا، کاهش عدم قطعیت‌ها و خطرات موجود در آن ایفا می‌کند. روش‌های مدیریت اعتماد در سال‌های اخیر به طور گسترده برای شناسایی رفتار غیرقابل اعتماد در اینترنت اشیاء استفاده شده است. با این حال، این روش‌ها هنوز محدودیت‌های زیادی دارند. سیستم‌های مدیریت اعتماد متمرکز برای اینترنت اشیاء دارای خطر بالقوه شکست و حملات هستند و سیستم‌های مدیریت اعتماد غیرمتمرکز کاملاً غیرمتمرکز نیستند و برای برای تکمیل محاسبات نهایی و نگهداری داده‌های اعتماد به سرورهای مرکزی نیاز دارند [۱]. در سال‌های اخیر، فناوری بلاک‌چین برای دستیابی به مدیریت اعتماد غیرمتمرکز در اینترنت اشیاء مورد مطالعه قرار گرفته است. بلاک‌چین یک دفتر کل توزیع شده است که قادر به حفظ یک

گزارش غیرقابل تغییر از تراکنش‌های انجام شده در یک شبکه است. بلاک‌چین از چندین بلوک تشکیل شده است که این بلوک‌ها به یکدیگر مرتبط هستند و کل اطلاعات بین آن‌ها توزیع می‌شود. در بلاک‌چین هر گره یک دفتر کل محلی دارد که تراکنش‌ها را برای ثبت در بلاک جدید به آن اضافه می‌کند، این گره‌ها از طریق یک شبکه همتا به همتا توزیع شده و مقیاس پذیر با یکدیگر ارتباط برقرار می‌کنند و پس از مدتی، یک دفتر منتخب از این رکوردها که شامل مجموعه ای از معاملات است، تأیید و به دفتر کل پیوست می‌شود [۲]. بلاک‌چین مجموعه‌ای از رکوردهای داده‌های تغییرناپذیر است که دارای ویژگی‌های غیرمتمرکز، سازگاری، ضد دستکاری است. با توجه به این ویژگی‌ها، بلاک‌چین به عنوان ابزاری امکان پذیر برای پیشبرد مدیریت اعتماد در نظر گرفته می‌شود و در نتیجه اعتماد و امنیت را در بین دستگاه‌های اینترنت اشیاء به طور موثر بهبود می‌بخشد. به طور خاص، تمرکززدایی تعاملات مستقیم همتا به همتا را امکان پذیر می‌کند و نقطه شکست را حذف می‌کند. سازگاری به این معنا است که اطلاعات نگهداری شده توسط هر یک از طرفین سازگار است. از آنجایی که اطلاعات ذخیره شده در بلاک‌چین در سراسر شبکه یکسان است، این می‌تواند ثبات، تداوم و یکپارچگی ارزیابی اعتماد را در شبکه اینترنت اشیاء تضمین کند. ویژگی ضد دستکاری تضمین می‌کند که داده‌های ثبت شده در بلاک‌چین نمی‌توانند دستکاری شوند تا بتوان رفتارهای مخرب را ردیابی کرد. البته حملاتی مانند حمله ۵۱ درصد وجود دارد که این دستکاری داده‌ها را ممکن می‌سازد. علاوه بر این، قراردادهای هوشمند می‌توانند به خودکارسازی فرایند مدیریت اعتماد به روشی قابل اعتماد کمک کنند [۳]. بنابراین، بلاک‌چین به یک فناوری امیدوارکننده برای غلبه بر مشکلات مدیریت اعتماد و دستیابی به مدیریت اعتماد غیرمتمرکز تبدیل می‌شود. به همین منظور در این مقاله یک روش مدیریت اعتماد مبتنی بر بلاک‌چین ارائه شده است که اعتماد گره‌ها را با توجه به معیار کیفیت خدمات ارزیابی و براساس امتیاز اعتماد آن‌ها را سطح‌بندی می‌کند.

در بخش ۲ به بررسی روش‌های مدیریت اعتماد مبتنی بر بلاک‌چین می‌پردازیم و سپس در بخش ۳ روش پیشنهادی شرح داده می‌شود و در بخش ۴ به ارزیابی روش پیشنهادی و مقایسه آن با روش‌های مطرح پرداخت خواهد شد، در انتها در بخش ۵ نتیجه‌گیری و کارهای آتی در این زمینه بیان شده است.

۲- مفاهیم پایه و پیشینه تحقیق

در این بخش ابتدا انواع حملات مربوط به اعتماد را بررسی خواهیم کرد و سپس به کارهای انجام شده در رابطه با مدیریت اعتماد و به طور خاص روش‌های مبتنی بر بلاک‌چین می‌پردازیم.

برخی از حملات و تهدیدها که روش‌های مدیریت اعتماد را به خطر می‌اندازند در ادامه توضیح داده شده‌اند. این تهدیدها می‌توانند اعتماد یک نهاد را به طور مخرب بالا یا پایین ببرند [۲۷].

- حملات خود تبلیغی(SPA^2): یک گره مخرب که می‌تواند اعتماد خود را با ارائه توصیه‌های خوب برای خود ارتقا دهد تا به عنوان یک ارائه‌دهنده خدمات انتخاب شود، اما پس از آن می‌تواند خدمات مخربی را ارائه دهد.
- حملات بدگویی(BMA^3): یک گره مخرب می‌تواند اعتماد یک گره با رفتار خوب را با ارائه توصیه‌های بد علیه آن از بین ببرد؛ بنابراین شانس انتخاب خدمات این گره‌های قابل اعتماد کاهش می‌یابد. این یک نوع حمله توصیه تبانی است، به عنوان مثال، یک گره مخرب می‌تواند با سایر گره‌های مخرب همکاری کند تا اعتماد یک گره خوب را از بین ببرد.
- حملات پر کردن رأی(BSA^4): یک گره مخرب می‌تواند اعتماد یک گره مخرب را با ارائه توصیه‌های خوب افزایش دهد، تا شانس انتخاب آن گره مخرب را به عنوان ارائه‌دهنده خدمات افزایش دهد. این شکل دیگری از حملات توصیه تبانی است، به عنوان مثال، می‌تواند با سایر گره‌های مخرب همکاری کند تا اعتماد یکدیگر را افزایش دهند.
- حملات روشن- خاموش(OOA^5): در این نوع حمله یک گره مخرب در یک دوره زمانی خوب رفتار می‌کند تا به شهرت خوبی دست یابد، سپس از این اعتماد برای فریب دادن سیستم اعتماد سوء استفاده می‌کند. در واقع یک گره مخرب خدمات بدی را به طور تصادفی انجام می‌دهد تا از برچسب‌زدن به عنوان یک گره مخرب و خطر انتخاب نشدن به عنوان یک ارائه‌دهنده خدمات جلوگیری کند.

روش‌های مختلفی برای مدیریت اعتماد ارائه شدند که می‌توان آن‌ها را به دو دسته متمرکز و توزیع‌شده طبقه‌بندی کرد. در رویکرد متمرکز، از یک ایستگاه پایه یا سرور برای محاسبه امتیاز اعتماد برای همه گره‌ها استفاده می‌شود. به دلیل چالش‌ها و مسائل مقیاس‌پذیری و وجود یک نقطه خرابی و هزینه زیاد که در روش‌های متمرکز وجود دارد، امروزه بیشتر از رویکردهای توزیع شده استفاده می‌شود. در رویکردهای توزیع شده، تمام گره‌های شرکت‌کننده می‌توانند امتیاز اعتماد را محاسبه کنند. اگر چه روش‌های غیرمتمرکز مزایای زیادی دارند؛ اما با محدودیت‌هایی در تبادل و ذخیره داده‌ها با منابع محدود مواجه هستند و برای تکمیل محاسبه نهایی و نگهداری اطلاعات اعتماد به سرورهای مرکزی نیاز دارند.

بنابراین، در سال‌های اخیر فناوری بلاک‌چین برای توسعه نوآوری‌های امنیتی در زمینه مدیریت اعتماد در اینترنت اشیاء مورد استفاده قرار گرفته است. به همین منظور در ادامه به بررسی روش‌های مدیریت اعتماد مبتنی بر بلاک‌چین می‌پردازیم.

مالک و همکاران [۴] یک چارچوب مدیریت اعتماد غیرمتمرکز و ایمن مبتنی بر بلاک‌چین برای زنجیره‌های تامین پیشنهاد کردند. این روش شامل سه لایه داده، بلاک‌چین و کاربردی است. در این روش داده‌های خام در یک پایگاه داده خارج از بلاک‌چین ذخیره می‌شود و تراکنش‌ها در بلاک‌چین ذخیره می‌شوند و توسط مجموعه‌ای از قوانین دسترسی مدیریت می‌شوند. این چارچوب به هر جزء در زنجیره تامین اجازه می‌دهد تا قابلیت اطمینان داده‌های تولید شده توسط شرکت‌کنندگان در زنجیره تامین را ارزیابی کند. در این روش از قراردادهای هوشمند برای محاسبه خودکار امتیازات اعتماد بر اساس داده‌های ارائه شده و اعمال مجازات و پاداش برای شرکت کنندگان در زنجیره تامین استفاده می‌شود. در واقع هدف از روش پیشنهادی تعیین مکانیزم‌هایی برای ایجاد اعتماد در داده‌ها در مبدا و اطمینان از داده‌های ثبت شده در بلاک‌چین است. این روش سربار و تاخیر کمی در مقایسه با روش‌های مشابه دارد اما تحت حملات مخربی مانند حملات بدگویی[۶] و رای گیری[۷] ارزیابی نشده است.

شالا و همکاران [۵] یک رویکرد جدید را با ادغام فناوری بلاک‌چین در فرآیندهای ارزیابی اعتماد پیشنهاد می‌کنند. در این روش رفتار یک سرویس کاربردی توسط یک یا چند کاربر نهایی که به عنوان عامل تست عمل می‌کنند، ارزیابی می‌شود. فرایند ارزیابی شامل تست عملکرد و کارایی است که در برابر سرویس کاربردی اجرا می‌شود. در این روش از بلاک‌چین برای ثبت ارائه‌دهندگان خدمات، ذخیره ایمن تمام داده‌های اعتماد محاسبه شده و هماهنگی و همکاری بین عوامل اعتماد در حین ارزیابی اعتماد استفاده می‌شود. روش پیشنهاد شده قابلیت اطمینان کلی محیط خدمات را افزایش می‌دهد اما فاقد جزئیات در مورد پارامترهای اعتماد و مدل ریاضی و ارزیابی روش ارائه شده می‌باشد.

وانگ و همکاران [۶] یک مدل مدیریت اعتماد مبتنی بر بلاک‌چین پیشنهاد دادند. طرح پیشنهاد شده از بلاک‌چین چند لایه که شامل مدیریت هویت گره‌ها نیز می‌باشد برای مدیریت اعتماد استفاده می‌کند. در این روش به هر دستگاه برچسب‌هایی اختصاص داده شده که این برچسب‌ها به عنوان تأیید اعتبار عمل می‌کنند، نویسندگان تاکید کرده‌اند که هیچ دسترسی غیرقانونی انجام نمی‌شود. روش پیشنهاد شده به افزایش سطح اعتماد دستگاه‌ها کمک می‌کند اما فاقد ارزیابی دقیقی از اعتماد می‌باشد و عملکرد آن در برابر حملات مختلف ارزیابی نشده است.

جدول ۱: بررسی روش‌های مدیریت اعتماد مبتنی بر بلاکچین

مرجع	سال	مزایا	معایب
[۴]	۲۰۱۹	سربار و تاخیر کم استفاده از سیستم مجازات و پاداش	عدم مقاومت در برابر حمله بدگویی و پرکردن رای
[۵]	۲۰۱۹	افزایش‌قابلیت اطمینان کلی محیط	فاقد جزئیات و پارامترهای اعتماد و مدل ریاضی
[۶]	۲۰۱۹	افزایش سطح اعتماد دستگاه‌ها	عدم ارزیابی عملکرد آن در برابر حملات مختلف
[۷]	۲۰۲۰	صرفه‌جویی در انرژی و هزینه‌های تراکنش	عدم ارزیابی آن در برابر حملات مختلف و عدم بررسی صداقت و رفتار غیر مستقیم گره‌ها
[۸]	۲۰۲۰	مقیاس‌پذیری مناسب حفظ حریم خصوصی	آسیب پذیر بودن در برابر حمله روشن-خاموش عدم ایجاد انگیزه برای صاحبان داده‌ها
[۹]	۲۰۲۰	مقیاس‌پذیری مناسب مقاوم در برابر حملات	عدم ایجاد سیستم مجازات و پاداش برای ایجاد انگیزه
[۱۰]	۲۰۲۲	مقیاس پذیر حفظ حریم خصوصی شامل‌سیستم مجازات و پاداش	عدم ارزیابی عملکرد آن در برابر حملات بدگویی و پرکردن رای

اوالحاج و همکاران [۷] یک مدل مدیریت اعتماد غیرمتمرکز را پیشنهاد کردند که از فناوری بلاک‌چین مبتنی بر زنجیره مارکوف استفاده می‌کند. در این روش امتیاز اعتماد توسط ماینرها و بر اساس میزان صداقت و همکاری محاسبه می‌شود. به‌روزرسانی امتیاز اعتماد بر اساس انتقال مستقیم بین گره‌ها است و صداقت و رفتار غیرمستقیم گره‌ها در نظر گرفته نمی‌شود. مدل پیشنهادی به همه دستگاه‌های اینترنت اشیاء اجازه می‌دهد، در به‌روزرسانی امتیاز اعتماد به روشی غیرمتمرکز شرکت کنند و گره‌هایی که رفتار مخربی دارند و امتیاز اعتماد اشتباهی را ارائه می‌کنند شناسایی کنند. این رویکرد مدیریت اعتماد غیرمتمرکز باعث صرفه‌جویی در هزینه‌های تراکنش و انرژی در نتیجه ادغام با فناوری بلاک‌چین می‌شود.

پوترا و همکاران [۸] یک سیستم اعتماد و اعتبار را معرفی کردند که از بلاک‌چین برای کنترل دسترسی بین دستگاه‌های اینترنت اشیاء استفاده می‌کند. نویسندگان از اعتبار به عنوان یک ویژگی برای کنترل دسترسی به یک دستگاه استفاده می‌کنند و حداقل اعتباری را که یک دستگاه باید برای تضمین دسترسی به داده‌ها داشته باشد تعریف می‌کنند. اجزای اصلی معماری پیشنهادی شامل دستگاه‌های اینترنت اشیاء، ذخیره سازی داده‌ها، مرجع ویژگی و بلاک‌چین است. این سیستم سه قرارداد هوشمند اصلی را برای

اعتبارسنجی ویژگی، محاسبه اعتماد و اعتبارسنجی خط مشی دسترسی در نظر می‌گیرد. روش پیشنهاد شده مقیاس‌پذیری خوبی دارد و حریم خصوصی هر گره را حفظ می‌کند، اما در برابر حملات روشن- خاموش[8] آسیب‌پذیر است و همچنین پاداشی به منظور ایجاد انگیزه برای صاحبان داده‌ها در نظر نمی‌گیرد.

دجمل ادین و همکاران [۹]، یک پروتکل مدیریت اعتماد غیرمتمرکز را پیشنهاد کردند. روش پیشنهادی مبتنی بر فناوری بلاک‌چین و الگوی محاسبات مه[9] می‌باشد، که در آن گره‌های مه با منابع محاسباتی کافی، بلاک‌چین را حفظ می‌کنند و تمام محاسبات اعتماد مورد نیاز را انجام می‌دهند، که این به کاهش سربارمحاسباتی در دستگاه‌ها با منابع محدود کمک می‌کند. در این روش قابل اعتماد بودن یک ارائه‌دهنده خدمات خاص از تجربه مستقیم کاربر و توصیه‌های همتایان ناشی می‌شود. این روش در برابر حملات شناخته شده مربوط به اعتماد مقاوم است، اما فاقد سیستم مجازات و پاداش، برای ایجاد انگیزه در گره‌ها می‌باشد و همچنین مشخص نشده که برای ارزیابی اعتماد چه معیارهایی را در نظر می‌گیرد.

عمار و همکاران [۱۰]، یک معماری مقیاس پذیر برای دستیابی به اعتماد پیشنهاد کردند. در این روش از فناوری بلاک‌چین به همراه قرارداد هوشمند استفاده شده است. از قرارداد هوشمند برای اعمال سیاست‌های کنترل دسترسی و تعاملات استفاده می‌شود. چارچوب پیشنهادی بر یک طرح پاداش و مجازات متکی است و یک معماری اعتماد قابل تنظیم، ایمن و مقیاس پذیر را برای دستگاه های IoT ارائه می‌دهد اما این روش تنها در برابر حمله روشن- خاموش ارزیابی شده است. در جدول ۱، مقایسه روش‌های مبتنی بر بلاک‌چین که به آن‌ها اشاره شد، انجام شده است.

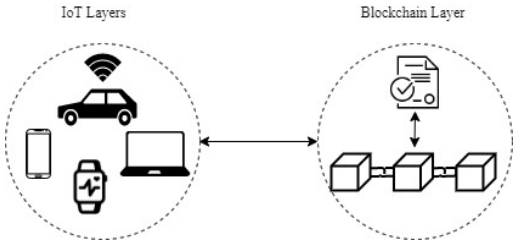
۳- روش پیشنهادی

در این بخش یک روش مدیریت اعتماد مبتنی بر بلاک‌چین به منظور ایجاد اعتماد بین گره‌های اینترنت اشیاء ارائه می‌دهیم. تا گره‌ها بتوانند با اطمینان با یکدیگر ارتباط برقرار کرده و از یکدیگر خدمات صحیح و با کیفیتی را دریافت کنند.

شکل ۱ شمای کلی معماری روش پیشنهادی را نشان می‌دهد. در روش پیشنهادی دو لایه وجود دارد که در ادامه به معرفی لایه‌ها در این روش می‌پردازیم:

لایه بلاک‌چین: در معماری پیشنهادی، بلاک‌چین مسئولیت مدیریت اعتماد را برعهده دارد. در واقع بلاک‌چین به‌واسطه استفاده از قرارداد هوشمند قادر است محیطی قابل اعتماد و اطمینان ایجاد کند که در آن دستگاه‌ها بتوانند بدون نگرانی با یکدیگر تعامل داشته باشند. قرارداد هوشمند مسئولیت ذخیره‌سازی امتیاز اعتماد تمام گره‌ها را بر عهده دارد.

لایه دستگاه‌های اینترنت اشیاء: این لایه شامل دستگاه‌های اینترنت اشیاء است هر دستگاه می‌تواند به دستگاه‌های دیگر خدمات ارائه دهد، بنابراین به عنوان ارائه‌دهنده خدمات (SP[10]) در نظر گرفته می‌شود یا می‌تواند از دستگاه‌های دیگر خدمات درخواست کند که در این صورت به عنوان درخواست‌کننده خدمات (SR[11]) در نظر گرفته می‌شود. هر دستگاه اینترنت اشیاء در سیستم با یک کلید عمومی مشخص می‌شود.



شکل ۱: معماری روش پیشنهادی

۳-۱- مراحل روش پیشنهادی

روش پیشنهادی شامل مراحل راه‌اندازی، درخواست خدمات، انتشار اعتماد و ارزیابی اعتماد می‌باشد. در مرحلهٔ راه‌اندازی، دستگاه‌های موجود در شبکه شناسایی و ثبت‌نام می‌شوند تا به عنوان یک موجودیت در شبکه محسوب گردند. این عمل باعث می‌شود تا اگر دستگاه جدیدی به شبکه اضافه شد قبل از ارتباط با دیگر دستگاه‌ها در شبکه، احراز هویت و در شبکه ثبت شود. پس از آن مقداردهی اولیه دستگاه‌ها و ثبت خدمات آن‌ها می‌باشد. در مرحله درخواست خدمات هر گره‌ای که مایل به دریافت خدمتی است، باید شناسه آن خدمت را به قرارداد هوشمند ارسال کند. پس از آن در مرحله انتشار اعتماد هر گره موظف است، پس از دریافت خدمات، میزان رضایت خود را در برابر سرویسی که دریافت کرده در قالب مشاهده مستقیم به قرارداد هوشمند ارسال کند. در نهایت در مرحله ارزیابی اعتماد، قرارداد هوشمند به بررسی امتیاز اعتماد ارسال شده بر اساس قوانین از پیش تعریف شده می‌پردازد. شکل ۲ مراحل مختلف روش پیشنهادی را نشان می‌دهد. در ادامه به توضیح هر کدام از مراحل می‌پردازیم:

۳-۱-۱- مرحله راه‌اندازی

۱) شناسایی و ثبت‌نام: در این مرحله هر دستگاه برای اضافه‌شدن به شبکه باید توسط مدیر سیستم بررسی شود و با استفاده از یک زیر ساخت کلید عمومی بر روی یک بستر امن توسط قرارداد هوشمند برای هر دستگاه یک جفت کلید عمومی و خصوصی ایجاد

می‌شود و در بلاک‌چین ثبت و نگهداری می‌شود. کلیدهای عمومی به عنوان شناسه موجودیت هر گره عمل می‌کنند و پس از ثبت کلید عمومی در بلاک‌چین و احراز هویت می‌تواند در شبکه شروع به کار نماید.

۲) مقداردهی اولیه: در این مرحله به هر دستگاه بر اساس تست عملکرد آن یک مقدار اعتماد اولیه داده می‌شود. بر اساس مقداراعتماد اولیه دستگاه‌ها هر کدام در سه سطح مختلف قرار می‌گیرند و هر درخواست‌کننده خدمات تنها می‌تواند از ارائه‌دهندگان سطح خود خدمات دریافت کند. مقدار پارامترهای a و b که اعتماد هر سطح را مشخص می‌کنند، بر اساس آزمایش‌ها به ترتیب برابر ۰. و ۰.۵ می‌باشند.

$$L_i = \begin{cases} \text{L3 (high trust)} & \text{if } T_i > a \\ \text{L2 (trust)} & \text{if } b \le T_i \le a \\ \text{L1 (low trust)} & \text{if } T_i \le b \end{cases} \quad (1)$$

۳) ثبت خدمات: برای این که دستگاه‌های اینترنت اشیاء بتوانند خدمات موجود را کشف کنند، ارائه‌دهندگان خدمات، خدمات خود را در بلاک‌چین ثبت می‌کنند که از یک جدول هش برای ذخیره خدمات مختلف استفاده می‌شود، این جدول در بلاک‌چین نگهداری می‌شود.

۳-۱-۲- مرحله درخواست خدمات

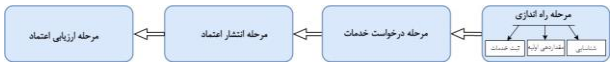
در این مرحله هر گره‌ای که نیازمند دریافت خدمتی است باید ابتدا شناسه آن خدمت را برای قرارداد هوشمند ارسال کند. قرارداد هوشمند پس از دریافت پیام درخواست خدمات، ابتدا امتیاز اعتماد آن درخواست‌کننده خدمات را بررسی می‌کند که تعیین کند که آن درخواست‌کننده خدمات در چه سطحی می‌باشد. پس از تعیین شدن سطح آن درخواست‌کننده خدمات، قرارداد هوشمند مجموعه‌ای از ارائه‌دهندگان آن خدمت که هم سطح با آن هستند را مشخص می‌کند. پس از تعیین شدن ارائه‌دهندگان خدمات هم سطح با آن درخواست‌کننده، قرارداد هوشمند براساس معیارهایی مانند زمان پاسخ‌گویی و پذیرش خدمات یکی از ارائه‌دهندگان خدمات را به SR برای دریافت خدمات معرفی می‌کند. در صورتی که خدمات‌دهنده‌ای در سطح گره درخواست‌کننده وجود نداشته باشد، قرارداد هوشمند یکی از خدمات‌دهندگان سطح پایین‌تر را معرفی می‌کند و در صورتی که خدمات‌دهنده‌ای در سطوح پایین‌تر نیز وجود نداشت، با درخواست آن مخالفت می‌کند و آن درخواست‌کننده برای گرفتن خدمات از سطح بالاتر باید ابتدا میزان اعتماد خود را با دادن خدمات بهتر ارتقا دهد و مجدداً درخواست خود را ارسال نماید.

۳-۱-۳- مرحله انتشار اعتماد

هر دستگاه باید مشاهده مستقیم خود را در مورد ارائه‌دهنده خدماتی که از آن خدمت دریافت کرده به بلاک‌چین گزارش کند. مقدار ارسال شده به بلاک‌چین حاوی اطلاعات شناسه گره اعتماد کننده، شناسه گره متولی، نوع سرویس، مجموعه‌ای از معیارها، مقدار اعتماد و زمان است.

- شناسه گره اعتماد کننده: کلید عمومی درخواست‌کننده خدمات می‌باشد.
- شناسه گره متولی: کلید عمومی ارائه‌دهنده خدمات می‌باشد.
- نوع سرویس: نشان‌دهنده سرویسی است که توسط SP به دستگاه SR ارائه می‌شود.
- معیارها: مجموعه‌ای از معیارها را نشان می‌دهد که درخواست‌کننده خدمات، خدمات را براساس آن ارزیابی کرده است.
- مقدار اعتماد: به سطح اطمینان ارائه‌دهنده خدمات اشاره دارد که توسط درخواست‌کننده خدمات ارزیابی شده است.
- زمان: نشان دهنده زمان دقیق اتمام تراکنش می‌باشد.

دستگاه ارسال‌کننده توصیه، تراکنش را با کلید خصوصی خود امضا و آن را به بلاک‌چین ارسال می‌کند، پس از دریافت تراکنش صحت امضاها بررسی و تراکنش‌های معتبر در یک بلوک جمع‌آوری می‌شوند. بلوک‌ها برای اعتبارسنجی به گره‌های اعتبارسنج ارسال می‌شوند و پس از تأیید به بلاک‌چین افزوده می‌شوند.



شکل ۲: مراحل روش پیشنهادی

۳-۱-۴- مرحله ارزیابی اعتماد

هر گاه یک دستگاه i بخواهد سرویس S_k را در زمان t درخواست کند. درخواست سرویس S_k را به بلاک‌چین ارسال می‌کند. قرارداد هوشمند پس از دریافت درخواست، ابتدا مقدار اعتماد آن گره را بررسی و سپس از بین ارائه‌دهندگان خدماتی که در آن سطح هستند یکی را به آن درخواست کننده خدمات (i) معرفی می‌کند. سپس درخواست‌کننده خدمات از آن ارائه‌دهنده خدمات (SP)، خدمت دریافت می‌کند. پس از دریافت خدمات گره i امتیاز اعتماد خود که حاصل تعامل مستقیم است را به بلاک‌چین ارسال می‌کند. مشاهده مستقیم هر دستگاه به صورت رابطه (۲) محاسبه می شود:

$$D_{ij}^{S_k}(t) = \frac{\alpha_{ij}}{n} = \frac{\sum_{t_\tau \in \{t_1,\dots,t_n\}} S_{ij}(t_\tau)}{n} \quad (۲)$$

$D_{ij}^{S_k}(t)$ یک عدد در محدوده $[0,1]$ می‌باشد که میزان رضایت دستگاه i در برابر سرویس S_k که از دستگاه j در زمان t دریافت کرده است، را نشان می‌دهد. $S_{ij}(t)$ سطح رضایت در زمان t را نشان می‌دهد و α_{ij} مجموع سطوح رضایت گره i از گره j از ابتدا تاکنون است که به صورت مداوم طبق رابطه (۳) به‌روز می‌شود.

$$\alpha_{ij} = \alpha_{ij} + S_{ij}(t) \quad (۳)$$

n نشان‌دهنده تعداد کل تجربیات مثبت و منفی می‌باشد و t نشان‌دهنده لحظه‌ای است که سرویس S_k درخواست شده است.

پس از ارسال مشاهده مستقیم، قرارداد هوشمند به بررسی شرط $|M_{T_j} - D_{ij}^{S_k}(t)| > 0.5$ می‌پردازد و در صورتی که شرط برقرار باشد، گره i صادق نیست و درصدی از امتیاز اعتماد او به عنوان مجازات کم می‌شود و همچنین توصیه i نادیده گرفته می‌شود. در صورتی که شرط برقرار نباشد به‌دلیل ارسال توصیه، به گره i پاداش داده می‌شود. (درصدی به امتیاز اعتماد او افزوده می‌شود)

$$M_{T_j}(t) = \begin{cases} M_{T_j}(t-1), & \text{if } |M_{T_j} - D_{ij}^{S_k}(t)| > 0.5 \text{(malicious)} \\ \gamma M_{T_j}(t-1) + (1-\gamma) D_{ij}^{S_k}(t), & \text{else (Honest)} \end{cases} \quad (۴)$$

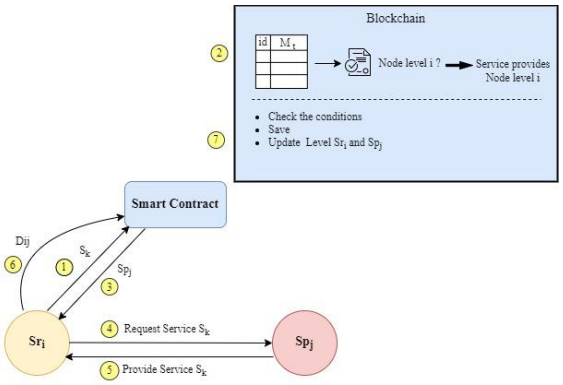
$M_{T_j}(t-1)$ نشان‌دهنده آخرین مقدار میانگین اعتماد ارائه‌دهنده خدمات j می‌باشد و γ برای سنجش اهمیت هر پارامتر می‌باشد. پس از هر بار تعامل بین درخواست‌کننده خدمات و ارائه‌دهنده خدمات، مقدار اعتماد ارائه‌دهنده و درخواست‌کننده خدمات توسط قرارداد هوشمند بررسی می‌شود تا بر اساس مقدار اعتماد خود در سطح مورد نظر قرار گیرند. شکل ۳ به صورت جامع مراحل روش پیشنهادی را نشان می‌دهد.

مرحله ۱: در مرحله اول گره درخواست‌کننده خدمات درخواست خود را برای دریافت خدمت S_k به قرارداد هوشمند ارسال می‌کند.

مرحله ۲: قرارداد هوشمند پس از دریافت درخواست خدمت، ابتدا مقدار اعتماد درخواست‌کننده خدمات را بررسی می‌کند تا تعیین کند که درخواست‌کننده خدمات در چه سطحی می‌باشد. پس از تعیین سطح، مجموعه‌ای از ارائه‌دهندگان هم سطح با درخواست‌کننده مشخص می‌شوند.

مرحله ۳: قرارداد هوشمند بر اساس معیارهایی مانند زمان پاسخ‌گویی، یکی از ارائه‌دهندگان خدمات را برای ارائه خدمت به درخواست‌کننده خدمات معرفی می‌کند.

مرحله ۴: درخواست‌کننده خدمات، درخواست خود را برای دریافت



شکل ۳: گام‌های اصلی روش پیشنهادی

خدمت به آن ارائه‌دهنده خدمات ارسال می‌کند.

مرحله ۵: ارائه‌دهنده خدمات پس از دریافت درخواست، خدمت مورد نظر را به آن درخواست‌کننده ارائه می‌کند.

مرحله ۶: درخواست‌کننده خدمات پس از دریافت خدمت باید میزان رضایت خود را در برابر خدمت دریافتی با عنوان مشاهده مستقیم به قرارداد هوشمند ارسال کند.

مرحله ۷: پس از دریافت مشاهده مستقیم، قرارداد هوشمند اختلاف آن را با میانگین اعتماد ارائه‌دهنده خدمات که تاکنون براساس خدمات ارائه شده به گره‌های شبکه به دست آمده است، بررسی می‌کند. در صورتی که اختلاف آن‌ها بیشتر از حد آستانه باشد، توصیه آن گره نادیده گرفته شده و آن گره به عنوان گره مخرب شناسایی می‌شود. پس از شناسایی آن گره به عنوان گره مخرب، درصدی از امتیاز اعتماد آن گره به منظور مجازات برای توصیه اشتباهی که ارائه داده است، کم می‌شود.

در صورتی که اختلاف مشاهده مستقیم با میانگین اعتماد آن ارائه‌دهنده خدمات کمتر از حد آستانه باشد توصیه آن گره طبق رابطه ۴ در نظر گرفته شده و آن گره به عنوان گره صادق شناسایی و شامل پاداش می‌شود. پس از آن به دلیل ارسال توصیه صادق، به امتیاز اعتماد آن گره افزوده می‌شود. با این روش گره‌های مخرب نمی‌توانند با توصیه‌های بد اعتماد یک گره را تغییر دهند.

در نهایت قرارداد هوشمند مجدداً به بررسی امتیاز اعتماد آن ارائه‌دهنده و درخواست‌کننده خدمات می‌پردازد تا در صورت لزوم سطح آن‌ها را تغییر دهد.

۳-۲- تولید بلوک و پروتکل اجماع

پس از ارزیابی اعتماد، امتیاز اعتماد ارزیابی شده و سایر اطلاعات مربوط به اعتماد با درج اطلاعات موجود در تراکنش در بلاک‌چین ذخیره می‌شود. اطلاعات ذخیره شده باید با استفاده از روش‌های اجماع اعتبارسنجی شوند. اجماع ما ترکیبی از الگوریتم‌های

PBFT[12] و POS[13] است و ارائه‌دهندگان با امتیاز اعتماد بالا به عنوان اعتبارسنج انتخاب می‌شوند. پس از دریافت درخواست معتبر اعتبارسنجی، هر اعتبارسنج تراکنش‌های تشکیل‌دهنده بلوک، صحت امضاها و مهر زمان را بررسی می‌کند، سپس تراکنش‌های تأیید شده در یک بلوک جمع‌آوری و به دفترکل افزوده می‌شوند.

برای اطمینان از سطح امنیتی بالا، امتیاز اعتماد هر ارائه‌دهنده خدمات به عنوان یک مفهوم از پشته در نظر گرفته می‌شود. بنابراین، ارائه‌دهندگان خدمات با امتیاز اعتماد بالا به احتمال زیاد به عنوان اعتبارسنج انتخاب می‌شوند. مکانیزم PBFT قادر به پشتیبانی حداکثر f "خطاهای بیزانس[14]" است اگر و فقط اگر شبکه حداقل از 3f+1 گره تشکیل شده باشد.

پروتکل اجماع شامل مراحل زیر می‌باشد:

۱) انتخاب اعتبارسنج‌ها: پس از تشکیل یک بلوک هر پیشنهاد دهنده بلوک نیاز به انتخاب $\log n$ اعتبارسنج از مجموعه n ارائه‌دهنده خدمات دارد که مقدار اعتماد بالاتر از آستانه دارند. انتخاب تصادفی با توجه به مقادیر اعتماد ارائه‌دهندگان خدمات است. بنابراین هر ارائه‌دهنده خدمات SP_j یک احتمال شناخته‌شده برای انتخاب دارد که با نسبت $\frac{T_j}{\sum_{k=1}^{n} T_k}$ مطابقت دارد. بنابراین ارائه‌دهندگان خدمات با قابلیت اطمینان بالا احتمال بالایی برای انتخاب دارند. هنگامی که انتخاب اعتبارسنج‌ها انجام شد پیشنهاد دهنده بلوک یک پیام معتبر به اعتبارسنج‌های انتخاب شده ارسال می‌کند و بلوک را برای همه‌ی گره‌های بلاک‌چین ارسال می‌کند.

۲) مرحله قبل از رأی‌گیری: پس از دریافت درخواست معتبر اعتبارسنجی، هر اعتبارسنج تراکنش‌های تشکیل دهنده بلوک را بررسی و صحت امضاها و مهر زمان را در هر تراکنش تأیید می‌کند. در صورت صحیح بودن بلوک، اعتبارسنج پیام‌های قبل از رأی‌گیری را برای سایر اعتبارسنج‌ها ارسال می‌کند. سپس منتظر پذیرش دریافت $\frac{2}{3} * \log n$ پیام قبل از رای می‌ماند.

۳) مرحله قبل از تعهد: هنگامی که گره اعتبارسنج $\frac{2}{3} * \log n$ پیام‌های پیش از رای‌گیری را از سایر گره‌های اعتبارسنج دریافت کرد، یک پیام پیش تعهد را برای همه شرکت‌کنندگان در بلاک‌چین پخش می‌کند.

۴) مرحله تعهد: هر گره در بلاک‌چین در صورت دریافت حداقل $\frac{2}{3} * \log n$ پیام قبل از تعهد، بلوک را متعهد می‌کند. به منظور محافظت از پروتکل در برابر خطاهای Byzantine در انتشار پیام‌ها و بلوک‌ها ما پس از ارسال هر پیام یا بلوک یک مهلت زمانی را در نظر می‌گیریم. بنابراین هر گره منتظر مهلت زمانی مشخص مربوط به هر مرحله است که در صورت منقضی شدن زمان، گره بلوک را برای تائید اعتبار رها می‌کند. تمام پیام‌هایی که در این مراحل رد و بدل می‌شوند توسط کلیدهای خصوصی فرستندگان به صورت دیجیتالی امضا می‌شوند.

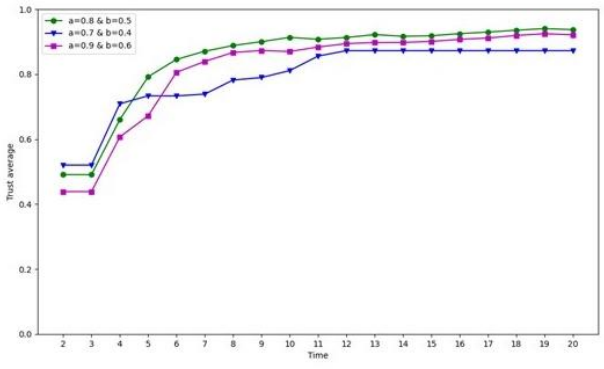
۴- ارزیابی و نتایج

در این بخش به منظور نشان دادن اثربخشی روش پیشنهادی، ابتدا روش پیشنهادی با مدل BC-Trust در مرجع [۹] مقایسه و سپس روش پیشنهادی در برابر حملات مختلف ارزیابی شده است. پارامترهای ارزیابی که برای انجام شبیه‌سازی در نظر گرفته شده است، در جدول ۲ آورده شده است، مقادیر مناسب این پارامترها پس از آزمایش‌های متعدد به دست آمده است. تمامی شبیه‌سازی‌های انجام شده در محیط چند نخی زبان جاوا پیاده‌سازی شده است و حداقل هر آزمایش ۱۰ بار انجام شده است و میانگین نتایج گزارش شده است.

جدول ۲: پارامترهای ارزیابی

پارامتر	مقدار
تعداد کل گره‌ها	۱۰۰
تعداد سرویس	۱
میزان پاداش	۰/۱۵
میزان مجازات	۰/۲۰
پارامتر a	۰/۸
پارامتر b	۰/۵
پارامتر γ	۰/۲۵

شکل ۴ میانگین اعتماد گره‌های صادق را با توجه به پارامترهای سطح‌بندی a و b نشان می‌دهد. همان‌طور که در شکل ۴ نشان داده شده است، در حالتی که پارامتر a برابر ۰/۸ و b برابر ۰/۵ باشد، میانگین اعتماد گره‌های صادق نسبت به حالت‌های دیگر مقدار بیشتری دارد. به همین منظور این مقادیر برای سطح‌بندی در نظر گرفته شده‌اند.



شکل۴: میانگین اعتماد گره‌های صادق با مقادیر مختلف پارامترهای a و b

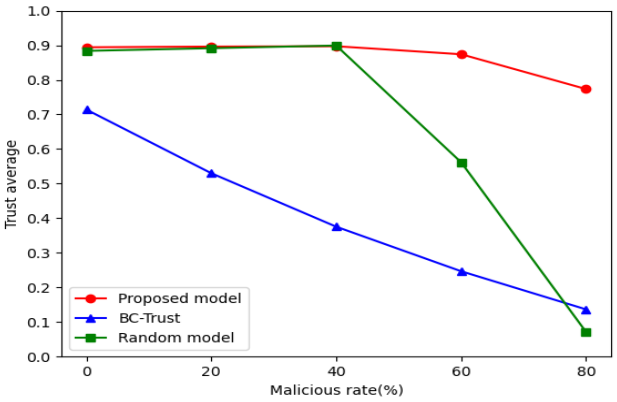
به منظور ارزیابی روش پیشنهادی در سناریوی اول درصد گره‌های مخرب در طول آزمایش افزایش می‌یابد و بر اساس آن میزان اعتماد گره‌های صادق ارزیابی می‌شود. هدف از این آزمایش بررسی تغییرات اعتماد و مقایسه روش پیشنهادی با روش BC-Trust [۹] و مدل تصادفی است. مدل تصادفی همان مدل پایه روش پیشنهادی می‌باشد با این تفاوت که انتخاب ارائه‌دهنده خدمات به صورت تصادفی صورت می‌گیرد و شامل روش سطح‌بندی گره‌های اینترنت اشیاء نمی‌باشد.

شکل ۵ امتیاز اعتماد گره‌های صادق نسبت به افزایش درصد گره‌های مخرب را نشان می‌دهد. همان‌طور که در شکل ۵ نشان داده شده است میانگین اعتماد گره‌های صادق در روش پیشنهادی در مقایسه با دو مدل دیگر بیشتر است. در حالتی که درصد گره‌های مخرب کمتر است، روش پیشنهادی با روش تصادفی تقریباً اعتماد یکسانی دارند، اما زمانی که درصد گره‌های مخرب از نصف بیشتر می‌شود روش پیشنهادی عملکرد مناسب‌تری در مقایسه با مدل تصادفی دارد. مدل BC-Trust در مقایسه با روش پیشنهادی و مدل تصادفی عملکرد مناسبی ندارد که این می‌تواند به دلیل انتخاب تصادفی ارائه‌دهندگان خدمات و نبود سیستم مجازات و پاداش باشد. مدل تصادفی در حالتی که درصد گره‌های مخرب بین ۰ تا ۴۰ درصد می‌باشد عملکرد مناسبی دارد چون درصد گره‌های مخرب در مقایسه با گره‌های صادق کمتر است بنابراین احتمال انتخاب یک گره مخرب به عنوان ارائه‌دهنده خدمات و تأثیر حملات نیز کمتر است. اما در حالتی که درصد گره‌های مخرب از ۴۰ درصد بیشتر شود احتمال انتخاب آن‌ها به عنوان ارائه‌دهنده خدمات و همچنین حملاتی که علیه گره‌های صادق انجام می‌دهند بیشتر می‌شود که این موجب کاهش میانگین اعتماد گره‌های صادق می‌شود.

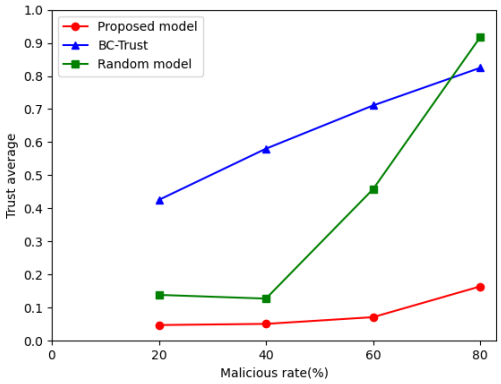
در روش پیشنهادی به دلیل سطح‌بندی گره‌ها، هر گره تنها امکان دریافت خدمات از ارائه‌دهندگان سطح خود را دارد که این موجب شده تا در صورتی که گره‌ها نیاز به دریافت خدمات بهتر و باکیفیت‌تری دارند تلاش کنند که امتیاز اعتماد خود را افزایش دهند تا به سطح بالاتری برسند و از ارائه‌دهندگان با اعتماد خدمات بهتری دریافت کنند. از طرفی شرطی که هر بار هنگام ارسال مشاهده مستقیم، به بررسی اختلاف مشاهده مستقیم و میانگین اعتماد می‌پردازد موجب شده تا گره‌هایی که رفتار نادرستی دارند و امتیاز اعتماد نادرستی را ارسال می‌کنند به عنوان گره مخرب شناسایی شده و شامل مجازات شوند که این مجازات با کاهش امتیاز اعتماد اعمال می‌شود. روش پیشنهادی در حالتی که میزان گره‌های مخرب افزایش می‌یابد، عملکرد مناسبی دارد و امتیاز اعتماد گره‌های صادق با افزایش گره‌های مخرب چندان کاهش نمی‌یابد. زیرا گره‌ها بر اساس امتیاز اعتماد اولیه سطح‌بندی شده و با انجام رفتار مخرب شامل مجازات و سپس به سطح پائین‌تر منتقل می‌شوند. این موجب شده که به مرور زمان بیشتر گره‌های مخرب در پائین‌ترین سطح قرار گرفته و دیگر قادر به دریافت خدمات از ارائه‌دهندگان صادق و حمله علیه آن‌ها نباشند. از طرفی به دلیل این‌که انتخاب ارائه‌دهنده خدمات توسط قرارداد هوشمند صورت می‌گیرد، گره‌های مخرب نمی‌توانند انتخاب کنند که از چه کسی خدمات دریافت کنند. بنابراین، این دلایل موجب شده که با گذشت زمان بیشتر گره‌های مخرب در پائین‌ترین سطح و گره‌های صادق در سطح بالاتر قرار گیرند و گره‌های مخرب نتوانند علیه آن‌ها حملاتی انجام دهند. به همین دلیل امتیاز اعتماد گره‌های صادق با وجود ۸۰ درصد گره مخرب چندان کاهش نمی‌یابد. بنابراین وجود سطح‌بندی، اعمال شرط بررسی اختلاف میانگین اعتماد و مشاهده مستقیم و سیستم مجازات و پاداش موجب شده تا روش پیشنهادی عملکرد بهتری در مقایسه با دو روش دیگر داشته باشد.

در شکل ۶ میانگین اعتماد گره‌های مخرب در مقایسه با مدل BC-Trust و مدل تصادفی نشان داده شده است. نتیجه نشان می‌دهد که میانگین اعتماد گره‌های مخرب در روش پیشنهادی در مقایسه با دو روش دیگر بسیار کمتر است. به دلیل استفاده از سیستم پاداش و مجازات گره‌های مخرب سریع‌تر شناسایی شده و برای ادامه فعالیت‌های خود بی‌انگیزه می‌شوند زیرا منجر به پایین آمدن امتیاز اعتماد و استقبال کمتر توسط دیگر گره‌ها می‌شود.

در ادامه اثربخشی روش پیشنهادی در برابر حملات خودتبلیغی، بدگویی، پرکردن رأی و روشن خاموش ارزیابی شده است.



شکل۵: میانگین اعتماد گره‌های صادق با افزایش گره‌های مخرب



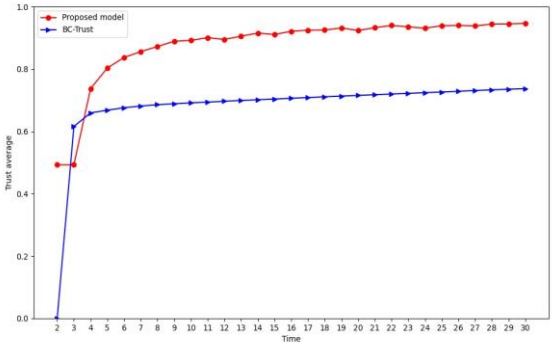
شکل۶: میانگین اعتماد گره‌های مخرب

۴-۱- حمله خود تبلیغی[۱۵]

در حمله خود تبلیغی یک سرویس‌دهنده مخرب توصیه‌های خوبی را برای خود ارسال می‌کند تا اهمیت خود را برای سایرین ارتقا دهد و سپس خدمات مخربی را ارائه دهد. در روش پیشنهادی شرطی اعمال شده که هنگام ثبت تراکنش شناسه اعتماد کننده و معتمد برابر نباشد. با اعمال این شرط هیچ گره‌ای نمی‌تواند برای خود توصیه‌ای ثبت کند، بنابراین روش پیشنهادی در برابر این حمله مقاوم است.

۴-۲- حمله بدگویی

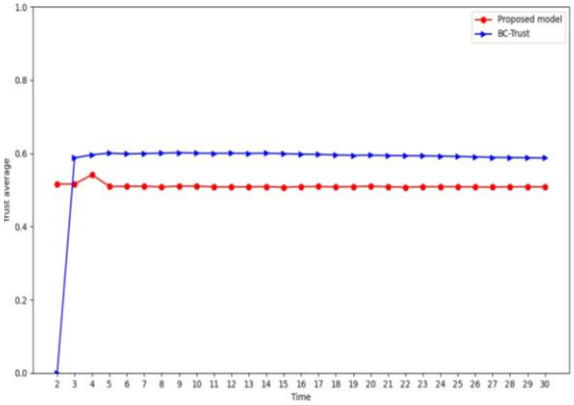
در حمله بدگویی گره‌های مخرب توصیه‌های بدی را نسبت به ارائه‌دهندگان قابل‌اعتماد ارائه می‌دهند تا آن‌ها را بدنام کرده و شانس انتخاب شدنشان را به عنوان ارائه‌دهنده خدمات کاهش دهند. برای مقابله با این حمله در روش پیشنهادی شرطی اعمال شده که پس از ارسال مشاهده مستقیم توسط هر گره، قرارداد هوشمند اختلاف میانگین اعتماد آن ارائه‌دهنده خدمات را با مشاهده مستقیم بررسی و در صورتی که اختلاف آن‌ها بیشتر از آستانه باشد، آن گره به عنوان گره مخرب شناسایی و درصدی از امتیاز اعتماد او به عنوان مجازات کم شده و آن توصیه نادیده گرفته می‌شود. به دلیل این که توصیه‌هایی که اختلاف زیادی با میانگین دارند در نظر گرفته نمی‌شوند می‌توان گفت توصیه‌های گره‌های مخربی که حمله بدگویی را انجام می‌دهند تأثیر چندانی در میانگین اعتماد ندارد و هم چنین به دلیل اعمال مجازات برای این گره‌ها و کم‌شدن امتیاز اعتماد آن‌ها از ادامه انجام کار خود دلسرد می‌شوند. بنابراین روش پیشنهادی عملکرد خوبی در برابر این حمله دارد. شکل ۷ میانگین اعتماد گره‌های صادق را زمانی که ۲۰ درصد گره‌ها مخرب هستند و حمله بدگویی را انجام می‌دهند در مقایسه با مدل BC-Trust نشان می‌دهد.



شکل۷: میانگین اعتماد گره‌های صادق تحت حمله بدگویی

۴-۳- حمله رأی‌گیری

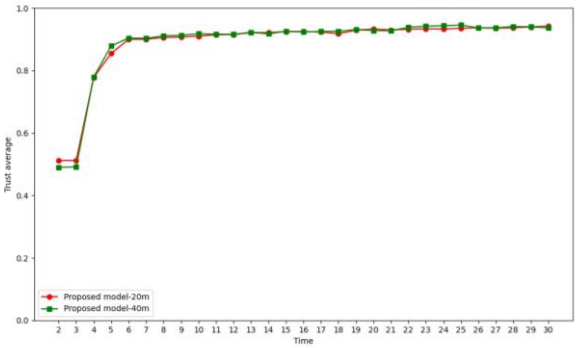
در حملات رأی‌گیری یک ارائه‌دهنده خدمات مخرب با ارائه توصیه‌های خوب نسبت به ارائه‌دهندگان خدمات مخرب سعی می‌کند قابلیت اطمینان آن‌ها را افزایش و شانس آن‌ها برای انتخاب شدن به عنوان ارائه‌دهنده خدمات افزایش دهد. در این حمله نیز مانند حمله بدگویی به دلیل استفاده از شرط بررسی اختلاف میانگین اعتماد با مشاهده مستقیم، این توصیه‌ها تأثیر کمی در میانگین اعتماد گره‌ها دارند. شکل ۸ میانگین اعتماد گره‌های مخرب را در حمله رأی‌گیری، زمانی که ۴۰ درصد از گره‌ها مخرب هستند در مقایسه با مدل BC-Trust نشان می‌دهد.



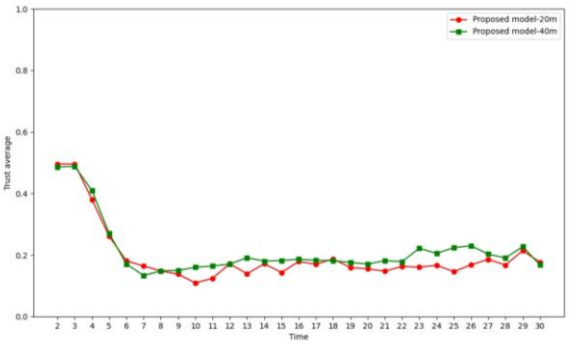
شکل ۸:میانگین اعتماد گره‌های مخرب در حمله رای گیری

۴-۴- روشن - خاموش

در حمله روشن - خاموش یک گره خدمات بد و خوب را به صورت تصادفی ارائه می‌دهد تا از خطر انتخاب نشدن به عنوان ارائه‌دهنده خدمات جلوگیری کند. شکل ۹ میانگین اعتماد گره‌های صادق را هنگامی که درصدی از گره‌های مخرب حمله روشن - خاموش را انجام می‌دهند، نشان می‌دهد. همان‌طور که در شکل مشخص می‌باشد در حالتی که ۲۰ درصد از گره‌ها مخرب هستند و حمله روشن-خاموش را انجام می‌دهند و حالتی که ۴۰ درصد از گره‌ها



شکل۹: میانگین اعتماد گره‌های صادق در حمله روشن-خاموش



شکل۱۰: میانگین اعتماد گره‌های مخرب در حمله روشن-خاموش

مخرب هستند، میانگین اعتماد گره‌های صادق در دو حالت تفاوت چندانی با هم ندارد که این نشان‌دهنده اثربخشی روش پیشنهادی در مقابله با این حمله می‌باشد.

همان‌طور که در شکل ۱۰ مشخص می‌باشد میانگین اعتماد گره‌های مخربی که حمله روشن - خاموش انجام می‌دهند با گذشت زمان کاهش می‌یابد که این نشان‌دهنده شناسایی گره‌های مخرب می‌باشد. کاهش امتیاز اعتماد گره‌های مخرب موجب عدم انتخاب این گره‌ها به عنوان ارائه‌دهنده خدمات توسط گره‌های دیگر می‌شود.

۵- نتیجه‌گیری

در این مقاله یک مدل مدیریت اعتماد مبتنی بر بلاک‌چین به منظور ارزیابی اعتماد و تشخیص گره‌های مخرب ارائه شد. در این روش هر گره پس از دریافت خدمات به ارزیابی قابلیت اطمینان آن ارائه‌دهنده خدمات می‌پردازد. مقدار اعتماد هر گره در بلاک‌چین ذخیره می‌شود به همین دلیل دستگاه‌ها نیازی به ذخیره‌سازی اطلاعات اعتماد ندارند و هم چنین امکان دست‌کاری اطلاعات اعتماد وجود ندارد. روش پیشنهادی به دلیل استفاده از سیستم مجازات و پاداش به گره‌ها انگیزه می‌دهد تا در فعالیت‌های اعتماد شرکت کنند و دلیل وجود مجازات به شناسایی گره‌های مخرب کمک می‌کند. نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی در مقایسه با روش‌های مشابه مقاومت بیشتری در برابر حملات مربوط به اعتماد دارد.

مراجع

[1] R. Kumar and R. Sharma, 'Leveraging blockchain for ensuring trust in IoT: A survey', *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8599–8622, Nov. 2022, doi: 10.1016/j.jksuci.2021.09.004.

[2] P. Cui, U. Guin, A. Skjellum, and D. Umphress, 'Blockchain in IoT: Current Trends, Challenges, and Future Roadmap', *J Hardw Syst Secur*, vol. 3, no. 4, pp. 338–364, Dec. 2019, doi: 10.1007/s41635-019-00079-5.

[3] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jantti, 'A Survey on Blockchain-based Trust Management for Internet of Things', *IEEE Internet Things J.*, pp. 1–1, 2023, doi: 10.1109/JIOT.2023.3237893.

[4] S. Malik, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, 'TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains', in *2019 IEEE International Conference on Blockchain (Blockchain)*, Atlanta, GA, USA, Jul. 2019, pp. 184–193. doi: 10.1109/Blockchain.2019.00032.

[5] B. Shala, U. Trick, A. Lehmann, B. Ghita, and S. Shiaeles, 'Blockchain-Based Trust Communities for Decentralized M2M Application Services', in *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*, vol. 24, F. Xhafa, F.-Y. Leu, M. Ficco, and C.-T. Yang, Eds. Cham: Springer International Publishing, 2019, pp. 62–73. doi: 10.1007/978-3-030-02607-3_6.

[6] Dr. Wang Haoxiang, 'Trust management of communication architectures of internet of things', *Journal of trends in Computer Science and Smart technology (TCSST) (2019) Vol.01/ No. 02 Pages: 121-130 https://www.irojournals.com/tcsst/*, Feb. 2019.

[7] O. A. Oualhaj, A. Mohamed, M. Guizani, and A. Erbad, 'Blockchain Based Decentralized Trust Management framework', in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 2210–2215. doi: 10.1109/IWCMC48107.2020.9148247.

[8] G. D. Putra, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, 'Trust Management in Decentralized IoT Access Control System', in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Toronto, ON, Canada, May 2020, pp. 1–9. doi: 10.1109/ICBC48266.2020.9169481.

[9] D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, 'A Decentralized Blockchain-Based Trust Management Protocol for the Internet of Things', *IEEE Trans. Dependable and Secure Comput.*, pp. 1–1, 2020, doi: 10.1109/TDSC.2020.3003232.

[10] A. A. Battah, Y. Iraqi, and E. Damiani, 'A Trust and Reputation System for IoT Service Interactions', *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 2987–3005, Sep. 2022, doi: 10.1109/TNSM.2022.3179875.

پاورقی‌ها:

[1] Internet of Things

[2] Self Promotion Attack

[3] Bad Mouthing Attack

[4] Ballot Stuffing Attack

[5] On-Off Attack
[6] Bad-Mouthing Attack
[7] Ballot-Stuffing Attack
[8] On-Off Attack
[9] Fog
[10] Service Provider
[11] Service Requester
[12] Practical Byzantine Fault Tolerance
[13] Proof of Stack
[14] Byzantine Faults
[15] Self Promotion Attack