الگوریتم‌های اعتماد در اینترنت اشیا: بررسی، تحلیل و ارائهٔ معیارهای ارزیابی

مریم ابراهیمی[۱]، محمد حسام تدین[۲*] و محمد صیاد حقیقی[۳]
[۱]پژوهشگاه ارتباطات و فناوری اطلاعات،
آموزشکده فنی و حرفه‌ای سما تهران، دانشگاه آزاد اسلامی، واحد تهران
[۲]پژوهشگاه ارتباطات و فناوری اطلاعات،
[۳] دانشکده مهندسی برق و کامپیوتر، دانشگاه تهران، تهران، ایران

چکیده

در فضایی که ارتباط بین انسان‌ها و اشیا و نیز اشیا با یکدیگر پیچیده است و انتظار اجرای برنامه‌های کاربردی فراوانی روی بستر شبکه می‌رود، یک رویکرد برای حرکت به سمت هوشمندی با حفظ امنیت، پیاده‌سازی سامانه‌های مدیریت اعتماد است. اعتماد همه مفاهیم امنیت، محرمانگی، حریم خصوصی و قابلیت اطمینان را تحت تأثیر قرار می‌دهد. تعداد زیاد اشیا در شبکه، قابلیت‌ها و کاربردهای متنوع، پویایی بسیار بالا و همچنین حضور اشیای مخرب، مدیریت اعتماد در شبکه اینترنت اشیا را به یک چالش جدی مبدل کرده است؛ به‌طوری که راه‌کارهای قدیمی پیاده‌سازی اعتماد، در این شبکه قابل استفاده نیست. در این مقاله علاوه‌بر این‌که تحلیل جامعی روی مدل‌های محاسبه مستقیم، غیرمستقیم و ترکیبی اعتماد انجام می‌شود، انواع حملات و روش‌های مقابله با آن‌ها، روش‌های ارزیابی مدل‌های ارائه‌شده و تأثیر محدودیت‌های اشیا بر مدل‌های محاسبه اعتماد، بررسی می‌شود. حیطه این بررسی، دو حوزه مدیریت اعتماد و اینترنت اشیای اجتماعی است. به‌طور خلاصه، مطالعات صورت‌گرفته در این حوزه از چهار دیدگاه مرور و مقایسه می‌شوند: (۱) مدل‌های محاسبه اعتماد، (۲) راه‌کارهای مقابله با حملات اعتماد، (۳) تأثیر محدودیت‌های عناصر اینترنت اشیا و (۴) روش‌های ارزیابی الگوریتم‌های اعتماد؛ تا به این ترتیب بتوان با تحلیلی مناسب، به نقاط قوت و ضعف الگوریتم‌های موجود در مقالات مطرح پی برد و متر و معیاری برای بحث ارزیابی اعتماد در اینترنت اشیا ارائه کرد. در این راستا، روش‌های ارزیابی (متریک‌های) کمی‌ای ارایه می‌شود که هدف آنها کشف معایب و مزایای مدل‌های تخمین اعتماد تحت شرایط مختلف است.

واژگان کلیدی: اعتماد، اینترنت اشیا، اینترنت اشیای اجتماعی، ارزیابی اعتماد

Trust Management in Internet of Things: Review, Analysis and Establishment of Evaluation Criteria

Maryam Ebrahimi[1], Mohammad Hesam Tadayon*[2] & Mohammad Sayad Haghighi[3]
[1]Iran Telecommunication Research Center, Iran,
Sama Technical and Vocational Training College, Islamic Azad University, Iran.
[2] Iran Telecommunication Research Center, Iran
[3]School of Electrical and Computer Engineering, University of Tehran, Iran

Abstract

In the complex Internet of Things (IoT) paradigm that things interact with each other as well as with human beings, one approach is to implement trust management systems in order to provide security for smart network applications. Trust, in general, overlaps with concepts such as privacy, security, and reliability. However, the high number of objects in IoT, along with its dynamic nature and existence of malicious entities, make IoT trust management quite challenging. These attributes rule out the possibility of using traditional best practices for IoT networks. Trust management algorithms have been implemented for a variety of applications in IoT environments. These algorithms are usually utilized to enhance the quality of received services in the presence of malicious entities. Such algorithms and methods have been proposed to secure IoT networks in different contexts, including traffic routing, smart cities, vehicular ad-hoc networks, healthcare ecosystems, and object authentication. In this paper,

* Corresponding author
*نویسندهٔ عهده‌دار مکاتبات

• تاریخ ارسال مقاله: ۱۳۹۸/۱۲/۲۰ • تاریخ پذیرش: ۱۳۹۹/۱۲/۱۸ • تاریخ انتشار: ۱۴۰۰/۰۷/۱۷ • نوع مطالعه: پژوهشی

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

first, different state of the art trust computation methods are numerically evaluated to estimate trust in a common testbed. Finding the best approach to assign a precise value to the trust level of an object is a crucial matter. Therefore, the principal parameters that make trust computation methods different are extracted and then, the existing trust calculation approaches built upon them are categorized. Type of relationship, direct trust, indirect trust, combination of trust values, trust updating process, data storage, and social relationships are considered as the parameters to analyze trust computation models with. Type of relationship between trustor and trustee can be different. Either of them can be object or human. Moreover, trust is usually a combination of direct experiences and recommenders' feedback. There are different update methods too. Trust estimation can be updated after each transaction, a definite time interval, or both of them. Depending on the storage and accessibility of data, algorithms can be built to be centralized, decentralized or semi-centralized. Moreover, social parameters can be involved in trust assessment, which is the subject of trust management in Social IoT. After analyzing each of these parameters' effect on trust assessment, in the next part of the article, trust-related attacks are studied. Every method that can make trust management models resistant to attacks is explained. We introduce relevant attacks and their countermeasures in direct, indirect, and hybrid trust calculation algorithms. More importantly, we study the methods of trust model evaluation and the effect of limited resources on the performance of trust calculation algorithms. In short, we conduct a comparative survey in which trust-related IoT works are studied from four perspectives: (1) Trust calculation principles, (2) Attack resistance, (3) The effect of resource limitation on model performance, and (4) Trust management evaluation framework. Through this, we find the advantages and disadvantages of existing algorithms and make a measure for the evaluation of IoT trust management systems. We provide comparative tables to show the differences between IoT trust models. A major contribution of this paper is establishing quantitative metrics to assess trust estimation models and reveal their strengths and weaknesses under different conditions.

Keywords: Trust, Internet of Things, Social Internet of Things, Trust Evaluation.

۱- مقدمه

اینترنت اشیا را می‌توان ارتباط بین حس‌گرها و محرک‌ها با هدف به اشتراک‌گذاشتن اطلاعات در چارچوب متحد تعریف کرد؛ به‌طوری‌که عملکرد مشترکی را برای ایجاد کاربردهای خلاقانه فراهم کنند [1]. اینترنت اشیا، شبکه‌ای سراسری با قابلیت خودپیکربندی براساس استانداردها و پروتکل‌های سازگار با ارتباطات است؛ به‌طوری‌که اشیای فیزیکی و مجازی دارای هویت، با استفاده از واسطه‌های هوشمند به‌صورت یک‌پارچه به شبکه اطلاعات متصل می‌شوند [2]. اشیا همان عناصر فعال در حوزه‌های تجارت، اطلاعات و فرآیندهای اجتماعی هستند که قادر به ایجاد تعامل و برقراری ارتباط بین خودشان و محیط از طریق تبادل اطلاعات و داده‌های حس شده هستند؛ به‌طوری‌که به رخدادهای دنیای واقعی واکنش نشان داده و با راه‌اندازی فرآیندها و ایجاد خدمات به همراه یا بدون دخالت انسان‌ها جهان فیزیکی را تحت تأثیر قرار می‌دهند [3]. یکی از مهم‌ترین بخش‌های ارائه خدمات در اینترنت اشیا نحوه مدیریت اعتماد است؛ چون کلیه اطلاعات جمع‌آوری‌شده از رأس ارائه‌دهنده خدمت باید تجزیه و تحلیل شوند تا تصمیمی درخصوص قابل اعتمادبودن آن گرفته شود. وقتی رأسی به شبکه اضافه می‌شود و درخواست خدمت دارد یا حتی خودش ارائه‌دهنده خدمت است، لازم است تصمیمی مبنی بر میزان قابلیت اعتماد به آن گرفته شود. این احتمال وجود دارد که این رأس مخرب باشد و موجب آسیب‌رسانی به سامانه شود و از طرفی این احتمال وجود دارد که این رأس مخرب نیست و قادر به انجام وظایفی است که بر عهده‌اش گذاشته می‌شود. اعتماد در برقراری ارتباط بین عناصر در شبکه اینترنت اشیا نقش مهمی ایفا می‌کند، چون کلید اصلی در شکل‌گرفتن تراکنش‌های موفق بین عناصر شبکه ارزیابی و مدیریت صحیح اعتماد است. مقالات مروری متعددی با عناوین مشابه و با هدف بررسی روش‌های پیاده‌سازی اعتماد در اینترنت اشیا ارائه شده است، به‌عنوان نمونه؛ مقاله [4] دیدگاه‌های موجود در اعتماد به نرم‌افزار، سخت‌افزار، دستگاه‌ها و خدمات در اینترنت اشیا را بررسی کرده است. در [5]، ابتدا رویکردهای سامانهٔ اعتماد و شهرت بیان شده و سپس در این زمینه که اگر این سامانه‌ها در اینترنت اشیا مورد استفاده قرار گیرند، تحلیل صورت می‌گیرد. در مقاله [6]، خواص اعتماد مورد بررسی قرار می‌گیرد، اهداف مدیریت اعتماد در اینترنت اشیا ارائه می‌شود و سپس در مورد پیشرفت‌های فعلی به سمت اینترنت اشیا قابل اعتماد توضیحاتی بیان شده است. در مقاله [7]، چالش‌های اصلی امنیت در اینترنت اشیا و راه‌حل‌های موجود ارائه شده و سپس مسائل حل‌نشده شناسایی شده است. مقاله [8]، علاوه‌بر بررسی اعتماد در حوزه اینترنت اشیا، برخی از چالش‌های پژوهشی با موضوع

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

اعتماد در اینترنت اشیا را نیز توصیف کرده است. تعدادی از مقالات مروری نیز پیشینه پژوهش‌های صورت گرفته در محاسبه اعتماد را بر روی وجه خاصی نظیر وابستگی اعتماد به روابط اجتماعی [9] و وابستگی اعتماد به موضوع [10] در اینترنت اشیا بررسی کرده‌اند. مقاله [11] نیز علاوه‌براین‌که پژوهش‌های چاپ‌شده در حوزه اینترنت اشیا را بررسی کرده، مقالات را از منظر تفاوت در پارامترهای محاسبه اعتماد دسته‌بندی کرده است. آنچه این مقاله را با سایر مقالات مشابه متفاوت نکرده، آن است که علاوه‌بر مقایسه طبقه‌بندی‌شده از پژوهش‌های موجود، ارزیابی کمی به همراه شبیه‌سازی مقایسه‌ای از دو مقاله را ارائه کرده است؛ به‌طوری که این دسته‌بندی و مقایسه در هیچ یک از ادبیات مروری مشاهده نمی‌شود. در این مقاله اقدامات انجام‌شده در حوزه مدیریت اعتماد در اینترنت اشیا از چهار جنبه مورد تحلیل و ارزیابی و مقایسه قرار گرفته‌اند. در ادامه و در بخش دوم، مفهوم اعتماد ارائه و سپس در بخش سوم از مقاله، پارامترهای محاسبه اعتماد در اینترنت اشیا معرفی شده‌اند. در بخش چهارم نیز، مدل‌های محاسبه اعتماد مستقیم و در بخش پنجم، مدل‌های محاسبه اعتماد غیرمستقیم ارائه و در بخش ششم نحوه ترکیب اعتماد مستقیم و غیرمستقیم بیان شده است. در ادامه و در بخش هفتم از مقاله به تحلیل مدل‌های اعتماد از منظر حملات پرداخته شده است. در بخش هشتم به مقالاتی که محدودیت‌های اشیا را مدنظر قرار داده‌اند، اشاره و در بخش نهم علاوه‌بر طرح روش‌های ارزیابی اعتماد، معیارهای عددی با هدف مقایسه الگوریتم‌های محاسبه اعتماد ارائه و سپس دو مقاله شناخته‌شده در این حوزه شبیه‌سازی شده و نتایج حاصل مورد بررسی قرار گرفته است. بخش انتهایی نیز نتیجه‌گیری و پیشنهادها را شامل می‌شود؛ به‌علاوه مقایسه کلیه موارد بیان‌شده با استفاده از جداول، امکان دسترسی سریع و خلاصه به ایده‌ها و مقایسه آن‌ها را فراهم کرده است.

۲- مدیریت اعتماد در اینترنت اشیا

اندازه‌گیری و پیش‌بینی قابلیت اعتماد همواره مشکل و محدود است و این به‌دلیل طبیعت فازی، پویایی و پیچیدگی اعتماد است. مفهوم فازی به معنی ناشناخته، مبهم و غیرقابل اندازه‌گیری‌بودن است؛ به‌طوری‌که وقتی می‌خواهیم اعتماد را تعریف و یا سطوح مختلف آن را توصیف کنیم به معیار صریحی دسترسی نداریم. پویایی اعتماد به معنی تغییر آن در طول زمان است و طبیعت پیچیده اعتماد از این حقیقت سرچشمه می‌گیرد که روش‌ها و بینش‌های متنوع و زیادی برای معین‌کردن آن وجود دارد. وقتی نتوان مفهومی را به‌صراحت تعریف کرد، پایدار نباشد یا همیشه تغییر کند و با بینش و نظرات متنوعی همراه شود، مدیریت و پیش‌بینی مقادیر آینده آن همیشه سخت و به همین دلیل است که اعتماد طبیعت پیچیده‌ای دارد. براساس مرجع [12]، اعتماد شش ویژگی اصلی دارد که بر فازی و پویایی‌بودن آن دلالت دارد و این ویژگی‌ها **ضمنی‌بودن**[1]، **نامتقارن‌بودن**[2]، **انتقال‌پذیری**[3]، **تضاد**[4]، **ناهم‌زمانی**[5] **و جاذبه**[6] است. در سال‌های اخیر استفاده از خدمات مبتنی بر اینترنت افزایش یافته است و انتظار می‌رود که این روند ادامه داشته باشد. بدون وجود مدیریت اعتماد، سامانه‌ها هرگز قادر به تصمیم‌گیری برای برقراری ارتباط به شکل مناسبی نخواهند بود؛ به‌طوری‌که در بدترین حالت هیچ ارتباطی برقرار نخواهد شد یا برقراری ارتباط همواره امکان‌پذیر است و هر دو این موارد می‌تواند فاجعه‌بار و با اثر معکوس باشد. در اینترنت اشیا ضروری است بدانیم به چه کسی باید اعتماد و به چه کسی نباید اعتماد کنیم. بنابراین، مدیریت اعتماد رویکردی یک‌پارچه به‌منظور تعیین و تبیین سیاست‌های امنیتی، اعتبارسنجی‌ها و ارتباطاتی است که اجازه اختیار مستقیم اقدامات حیاتی-امنیتی را صادر می‌کند [13]. همچنین، مدیریت اعتماد مجموعه‌ای از فعالیت‌ها شامل ابداع سامانه‌ها و روش‌هایی است که امکان ارزیابی میزان اعتماد به تراکنش‌های بالقوه همراه با برآورد مخاطرات را به کاربران می‌دهد و به‌علاوه این موقعیت را برای صاحبان سامانه‌ها فراهم می‌کند تا قابلیت اطمینان حال حاضر دستگاه‌های خود را به نمایش بگذارند و یا بهبود بخشند [14]. در شبکه اینترنت اشیا مبتنی بر خدمت[7]، تعدادی ارائه‌دهنده خدمت متناسب با نیاز متقاضی پیشنهاد می‌شوند و سپس گیرنده خدمت با استفاده از روش‌های محاسبه اعتماد، قابل اطمینان‌ترین خدمت‌دهنده را انتخاب می‌کند. از طرف دیگر، تعدادی کاربر و به‌دنبال آن‌ها اشیای بدرفتار و مخرب در شبکه وجود دارند که با اقدامات مخرب و ایجاد حملاتی نظیر خوب‌جلوه‌دادن خود و یا کاهش محبوبیت و شهرت دیگران عملکرد شبکه را

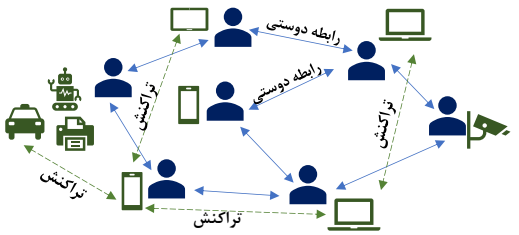
[1] Implicitness
[2] Asymmetry
[3] Transitiveness
[4] Antonymy
[5] Asynchrony
[6] Gravity
[7] service oriented architecture (SOA)

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

مختل می‌سازند. به این ترتیب رئوس مخرب به‌تنهایی و یا تبانی، ارائه خدمت در شبکه را با مشکل مواجه می‌سازند. از آنجایی که اینترنت اشیا شبکه‌ای بسیار بزرگ با انواع و اقسام عناصر است، بزرگ‌ترین سؤال در برقراری ارتباط بین اشیا، ارزیابی میزان اعتمادی است که به یکدیگر دارند. اینترنت اشیا با بسیاری از مسائل امنیتی مانند احراز هویت، مدیریت کلید [15]، شناسایی، دردسترس‌بودن، حفظ حریم خصوصی و مدیریت اعتماد روبه‌رو است. درواقع، ایجاد روابط اعتماد بین گره‌ها در اینترنت اشیا نشان‌دهنده یک نقطه عطف امنیتی برای داشتن سامانه‌های قابل اعتماد است که گره‌های مخرب را حذف می‌کند؛ درواقع در حوزه اینترنت اشیا مفاهیمی شامل امنیت، محرمانگی و قابلیت اطمینان به شکل اعتماد جلوه می‌کند؛ به طوری که اعتماد به یک شیء در اینترنت اشیا به معنی رفتار قابل انتظار از یک شیء در قالب گرفتن خدمت از آن است.

۲-۱- تراکنش قابل اعتماد

درکل هدف از پیاده‌سازی الگوریتم‌های مدیریت اعتماد در شبکه اینترنت اشیا بالابردن کیفیت خدمت و مقابله با حملات احتمالی است. برای نمونه نویسندگان در [16] مدل مدیریت اعتماد مبتنی بر شهرت را برای شبکه‌های حس‌گر بی‌سیم[1] با هدف ایجاد ارتباط امن بین اجزای شبکه ارائه کرده‌اند. نویسندگان در [17]، [18]، [19] و [20] با پیاده‌سازی الگوریتم‌های مدیریت اعتماد در شبکه اینترنت اشیا و در مقالات [21]، [22]، [23]،[24] و [25] در شبکه اینترنت اشیای اجتماعی به‌دنبال برقراری تراکنش امن هستند تا علاوه‌بر مقابله با رئوس مخرب کارایی بیشینه شود. شکل (۱) عناصر شبکه اینترنت اشیا و ارتباط بین آن‌ها را نشان می‌دهد.



(شکل-۱): اشیا و صاحبان آنها در شبکه اینترنت اشیا
(Figure-1): Objects and their owners in the IoT network

۲-۲- مسیریابی امن

نویسندگان در [26] و [27] با استفاده از سازوکارهای مدیریت اعتماد مسیریابی امن را در شبکه اینترنت اشیا ایجاد کرده‌اند. نویسندگان در [28]، [29]، [30]، [31]، [32]، [33]، [34] و [35] با استفاده از الگوریتم‌ها اعتماد، مسیریابی امن در شبکه‌های حس‌گر بی‌سیم را بهبود بخشیده‌اند. الگوریتم‌های مدیریت اعتماد با هدف مسیریابی امن در شبکه‌های هوشمند برق[2] در مقاله [36] و در شبکه‌های موردی متحرک[3] در [37] و [38] پیاده‌سازی شده‌اند.

۲-۳- شهر هوشمند

نویسندگان در [39] ایده سنجش اعتماد با نام RealAlert را در شبکه اینترنت اشیا ارائه کرده‌اند؛ به‌طوری‌که میزان اعتماد به رئوس شبکه و داده را در شهرهای هوشمند تخمین می‌زنند. نویسندگان در [40] یک مدل مدیریت اعتماد برای شهرهای هوشمند با هدف ارائه خدمات در محاسبات لبه پیشنهاد داده‌اند. برای ممانعت از شکستن حریم خصوصی، هدف اصلی از ارائه این مدل بهبود کارآیی واحدهای محاسبه لبه[4] است، به طوری که میزان استفاده از منابع و توان مصرفی واحدهای محاسبه لبه به‌عنوان معیارهای سنجش عملکرد این واحدها در نظر گرفته شده‌اند. هدف اصلی در [41]، انتخاب قابل اعتمادترین ابزار در سامانهٔ تشخیص کیفیت هوا است. این مدل متمرکز با ارائه خدمت اعتماد به‌عنوان خدمت[5]، تجربیات و مشاهدات مرتبط با اعتماد را ترکیب کرده تا قابل اعتمادترین خدمت تشخیص کیفیت هوا انتخاب شود. مدل ارائه‌شده در [42]، اعتبار داده‌های عددی استخراج‌شده را از حس‌گرهای دما در یک شهر هوشمند با استفاده از الگوریتم مدیریت اعتماد می‌سنجد. در این مدل از خروجی‌های حس‌گرها به‌عنوان داده‌های ورودی دو مدل یادگیری ماشین استفاده و سپس با استفاده از خروجی‌های طبقه‌بندی‌شده این دو مدل، توابع جرم و اعتماد مطابق با قوانین تئوری شواهد Dempster-Shafer استخراج و ترکیب می‌شوند.

۲-۴- شبکه اقتضایی خودرویی[6]

مطابق با [43] در صورت وقوع تصادف جاده‌ای، پیام‌های اضطراری به‌وسیله قابل اعتمادترین وسایل نقلیه به سایرین اطلاع داده می‌شود. بر اساس این مدل، انتشار پیام اضطراری مبتنی بر اعتماد زنجیره‌ای است؛ به‌طوری که مدل در برابر حملات مقاوم و با ساختار شبکه اقتضایی وسایل نقلیه نیز سازگار است. ارزیابی اعتماد در [44]،

[1] Wireless Sensor Networks (WSNs)
[2] Smart Grid Networks
[3] Mobile Ad-hoc Networks
[4] Edge Computing Units (ECU)
[5] Trust as a Service
[6] Vehicular Ad-hoc Network (VANET)

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

مبتنی بر پیشنهاد است که با هدف محاسبه اعتماد وسایل نقلیه و هر عنصر در سامانه حمل و نقل ارائه شده است. در این مدل غیرمتمرکز که اعتماد ترکیبی از اعتماد مستقیم و غیرمستقیم است، اعتماد غیرمستقیم جمع وزن‌دار پیشنهاددهندگانی است که به روش خوشه‌بندی به دو دسته مثبت و منفی، تقسیم شده‌اند. مدل ارائه‌شده در [45]، بر اساس ویژگی‌های ناپایدار شبکه‌های اقتصایی خودرویی با آگاهی از موضوع، اعتماد را تخمین می‌زند. اعتماد با استفاده از آنتروپی اطلاعات و یادگیری تقویتی[1] محاسبه می‌شود تا وسیله نقلیه توانایی انتخاب بهترین تصمیم را داشته باشند. نویسندگان در [46]، مدل مدیریت اعتماد برای شبکه‌های اقتصایی خودرویی را ارائه کرده‌اند که در برابر حمله man-in-the-middle مقاوم است. اعتماد نسبت به یک وسیله نقلیه ترکیبی از اعتماد بین خودرویی و میزان اعتماد مبتنی بر زیرساخت است که توسط واحدهای مستقر در امتداد جاده محاسبه می‌شود.

۲-۵- اکوسیستم سلامت مبتنی بر اینترنت اشیا

با توجه به اهمیت امنیت در ابزارهای سلامت اینترنت اشیای نویسندگان در مقالات [47] و [48] با مطالعه پژوهش‌های ارائه‌شده، سازوکارهای پیاده‌سازی امنیت در اینترنت ابزارهای سلامت را طبقه‌بندی و بررسی کرده‌اند. نویسندگان سازوکارهای پیاده‌سازی امنیت را در اینترنت ابزارهای سلامت از نگاه روش‌های رمزنگاری، توزیع و مدیریت کلید، مدیریت هویت دیجیتال، مدیریت نگهداشت چرخه حیات سامانه و مسیریابی امن مورد تحلیل و بررسی قرار داده‌اند. نویسندگان در [49] با استفاده از یک مدل مدیریت اعتماد در اینترنت اشیا کارآیی اکوسیستم‌های سلامت در اینترنت اشیا را بهبود بخشیده‌اند. پروتکل مدیریت اعتماد متمرکز ارائه‌شده در [50] به کاربران اینترنت اشیا در حوزه سلامت کمک می‌کند تا در صورت نیاز به مراکز درمانی، بهترین انتخاب را داشته باشند. در این مدل با سه پارامتر طبقه‌بندی ریسک، قابلیت اطمینان و احتمال ازدست‌رفتن سلامتی، سطح اعتماد به سامانهٔ سلامت ارائه‌شده در شبکه اینترنت اشیا ارزیابی می‌شود.

۲-۶- احراز هویت اشیا

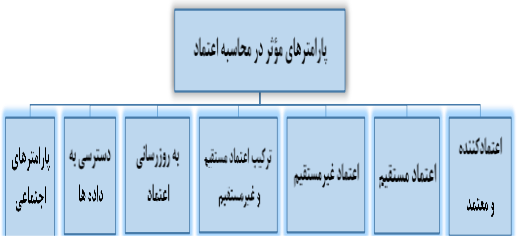
حباب اعتماد[2] عنوان یک رویکرد جدید در مدیریت اعتماد مبتنی بر زنجیره بلوکی[3] است که در مقاله [51] ارائه شده است. در این مدل عناصر شبکه اینترنت اشیا تراکنش‌های قابل اعتماد را در نواحی مجازی ایمن که حباب نام‌گذاری شده، با شناسایی و احراز هویت با قابلیت اطمینان بالا برقرار می‌کنند. چارچوب صدور مجوز مبتنی بر رفتار و آگاه از موضوع برای اینترنت اشیای خانگی نیز در [52] ارائه شده است. نویسندگان در [53] علاوه‌بر اینکه پروتکل‌های احراز اصالت در اینترنت اشیا را معرفی کرده‌اند، با هدف ارائه یک مدل جدید محدودیت‌ها و آسیب‌پذیری‌های امنیتی آن‌ها را بررسی می‌کنند. پروتکل ارائه‌شده علاوه‌بر سبک‌بودن از قابلیت گمنامی و اعتماد استفاده کرده و در برابر حملاتی مانند جعل هویت، تکرار و مرد میانی مقاوم است.

۲-۷- مدیریت اعتماد مبتنی بر زنجیره بلوکی

هدف اصلی در [54] تأمین سطح قابل قبولی از امنیت با تلفیق فناوری زنجیره بلوکی و فناوری شبکه لورا[4] در اینترنت اشیا است. نویسندگان در [55] نیز یک راه حل امنیتی مبتنی بر زنجیره بلوکی برای اینترنت اشیای توزیع‌شده پیشنهاد می‌دهند. نویسندگان در [56] برای اطمینان از عملکرد داده‌های کلان اینترنت اشیا، مدل مدیریت اعتماد غیرمتمرکز را بر اساس قرارداد هوشمند زنجیره بلوکی پیشنهاد می‌کنند. مدل پیشنهادی غیرمتمرکز در [57] از فناوری زنجیره بلوکی برای اطمینان از اشتراک قابل اعتماد منابع، بین ارائه‌دهندگان خدمات و مصرف‌کنندگان استفاده می‌کند.

۳-پارامترهای مؤثر در محاسبه اعتماد

پارامترهای محاسبه اعتماد در اینترنت اشیا که با هدف تخمین مقدار عددی اعتماد ارائه شده‌اند، در شکل (۲) نشان داده شده است که در ادامه به‌تفضیل مورد بحث و بررسی قرار خواهند گرفت.



(شکل-۲): پارامترهای مؤثر در محاسبه اعتماد در اینترنت اشیا

(Figure-2): Effective parameters in trust computing

[1] Reinforcement learning
[2] Bubbles of Trusts
[3] Blockchain
[4] LoRaWAN

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

۳-۱- اعتمادکننده و معتمد

نخستین قدم در محاسبه اعتماد، تعیین ماهیت اعتمادکننده و معتمد است. در شبکه اینترنت اشیا اعتمادکننده و معتمد عناصر شبکه اینترنت اشیا هستند که از یک برچسب RFID تا یک گوشی هوشمند را شامل می‌شوند. در شبکه اینترنت اشیای اجتماعی نیز انسان‌ها به‌عنوان کاربران این ابزارها می‌توانند در نقش اعتمادکننده ظاهر شوند. مطابق با جدول (۱)، اعتمادکننده در مقالات [17]، [18]، [21]، [22]، [23]، [24]، [25]، [37] و [58] شیء؛ و در [19]، [20] و [49] صاحبان اشیا یا انسان‌ها هستند. معتمد در کلیه مقالات به استثنای [49] که برنامه‌های تلفن همراه در نظر گرفته شده، در همه مدل‌ها اشیا فرض شده است.

۳-۲- اعتماد مستقیم

اعتماد مستقیم در نتیجه تعامل و تراکنش مستقیم با سایر اشیا در طول زمان به‌دست می‌آید؛ به این ترتیب اعتماد مستقیم به دو متغیر اصلی بازخورد و زمان وابسته است. آنچه مقالات مختلف را در محاسبه اعتماد مستقیم از یکدیگر متمایز می‌کند، نحوه استفاده از این دو مؤلفه به‌همراه سایر پارامترهای اینترنت اشیا است. در بخش ۴ از مقاله به مدل‌های محاسبه اعتماد مستقیم اشاره خواهد شد.

۳-۳- اعتماد غیرمستقیم

شبکه اینترنت اشیا شبکه‌ای بسیار بزرگ و اطلاعات مورد نیاز برای محاسبه اعتماد نه‌تنها به تجربیات مستقیم بلکه به پرسش از دیگران نیز وابسته است. به این ترتیب اعتماد به یک شیء ترکیبی از تجارب حاصل از تراکنش مستقیم و نیز پرسش از دیگران است. در بخش ۵ مدل‌های محاسبه اعتماد غیرمستقیم بیان خواهد شد.

۳-۴- ترکیب اعتماد مستقیم و غیرمستقیم

شیء نیازمند به خدمت در شبکه اینترنت اشیا، پس از محاسبه اعتماد مستقیم و غیرمستقیم و سپس ترکیب آن‌ها قادر به ارزیابی سطح اعتماد ارائه‌دهنده خدمت خواهد بود. بخش ۶ از مقاله به بررسی روش‌های ترکیب اعتماد مستقیم و غیرمستقیم اختصاص یافته است.

۳-۵- به روزرسانی اعتماد

به‌روزرسانی اعتماد می‌تواند بعد از انجام هر تراکنش [17]، [18]، [20]، [21]، [22]، [23]، [25]، [49] و [58] در بازه‌های زمانی خاص [37] و یا در هر دو مورد [19] و [24] صورت گیرد.

۳-۶- دسترسی به داده‌ها

الگوریتم مدیریت اعتماد با توجه به نحوه دسترسی به اطلاعات می‌تواند به صورت متمرکز[1] [18]، [20] و [49]؛ غیرمتمرکز[2] [17]، [19]، [21]، [22]، [23]، [24]، [25] و [37] و یا حتی نیمه متمرکز[3] [23] و [58] طراحی شود.

۳-۷- اینترنت اشیای اجتماعی[4]

اگر پارامترهای اجتماعی در محاسبات اعتماد وارد شوند، [17]، [19]، [20]، [21]، [22]، [23]، [24]، [25] و [58] شبکه اینترنت اشیای اجتماعی خواهیم داشت.

۴- تحلیل مدل‌های محاسبه اعتماد مستقیم

۴-۱- فاکتورهای اصلی در محاسبه اعتماد مستقیم

۴-۱-۱- بازخورد[5]

گیرنده خدمت می‌تواند میزان رضایت‌مندی خود از خدمت‌دهنده را در قالب بازخورد نشان دهد.

- بازخورد منطقی: گیرنده خدمت میزان رضایت و عدم رضایت خود را از ارائه‌دهنده به‌صورت یک و صفر اعلام می‌کند.
- بازخورد فازی: گیرنده خدمت میزان رضایت و عدم رضایت خود را در قالب اعدادی بین صفر و یک اعلام می‌کند. در این حالت مقادیر بین صفر و یک میزان رضایت‌مندی را در سطوح مختلف نشان می‌دهند.

۴-۱-۲- زمان

اعتماد تابعی از زمان است؛ به‌طوری که نتایج تراکنش‌های اخیر نسبت به تراکنش‌های قدیمی‌تر اهمیت بیشتری دارند و به عبارت دیگر اطلاعات جدیدتر مهم‌تر هستند. اگر $O = \{o_0\ o_1\ o_2\ \dots\ o_l\}$ دنباله‌ای از مشاهدات باشد و o_i میزان رضایت‌مندی خدمت‌گیرنده را در زمان i نشان دهد، آن‌گاه با استفاده از روش‌های هموارسازی نمایی[6]

[1] Centeralized
[2] Decentralized
[3] Semicentralized
[4] Social Internet of Things (SIoT)
[5] Feedback
[6] Exponential smoothing Methods

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

می‌توان مشاهدات را به‌صورتی ترکیب کرد که مشاهدات اخیر وزن بیشتری داشته باشند. رابطه (۱) نحوه ترکیب بازخوردها را به روش هموارسازی نمایی نشان می‌دهد. با استفاده از رابطه (۱) و دنباله مشاهدات، می‌توان مقادیر عددی رضایتمندی و عدم رضایت را با گذشت زمان ترکیب و محاسبه کرد.

$$= \sum_{i=0}^{l} r^{l-i}\ \delta_i(X),\ \delta_i(X) = \begin{cases} 1 & \text{اگر } o_i = X \\ 0 & \text{در غیر اینصورت} \end{cases} \qquad (۱)$$

در رابطه (۱)، r فاکتور تضعیف زمان[1] است و با توجه به مدل محاسبه اعتماد، بهینه می‌شود.

۲-۴- مدل‌های ارائه‌شده محاسبه اعتماد مستقیم

۱-۲-۴- جمع وزن‌دار ایستا

در این روش، اعتماد مستقیم ترکیب خطی از پارامترهای مؤثر بر مقدار اعتماد است. این پارامترها متغیرهای محاسبه اعتماد مستقیم در شبکه اینترنت اشیا و شبکه اینترنت اشیای اجتماعی را شامل می‌شوند. ضرایب پارامترها در این روش اعداد ثابتی هستند که با توجه به مدل بهینه می‌شوند. اگر قابلیت اعتماد مستقیم به شیء **j**، ارزیابی‌شده به‌وسیلهٔ شیء i با T_{ij} نشان داده شود رابطه (۲) نحوه محاسبه اعتماد مستقیم به روش جمع وزن‌دار ایستا را نشان می‌دهد.

$$T_{ij} = \sum_{i=1}^{n} \alpha_i\ P_i \qquad (۲)$$

در این رابطه باید $\sum_i \alpha_i = 1$ شود تا T_{ij} همواره بین صفر و یک بماند.

مقاله [21]، اعتماد مستقیم را با استفاده از پارامترهایی که دربرگیرنده ویژگی‌های شبکه اینترنت اشیای اجتماعی هستند و با روش **جمع وزن‌دار ایستا** به‌صورت عددی بیان کرده است. (رابطه ۳)

$$O_{ij}^{dir} = \begin{cases} F_{ij} & \text{if } N_{ij} = 0 \\ \left(\frac{\log(N_{ij}+1)}{1+\log(N_{ij}+1)}\right)\left(\epsilon O_{ij}^{lon} + \chi O_{ij}^{rec}\right) + \left(\frac{1}{1+\log(N_{ij}+1)}\right)F_{ij} & \text{if } N_{ij} > 0 \end{cases} \qquad (۳)$$

در رابطه (۳)، i گیرنده خدمت و j خدمت‌دهنده هستند و $\chi + \epsilon = 1$ است تا O_{ij}^{dir} یا همان اعتماد مستقیم همواره بین صفر و یک بماند. در این مدل، پارامترهای ارزیابی اعتماد مستقیم عبارتند از:

- N_{ij}: تعداد کل تراکنش‌ها
- O_{ij}^{lon}: نظر مستقیم در بازه زمانی طولانی
- O_{ij}^{rec}: نظر مستقیم در بازه زمانی کوتاه‌مدت

نظرات طولانی‌مدت و کوتاه‌مدت بازخوردهای وزن‌دار نرمال‌شده هستند و برای هر بازخورد با این هدف که رئوس، قابلیت اعتمادشان را بر تراکنش‌های ضعیف بنا نکنند، وزن در نظر گرفته شده است.

- F_{ij}: فاکتور رابطه[2]، مقداری بین صفر و یک است که بر اساس نوع رابطه بین اشیا مقداردهی می‌شود. براساس مدل ارائه‌شده مجموعه‌ای از انواع ارتباطات اجتماعی بین اشیا برقرار است و ارتباطات اجتماعی بین اشیا با پارامترهای زیر سنجیده می‌شود:
  - ارتباط خانوادگی اشیا[3]: اشیای مشابهی که در یک بازه زمانی و به‌وسیلهٔ یک کارخانه تولید می‌شوند.
  - رابطه هم‌مکانی[4] و همکاری[5] اشیا: ارتباطی همانند انسان‌ها وقتی منافع شخصی نظیر محل زندگی خود را به اشتراک می‌گذارند و یا در حالتی که منافع عمومی مانند محیط کار خود را به اشتراک می‌گذارند.
  - ارتباط اشیا از طریق مالکیت[6]: اشیا با صاحبان یکسان.
  - ارتباط اجتماعی اشیا[7]: ارتباطی است که اشیا به‌واسطه صاحبانشان به هم مرتبط هستند.

به این ترتیب مطابق با رابطه (۳)، اگر دو شیء تراکنش نداشته باشند، اعتماد مستقیم همان مقدار عددی فاکتور رابطه است و در صورت داشتن تراکنش مستقیم، اعتماد از **جمع وزن‌دار ایستای** نظرات مستقیم و فاکتور رابطه حاصل می‌شود.

اعتماد مستقیم در مقالات [17] و [24] در قالب ویژگی سه‌گانه صداقت، همکاری و عضویت در انجمن علاقمندی تعریف شده است. در لحظه t مقدار اعتماد i نسبت به j با توجه به رابطه (۴) و از **جمع وزن‌دار ایستای** اعتماد مستقیم ($D_{ij}^{X}(t)$) و آخرین مقدار اعتماد در زمان $(t-\Delta t)$ به‌دست می‌آید و ضریب ایستای α همان فاکتور تضعیف، به‌منظور اعمال تأثیر گذشت زمان است.

$$T_{ij}^{X}(t) = (1-\alpha)T_{ij}^{X}(t-\Delta t) + \alpha D_{ij}^{X}(t) \qquad (۴)$$

X در رابطه (۴) متریک‌های صداقت، همکاری و علاقمندی به انجمن هستند و Δt فاصله زمانی بعد از آخرین تراکنش است.

[1] Decay Fator

[2] Relationship Factor
[3] Parental Object Relationship
[4] Co-location Object Relationship
[5] Co-work Object Relationship
[6] Ownership Object Relationship
[7] Social Object Relationship

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

- صداقت ($D_{ij}^{honesty}$): ویژگی صداقت با شمارش تجارب تقلبی در بازه زمانی Δt و از رابطه $1 - \frac{\text{تعداد تجربه‌های مشکوک}}{\text{مقدار آستانه}}$ حاصل می‌شود.
- همکاری ($D_{ij}^{cooperativeness}$): ویژگی همکاری به معنای رابطه دوستی اجتماعی بین صاحبان اشیا است و مقدار عددی آن با تقسیم تعداد دوستان مشترک بر کل دوستان به‌دست می‌آید.
- علاقمندی‌های مشترک ($D_{ij}^{community-interest}$): ویژگی علاقمندی‌های مشترک یا ظرفیت‌های یکسان نشان می‌دهد که اعتمادکننده و معتمد در چه تعداد انجمن‌های یکسانی عضو و از تقسیم تعداد انجمن‌هایی که هر دو رأس در آن‌ها عضو هستند بر مجموع تعداد انجمن‌هایی که دو رأس i و j به‌تنهایی در آن‌ها عضو هستند، به‌دست می‌آید.

مقاله [22] نشان می‌دهد با وجود این‌که گره‌ها نمی‌دانند به کدام انجمن علاقه‌مندی تعلق دارند، برآورد اعتماد رئوس به سمت توافق انجمن[1] هم‌گرا می‌شود. براساس پروتکل اعتماد ارائه‌شده در این مقاله، هر رأس اعتماد مستقیم را براساس سه ویژگی صداقت، مشارکت و انجمن علاقه‌مندی همانند مقاله [59] و رابطه (۴) می‌سنجد. صداقت به معنای درست‌کاری رأس و مشارکت مطابق با مقاله [60] به این معنی است که معتمد از نظر اجتماعی با اعتمادکننده در ارتباط است. انجمن علاقه‌مندی به این معنی است که اعتمادکننده و معتمد متعلق به انجمن‌های اجتماعی علاقه‌مندی نظیر هم‌مکانی، هم‌کاری یا هم‌خانوادگی یکسان هستند. (تعاریف مقاله [61])

در [58] هدف، ارزیابی اعتماد بین دو شیء با درنظرگرفتن لایه اجتماعی و استفاده از شواهد مستقیم و غیرمستقیم است؛ به‌طوری که در برابر حمله تبعیض اجتماعی مقاوم باشد. هر شخص، مالک یک یا چند شیء است و هر شیء یک یا چند سرویس ارائه می‌کند؛ به‌طوری‌که هر گره ممکن است، خدمت بد یا پیشنهاد غلط بدهد. اشیا بعد از گرفتن خدمت نظرات خود را در قالب بازخوردهای مثبت و منفی ذخیره می‌کنند و اعتماد مستقیم زمینه محور با روش **جمع وزن‌دار ایستا** و با استفاده از نظرات وزن‌دار با درنظرگرفتن فاکتور کاهشی زمان محاسبه می‌شود. در این مدل وزن‌ها اعتبار یک شیء، اهمیت خدمت، سطح انرژی گیرنده خدمت، شباهت اجتماعی و فاصله اقلیدسی بین مشاهده قبلی و درخواست جدید هستند.

[1] Community of Interest Ground Truth (CoI Ground truth)

۲-۲-۴- جمع وزن‌دار پویا

در این روش، اعتماد مستقیم از همان رابطه (۲) به‌دست می‌آید با این تفاوت که ضرایب α_i به‌صورت پویا مطابق با مدل ارائه‌شده مقداردهی می‌شوند.

در مقاله [25] که هدف اصلی، ارائه مدل اعتماد اجتماعی مبتنی بر محتوا است، اعتماد مستقیم با روش **جمع وزن‌دار پویا** و از رابطه (۵) به‌دست می‌آید:

$$DT_{i,j} = \sum_{1}^{n} (DT_{i,j}^{cn} * WW_{i,j}^{cn}) \quad (۵)$$

در رابطه (۵)، $WW_{i,j}^{cn}$ وزن‌های نرمال‌شده برای نشان‌دادن میزان اهمیت محتواها است، به‌طوری که $WW_{i,j}^{cn} = \frac{W_{i,j}^{cn}}{W^{Total}}$ و $\sum WW_{i,j}^{cn} = 1$ هستند و اهمیت هر زمینه از تقسیم تعداد تراکنش‌های مستقیم i و j در زمینه c ($Tr_{i,j}^{c}$) بر تعداد کل تراکنش‌های صورت‌گرفته بین i و j در کلیه زمینه‌ها به‌دست می‌آید. (رابطه ۶)

$$W_{i,j}^{c} = \frac{Tr_{i,j}^{c}}{\sum_{1}^{k} Tr_{i,j}^{cn}} \quad (۶)$$

مقدار $DT_{i,j}^{cn}$ در رابطه (۵) (اعتماد مستقیم بین i و j در زمینه cn) نیز از رابطه (۷) به‌دست می‌آید که در آن $DT_{i,j(old)}^{cn}$، مقدار قدیمی اعتماد مستقیم بین i و j در زمینه cn و $\Delta DT_{i,j}^{cn}$، تغییر در اعتماد در زمینه cn است.

$$DT_{i,j}^{cn} = DT_{i,j(old)}^{cn} + \Delta DT_{i,j}^{cn} \quad (۷)$$

در رابطه بالا $\Delta DT_{i,j}^{cn}$، از فرمول $\Delta DT_{i,j}^{cn} = {fb_{i,j}^{cn}}/{S}$ به‌دست می‌آید که در این رابطه $fb_{i,j}^{cn}$، بازخورد i (خدمت‌گیرنده) نسبت به عملکرد j (خدمت‌دهنده) است و در محدوده [۱۰و۱۰-] قرار دارد. S نیز از رابطه $S = {fb_{max}}/{MD}$ حاصل می‌شود و منظور از fb_{max} بیشترین مقدار $fb_{i,j}^{cn}$ برای هر تراکنش یا به عبارتی ۱۰ و MD، بیشینه تغییری است که می‌تواند در مقدار اعتماد رخ دهد. به این ترتیب اعتماد مستقیم با توجه به ضرایب پویا در بازه‌های زمانی Δt به‌دست خواهد آمد.

۳-۲-۴- امید ریاضی توزیع بتا

اگر شیء گیرنده خدمت (i) پس از دریافت خدمت از شیء (j) میزان رضایت خود را با صفر یا یک نشان دهد؛ بعد از انجام تعدادی تراکنش مستقیم، مشاهدات، دنباله‌ای از صفر و یک‌ها هستند که از توزیع برنولی پیروی می‌کنند. به این ترتیب احتمال موفقیت یا انتظار رضایت‌مندی (تابع توزیع ثانویه) به شرط داشتن دنباله‌ای از داده‌های آزمایش برنولی از توزیع بتا پیروی می‌کند. در این حالت اعتماد

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

مستقیم، میانگین توزیع بتا با پارامترهای α و β مطابق با رابطه (۸) خواهد شد.

$$T_{ij} = \frac{\alpha}{\alpha + \beta} \quad (۸)$$

در این رابطه α تعداد رضایت‌مندی‌ها (۱ها) و β تعداد عدم رضایت‌ها (صفرها) است.

الگوریتم مدیریت اعتماد مبتنی بر پیشنهاد، در مقاله [37] با هدف امن‌سازی مسیر بین مبدأ و مقصد براساس ارزش اعتماد هر رأس ارائه شده است. در این مقاله، برای محاسبه اعتماد مستقیم از **امید ریاضی توزیع بتا** استفاده شده است. توزیع بتا با استفاده از دو پارامتر (α, β) تخمین زده می‌شود که در این مقاله این دو پارامتر با جمع‌آوری مشاهدات از رساندن و صرف‌نظرکردن بسته‌ها محاسبه می‌شوند. به‌صورتی که اگر ρ نشان‌دهنده مجموع مشاهدات مثبت (بسته‌های ارسال‌شده) و n نشان‌دهنده مجموع مشاهدات منفی (بسته‌های صرف‌نظرشده) باشد و در یک بازه زمانی تراکنش مثبت یا منفی بین دو رأس رخ داده باشد، آن‌گاه مقدار قدیمی ρ و n ابتدا در ضریب کاهش ضرب و سپس با مقدار جدید ترکیب می‌شود و سپس α_{ij} و β_{ij} با استفاده از روابط $\alpha_{ij} = \rho + ۱$ و $\beta_{ij} = n + 1$ محاسبه می‌شوند. مقدار اعتماد مستقیم بین هر دو رأس نیز با محاسبه امید ریاضی توزیع بتا $\frac{\alpha_{ij}}{\alpha_{ij}+\beta_{ij}}$ به‌روزرسانی می‌شود.

پروتکل مدیریت اعتماد در مقاله [19] توزیع شده است و هر کاربر اعتماد نسبت به سایر اشیا را خودش محاسبه و فقط تعداد محدودی از اطلاعات را حفظ و نگهداری می‌کند. نظر کاربر u_x نسبت به شیء d_i بعد از هر تراکنش مستقیم به‌صورت یک و صفر (دودویی) که به‌ترتیب به معنی رضایت‌مندی و عدم رضایت است، ذخیره می‌شود. رابطه (۹) نحوه به‌روزشدن $\beta_{x,i}$ و $\alpha_{x,i}$ را به روش **هموارسازی نمایی** نشان می‌دهد.

$$\begin{aligned} \alpha_{x,i} &= e^{-\varphi \Delta t}.\alpha_{x,i}^{(old)} + f_{x,i} \\ \beta_{x,i} &= e^{-\varphi \Delta t}.\beta_{x,i}^{(old)} + 1 - f_{x,i} \end{aligned} \quad (۹)$$

در رابطه بالا $f_{x,i}$ نشان‌دهنده نظر مثبت و $1 - f_{x,i}$ نشان‌دهنده نظر منفی است. Δt بازه زمانی است که در آن $\beta_{x,i}$ و $\alpha_{x,i}$ به‌روز می‌شوند و φ فاکتور تضعیف زمان است. در این صورت اعتماد مستقیم کاربر u_x نسبت به شیء d_i $(t_{x,i}^{d})$ با محاسبه **امید ریاضی توزیع بتا** در [19] و [20] به‌دست می‌آید. (رابطه ۱۰)

$$t_{x,i}^{d} = \frac{\alpha_{x,i}}{\alpha_{x,i} + \beta_{x,i}} \quad (۱۰)$$

۴-۲-۴- میانگین وزن دار

مدل ارائه‌شده در مقاله [18] به‌صورت متمرکز عمل می‌کند و ایده اصلی برای ارزیابی قابل اعتمادبودن یک شیء در شبکه، تجمیع نظرات خدمت‌گیرندگان پس از ارائه تعدادی خدمت مختلف است و به‌صورت توانایی یک شیء در ارائه خدمت خاص تعریف شده است. مدل ارائه‌شده در این مقاله برای ارزیابی اعتماد پنج مرحله را شامل سه فاز می‌شود:

- مرحله جمع‌آوری اطلاعات: مدیریت سامانه اعتماد، پیش از محاسبه، اطلاعات کافی از شبکه را جمع‌آوری می‌کند.
- مرحله انتخاب: زمانی که شیء اعلام می‌کند قادر است خدمت مورد نیاز را ارائه کند، سامانه مدیریت اعتماد مرحله انتخاب را آغاز می‌مند که این فرآیند پنج مرحله را شامل می‌شود:

- مرحله نخست: در ابتدا سامانه مدیریت اعتماد تعدادی از اشیا را براساس نیازمندی به خدمت و پتانسیل آن‌ها به‌عنوان نامزد برمی‌گزینند.
- مرحله دوم: پس از انتخاب اولیه، اشیا برای انتخاب نهایی با یکدیگر رقابت می‌کنند. در این مقاله رئوس نامزد که پتانسیل انتخاب‌شدن دارند با دو معیار نوع خدمت و ظرفیت مورد بررسی قرار می‌گیرند. هرچند که مجزاکردن خدمت‌های قابل ارائه مشکل است، ولی منظور از ظرفیت شیء، درصد باتری، قدرت پردازش و حافظه آن است.
- مرحله سوم: از آن‌جایی که همه نظرات، از اهمیت یکسانی برخوردار نیستند به بازخوردها وزن نسبت داده می‌شود. وزن نسبت داده‌شده به هر بازخورد مطابق با رابطه $w_{R_{ij}} = \lambda^{d_{ij}} \theta^{(s+1)(t_{now}-t_j)}$ با درنظرگرفتن گذشت زمان، بازخورد خدمت گیرنده (میزان رضایت از خدمت) و فاصله بین گیرنده و ارائه‌دهنده خدمت محاسبه شده است. پارامترهای λ و θ بین صفر و یک هستند که قابل تنظیم هستند. s نیز از رابطه $s = \frac{1}{2} * (N_j^2 - N_j)$ به‌دست می‌آید. درصورتی‌که ۱ یا ۰ $= N_j$ شود، مقدار s برابر صفر خواهد شد؛ ولی اگر ۱- $= N_j$ شود، مقدار s برابر یک خواهد شد و به این معنی است که اثر نظر منفی در مقایسه با مثبت و خنثی دو برابر است.
- مرحله چهارم: در این مرحله اعتماد با گرفتن **میانگین وزن‌دار** نظرات محاسبه می‌شود و وزن نظرات همان $w_{R_{ij}}$ و کیفیت رأسی است که به خدمت‌دهنده امتیاز داده است.

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

- مرحله پنجم: بعد از محاسبه سطح اعتماد همه نامزدها، قابل اعتمادترین شیء انتخاب و سپس رأس درخواست‌کننده پس از دریافت خدمت، با توجه به میزان رضایت از عملکرد خدمت‌دهنده به آن امتیاز می‌دهد.

- مرحلهٔ یادگیری: زمانی که شیء گیرنده خدمت ارزیابی خود نسبت به ارائه‌دهنده را به سامانهٔ مدیریت اعتماد بازمی‌گرداند، سامانهٔ مدیریت اعتماد وارد مرحلهٔ یادگیری می‌شود و سطح اعتماد رئوسی را که درباره خدمت‌دهنده بازخورد داده بودند، به‌روزرسانی می‌کند. مرحلهٔ یادگیری دو مرحله به‌روزرسانی کیفیت پیشنهاددهنده و به‌روزرسانی شهرت را شامل می‌شود.

مقاله [23] دو روش ذهنی و عینی برای محاسبه اعتماد ارائه کرده که روش ذهنی همان روش ارائه‌شده در مقاله [21] است. در مدل عینی مقادیر مورد نیاز برای محاسبه اعتماد در کل شبکه توزیع شده‌اند و برای رسیدن به این هدف از جدول هش توزیع‌شده[1] استفاده شده است. زمانی که رأس i نیاز به دانستن اعتماد رأس j دارد از DHT درباره j می‌پرسد و نظرات مستقیم کوتاه‌مدت (O_j^{rec}) و طولانی‌مدت (O_j^{lon}) که همان **میانگین وزن‌دار** بازخوردهای دریافت‌شده از همه رئوسی است که رأس j با آن‌ها تراکنش داشته است، با استفاده از رابطه (۱۱) به‌دست می‌آیند.

$$O_{ij}^{rec\,/\,lon} = \sum_{i=1}^{M}\sum_{l=1}^{L^{rec\,/\,lon}} f_{ij}^{l}\,\omega_{ij}^{l}\,C_{ij}^{l} \Big/ \sum_{i=1}^{M}\sum_{l=1}^{L^{rec\,/\,lon}} \alpha \qquad (۱۱)$$

در رابطه بالا ω_{ij}^{l}، وزن در نظر گرفته‌شده برای هر بازخورد است تا رئوس، قابلیت اعتمادشان را بر تراکنش‌های ضعیف بنا نکنند و به‌منظور جلوگیری از اعمال بازخوردهای ناصحیح توسط رئوس مخرب هر بازخورد توسط پارامتر اعتبار (C_{ij}^{l}) وزن‌دار می‌شود. ($L^{lon} > L^{rec}$)

۵-۲-۴- سایر روش‌ها

در مقاله [49] با ارائه مدلی براساس تراکنش بین کاربران و بازار برنامه‌ها، میزان امنیت و اعتماد به برنامه‌ها ارزیابی می‌شود. ارزشیابی با اندازه‌گیری میزان شباهت رفتار برنامه و رفتاری که کاربر از برنامه انتظار دارد انجام می‌شود. برای هر برنامه می‌توان یک بردار خصوصی تعریف کرد که وضعیت دسترسی برنامه به محرمانگی کاربر را نشان دهد. واضح است که کاربران تمایل زیادی دارند که برنامه‌ها به هیچ بخش از حریم خصوصی آن‌ها وارد نشوند؛ بنابراین برداری به نام مطلوب‌ترین بردار به شکل $P_{best} = \underbrace{(0,0,\dots,0)}_{n}\ (n \in R^{+})$ تعریف شده است. مقدار عددی اعتماد به یک برنامه با محاسبه شباهت بین دو بردار P و P_{best} و با استفاده از **ضریب شباهت** Jaccard مطابق با رابطه (۱۲) به‌دست می‌آید.

$$T(A)_m = Jaccard(P_m, P_{best}) == \frac{|P_m \cap P_{best}|}{|P_{best}|} \times 100\% = \left(1 - \frac{\sum_{i=1}^{n} p_i}{n}\right) \times 100\% \qquad (۱۲)$$

جدول (۱) با هدف مقایسه مدل‌های محاسبه اعتماد، هر سطر را به یک مدل اختصاص داده و در هر ستون ویژگی‌های آن مدل ارائه شده است. برای محاسبه اعتماد مستقیم در مقالات [21]، [17]، [22]، [23]، [24] و [58] از **جمع وزن‌دار ایستا** استفاده شده است. در مقالات [19]، [20] و [37] از **امید ریاضی توزیع بتا**، در [49] از **معیار شباهت جاکارد** و در [25] از جمع **وزن‌دار پویا** برای محاسبه اعتماد مستقیم استفاده شده است.

۵- تحلیل مدل‌های محاسبه اعتماد غیرمستقیم

۵-۱- فاکتورهای اصلی در محاسبه اعتماد غیرمستقیم

با توجه به این‌که شبکه اینترنت اشیا تعداد زیادی شیء با قابلیت‌های متنوع را شامل می‌شود، تجربه‌های مستقیم حاصل از تراکنش‌ها برای ارزیابی شیء ارائه‌دهنده خدمت کافی نیست؛ بنابراین شیء نیازمند خدمت با پرسش از سایر رئوسی که با نامزد ارائه خدمت تراکنش داشته‌اند، اطلاعات خود را کامل می‌کند. به این ترتیب پارامتر اصلی در محاسبه اعتماد غیرمستقیم نظرات اشیا یا صاحبان اشیایی هستند که از آن‌ها راجع به داوطلب ارائهٔ خدمت پرسیده می‌شود و درقبل با رأس یادشده تراکنش داشته‌اند؛ علاوه‌براین، استفاده از پارامترهایی که با ویژگی‌های شبکه اینترنت اشیا در ارتباط هستند در مدل‌های ارائه‌شده مرسوم است.

۵-۲- مدل‌های ارائه‌شده محاسبه اعتماد غیرمستقیم

۵-۲-۱- میانگین وزن‌دار

[1] Distributed Hash Table (DHT)

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

در مقاله [21] نظر غیرمستقیم (O_{ij}^{ind}) از **میانگین وزن‌دار** نظرات مستقیم رئوسی که با معتمد در ارتباط هستند، محاسبه می‌شود. (رابطه ۱۳)

$$O_{ij}^{ind} = \sum_{\mathcal{K}=1}^{|\mathcal{K}_{ij}|} C_{ik}\, O_{kj}^{dir} \Big/ \sum_{\mathcal{K}=1}^{|\mathcal{K}_{ij}|} C_{ik} \qquad (۱۳)$$

اعتبار رأس k در نزد i (همان دوست مشترک i و j) از رابطه (۱۴) به‌دست می‌آید و با تجربه مستقیم i از k (O_{ik}^{dir}) و مرکزیت i از نظر k رابطه مستقیم و با هوش k رابطه عکس دارد.

$$C_{ik} = \eta O_{ik}^{dir} + \mu R_{ik} + \rho(1 - I_k) \qquad (۱۴)$$

در مقاله [19] هر کاربر می‌تواند از دوستانش بخواهد که به‌عنوان پیشنهاددهنده نظرشان را راجع به شیء ناشناس بگویند. انتخاب پیشنهاددهندگان به این شرط است که این افراد شبیه‌ترین به خود او باشند. برای اندازه‌گیری شباهت از معیار ضرب داخلی استفاده شده است؛ پارامترهای شباهت هم دوستان مشترک، ارتباط اجتماعی مشترک و علاقه‌مندی‌های مشترک هستند و شباهت بین دو کاربر با گرفتن میانگین این سه مقدار به‌دست می‌آید. به این ترتیب اعتمادکننده وقتی پیشنهادهای سایر کاربران را دریافت کرد، k نفر را که بیشترین شباهت را به او دارند، انتخاب (مجموعه U) و با استفاده از **میانگین وزن‌دار** اعتماد غیرمستقیم را مطابق با رابطه (۱۵) محاسبه می‌کند.

$$t_{x,i}^{r} = \sum_{u_y \in U} \frac{sim(u_x, u_y)}{\sum_{u_y \in U} sim(u_x, u_y)} . t_{y,i}^{d} \qquad (۱۵)$$

در مقاله [25] برای محاسبه اعتماد غیرمستقیم اگر رأسi از سایر رئوس درباره j بپرسد، اعتماد غیرمستقیم از **میانگین وزن‌دار** اعتماد مستقیم پیشنهاددهندگان مطابق با رابطه (۱۶) به‌دست خواهد آمد.

$$Ind_{i,j}^{c} = \frac{\sum_{1}^{M} (RT_{j,k}^{cn} * X_k)}{M} \qquad (۱۶)$$

در رابطه بالا $RT_{j,k}^{cn}$، اعتماد نسبت به j در زمینه c از نظر k به‌عنوان پیشنهاددهنده است و X_k، میزان اطمینان رأس i به پیشنهاددهنده (k) را نشان می‌دهد و M تعداد کل پیشنهادهایی است که از همه رئوس پیشنهاددهنده به‌دست آمده است.

در مقاله [58] اعتماد غیرمستقیم که شهرت عمومی نام‌گذاری شده، **میانگین وزن‌دار** نظرات مستقیم بدون درنظرگرفتن موضوع است. وزن نظرات بدون درنظرگرفتن نوع خدمت، فاکتور گذشت زمان و اعتبار در نظر گرفته شده است.

(جدول-۱): مقایسه روش‌های محاسبه اعتماد در اینترنت اشیا

(Table-1): The comparison of trust computation features in the IOT

پارامترهای اجتماعی	روش‌های محاسبه اعتماد													منابع
	به روز رسانی اعتماد		دسترسی به داده‌ها	ترکیب اعتماد		اعتماد غیر مستقیم			اعتماد مستقیم		مدل ارتباطی			
	بازه زمانی	بعد از تراکنش		متغیرها	روش	انتخاب پیشنهاددهندگان	متغیرها	روش محاسبه	متغیرها	روش محاسبه	معتمد	اعتمادکننده		
فاکتور رابطه و مرکزیت	---	√	غیر متمرکز	مرکزیت، هوش، اعتماد مستقیم و اعتماد غیرمستقیم	جمع وزن‌دار ایستا	---	نظرات غیرمستقیم و اعتبار	میانگین وزن دار	فاکتور رابطه، نظر بلند مدت و نظر طولانی مدت مستقیم	جمع وزن‌دار ایستا	شیء	شیء		[21]
علاقه‌مند به همکاری و گروه علاقه‌مندی‌های مشترک	---	√	غیر متمرکز	مقدار قبلی اعتماد و نظر پیشنهاددهنده	جمع وزن‌دار پویا	---	نظر پیشنهاددهنده	---	تجربه گذشته و مشاهدات مستقیم از صداقت، همکاری و گروه	جمع وزن‌دار ایستا	شیء	شیء		[17]
علاقمند به همکاری و گروه علاقه‌مندی‌های مشترک	---	√	غیر متمرکز	مقدار قبلی اعتماد و نظر پیشنهاددهنده	جمع وزن‌دار پویا	---	نظر پیشنهاددهنده	---	تجربه گذشته و مشاهدات مستقیم از صداقت، همکاری و گروه	جمع وزن دار ایستا	شیء	شیء		[22]
---	---	√	متمرکز	---	---	شباهت موضوعی و قابلیت	---	---	کیفیت پیشنهاددهندگان ، فاصله، زمان و وزن امتیازات	میانگین وزن‌دار پویا	شیء	شیء		[18]
---	---	√	متمرکز	اعتماد مستقیم داوطلبان	میانگین ریاضی	---	---	---	بردار محرمانگی واقعی و بردار محرمانگی ایده‌آل	ضریب شباهت Jaccard	برنامه موبایل	انسان		[49]

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

فاکتور رابطه و مرکزیت	---	√	غیر متمرکز	مرکزیت، اعتماد مستقیم و اعتماد غیرمستقیم	جمع وزن‌دار ایستا	---	نظرات غیرمستقیم و اعتبار	میانگین وزن‌دار	هوش، نظر بلند مدت و نظر طولانی‌مدت مستقیم	جمع وزن‌دار ایستا	شیء	شیء	ذهنی	[23]
فاکتور رابطه و مرکزیت	---	√	نیمه متمرکز	---	---	---	---	---	مرکزیت، نظر بلند مدت و نظر طولانی‌مدت مستقیم	جمع وزن‌دار ایستا	شیء	شیء	عینی	
---	√	---	غیر متمرکز	اعتماد مستقیم و اعتماد غیر مستقیم	جمع وزن‌دار ایستا	مقدار اطمینان، انحراف و اندازه نزدیکی	تراکنش مثبت و منفی همسایگان	مجموع امیدهای ریاضی توزیع	تراکنش مثبت، تراکنش منفی و فاکتور اثر گذشت زمان	امید ریاضی توزیع بتا	شیء	شیء	[37]	
دوستان مشترک، ارتباط اجتماعی مشترک و علاقه‌مندی‌های مشترک	√	√	غیر متمرکز	اعتماد مستقیم، اعتماد غیرمستقیم و وزن پویا	جمع وزن‌دار پویا	دوستان مشترک، ارتباط اجتماعی مشترک و علاقه‌مندی‌های مشترک	نظر مستقیم پیشنهاددهندگان ، شباهت اجتماعی	میانگین وزن‌دار	تراکنش مثبت، تراکنش منفی و فاکتور اثر گذشت زمان	امید ریاضی توزیع بتا	شیء	انسان	[19]	
علاقمند به همکاری و گروه علاقه‌مندی‌های مشترک	√	√	غیر متمرکز	مقدار قبلی اعتماد و نظر پیشنهاددهنده	جمع وزن‌دار پویا	---	نظر پیشنهاددهنده	---	تجربه گذشته و مشاهدات مستقیم از صداقت، همکاری و گروه علاقه‌مندی‌های	جمع وزن‌دار ایستا	شیء	شیء	[24]	
اعتماد به مالک (مرکزیت و تعداد دوستان مشترک) و فاکتور ارتباط	---	√	غیر متمرکز	اعتماد مستقیم، اعتماد غیرمستقیم و وزن ایستا	جمع وزن‌دار ایستا	---	کیفیت پیشنهاددهندگان ، زمان، مرکزیت و اعتماد صاحبان اشیا	میانگین وزن‌دار	مشاهدات مستقیم، وزن نرمال شده موضوعات و زمان	جمع وزن‌دار پویا	شیء	شیء	[25]	
اعتبار	--	√	متمرکز	اعتماد مستقیم پیشنهاددهندگان و اعتبار آنها	جمع وزن‌دار ایستا	اعتبار پیشنهاد دهندگان	---	---	تجارب مثبت و منفی، فاکتور اثر گذشت زمان	توزیع بتا	شیء	انسان	[20]	
شباهت اجتماعی	--	√	نیمه متمرکز	اعتماد مستقیم، شهرت عمومی و پارامتر تبعیض	جمع وزن‌دار پویا	---	تجارب مثبت و منفی، زمان و اعتبار	میانگین وزن‌دار	تجارب مثبت و منفی وزن‌دار، فاکتور اثر گذشت زمان	جمع وزن‌دار ایستا	شیء	شیء	[58]	

۲-۲-۵- امید ریاضی توزیع بتا

اعتماد غیرمستقیم در مقاله [37] با استفاده از **توزیع بتا** محاسبه می‌شود، به‌طوری‌که اعتماد غیرمستقیم درواقع مشاهدات مستقیمی است که همسایه‌های رئوس ارزیابی‌کننده از ارزیابی‌شونده، داشته‌اند. با استفاده از اعتماد غیرمستقیم می‌توان بر مشکل ناکافی‌بودن اطلاعات غلبه کرد و رئوس جدید با استفاده از پیشنهادهای سایر رئوس، میزان اعتماد را پیش از انجام تراکنش محاسبه کند.

۳-۲-۵- سایر روش‌ها

در مقالات [17]، [22] و [24] درصورتی‌که دو رأس تراکنش مستقیم نداشته باشند، نظر پیشنهاددهنده ($R_{ij}^{X}(t)$) در متریک‌های صداقت، همکاری و علاقمندی به انجمن، اعتماد غیرمستقیم درنظرگرفته می‌شود.

مطابق با آنچه در جدول (۱) نشان داده شده است، در محاسبه اعتماد غیرمستقیم از روش **میانگین وزن دار**، در مقالات [19]، [21]، [25] و [58]؛ از **جمع امیدهای ریاضی توزیع بتا** در مقاله [37] استفاده شده است. فقط در مقالات [18]، [19]، [20] و [37] پیشنهاددهندگان با فیلترهای شباهت انتخاب شده‌اند.

۶- تحلیل مدل‌های ترکیب اعتماد مستقیم و غیرمستقیم

۱-۶- فاکتورهای اصلی در ترکیب اعتماد مستقیم و غیرمستقیم

اعتمادکننده در شبکه اینترنت اشیا پس از محاسبه اعتماد مستقیم و غیرمستقیم با استفاده از متغیرهای وابسته به شبکه اینترنت اشیا و روش‌های زیر می‌تواند این دو مقدار

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

را با یکدیگر ترکیب و مقدار نهایی اعتماد را محاسبه کند. مطابق با جدول (۱) اعتماد مستقیم و غیرمستقیم با استفاده از **جمع وزن‌دار ایستا** در [20]، [21]، [23]، [37] و [25]؛ **میانگین ریاضی** در [49] و **جمع وزن‌دار پویا** در [19] و [58] با یکدیگر ترکیب شده‌اند.

۲-۶- مدل‌های ارائه‌شده در ترکیب اعتماد مستقیم و غیرمستقیم

۱-۲-۶- جمع وزن‌دار ایستا

در مدل مقاله [21]، اعتماد نهایی از رابطه (۱۷) که **جمع وزن‌دار** اعتماد مستقیم، اعتماد غیرمستقیم، هوش و مرکزیت با ضرایب **ایستا** به‌دست می‌آید. R_{ij} که همان مرکزیت i نسبت به j است و به‌صورت $R_{ij} = \frac{|\mathcal{K}_{ij}|}{|\mathcal{N}_i|}$ تعریف می‌شود، نشان‌دهنده افرادی است که دوستان مشترک زیادی دارند و به این ترتیب در بسیاری از موارد نیز هم‌عقیده هستند:

$$T_{ij} = \alpha R_{ij} + \beta I_j + \gamma O_{ij}^{dir} + \delta O_{ij}^{ind} \qquad (۱۷)$$
$$\alpha + \beta + \gamma + \delta = 1$$

در مقاله [23] زمانی که رأس i نیاز به دانستن اعتماد j دارد از DHT درباره رأس j می‌پرسد و همه رئوس می‌توانند میزان اعتماد به یک رأس را از DHT بخوانند و اعتماد از جمع وزن‌دار ایستای نظرات مستقیم (رابطه ۱۱) و مرکزیت مطابق با رابطه (۱۸) حاصل می‌شود.

$$T_j = (1 - \alpha - \beta)R_j + \alpha O_j^{lon} + \beta O_j^{rec} \qquad (۱۸)$$

مرکزیت در رابطه (۱۸) به این معنی است که رأس در بسیاری از تراکنش‌ها درگیر بوده و به‌صورت رابطه (۱۹) تعریف می‌شود:

$$R_j = {(A_j + H_j)}/{(Q_j + A_j + H_j)} \qquad (۱۹)$$

در رابطه (۱۹)، Q_j تعداد دفعاتی است که رأس j درخواست خدمت کرده است. A_j معادل تعداد مرتبه‌هایی است که این رأس به‌عنوان واسطه در تراکنش حضور داشته و H_j تعداد دفعاتی است که رأس j تأمین‌کننده خدمت بوده است. به عبارتی رأسی در شبکه اینترنت اجتماعی، مرکزی به حساب می‌آید که در تعداد بیشتری تراکنش به‌عنوان خدمت‌دهنده یا واسطه حضور داشته باشد.

مدل ارائه‌شده در مقاله [25] برای محاسبه اعتماد نهایی بین دو رأس مفروض از **جمع وزن‌دار اعتماد مستقیم و غیرمستقیم با ضرایب ایستا** مطابق با رابطه (۲۰) استفاده می‌کند.

$$T_{ij}^X(t) = \alpha * DT_{i,j} + \beta * IndT_{i,j} \qquad (۲۰)$$

مدل ارائه‌شده در [20]، در صورتی که نیاز به پرسش از سایرین داشته باشد، اعتبار پیشنهاددهندگان (شاهدان)، همان اعتماد مستقیم در زمینه پیشنهاد است که با سه معیار شباهت، اعتبار مشارکت و اعتبار مکانی محاسبه می‌شود. زمانی که ابر مرکزی مقادیر اعتماد را از شواهد دریافت می‌کند، اعتماد نهایی از **جمع وزن‌دار** اعتماد مستقیم شاهدان حاصل می‌شود؛ به‌طوری‌که وزن‌ها همان اعتبار شاهدان هستند.

۲-۲-۶- جمع وزن‌دار پویا

در مقالات [17]، [22] و [24] در صورتی که دو رأس i و j تراکنش مستقیم نداشته باشند، مطابق با رابطه (۲۱) اعتماد از **جمع وزن‌دار پویا** مقدار عددی قبلی و نظر پیشنهاددهنده ($R_{ij}^X(t)$) به‌دست می‌آید.

$$T_{ij}^X(t) = (1-\gamma)T_{ij}^X(t - \Delta t) + \gamma R_{ij}^X(t) \text{ اگر } j! = k \qquad (۲۱)$$

وزن γ که به‌منظور اعتباردهی به نظر پیشنهاددهنده و تجارب قدیمی استفاده شده است، با رابطه $\gamma = \frac{\beta D_{ik}^X(t)}{1+\beta D_{ik}^X(t)}$ به‌دست می‌آید.

اعتماد کل در مدل [37] از **جمع وزن‌دار پویا** اعتماد مستقیم و غیرمستقیم مطابق با رابطه (۲۲) حاصل می‌شود. در این مدل وزن به‌صورت پویا براساس کمیت و کیفیت تراکنش‌های رئوس ارزیابی‌شونده محاسبه می‌شود.

$$T_{ij} = \omega_d * T_{ij}^d + \omega_i * T_{ij}^i, \quad \omega_d + \omega_i = 1 \qquad (۲۲)$$

اعتماد نهایی در مدل [19] نیز ترکیب اعتماد مستقیم و غیرمستقیم است که با استفاده از **جمع وزن‌دار پویا** و از رابطه (۲۳) حاصل می‌شود.

$$t_{x,i} = \mu . t_{x,i}^d + (1-\mu). t_{x,i}^r \qquad (۲۳)$$

۳-۲-۶- میانگین ریاضی

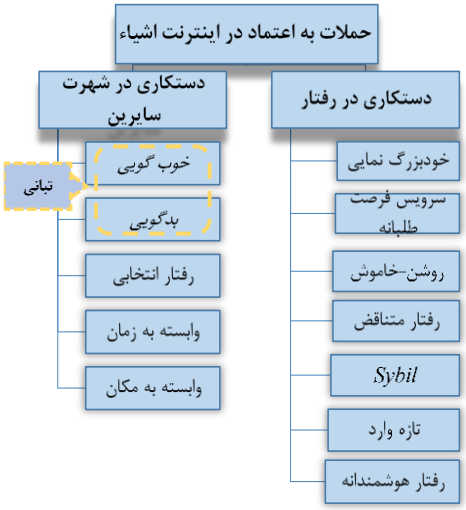
مدل ارائه‌شده در مقاله [49] به‌صورت به‌طورکامل متمرکز عمل می‌کند و میزان اعتماد به برنامه با محاسبه **میانگین ریاضی** کلیه بازخوردهای دریافتی از رأی‌دهندگان به‌دست می‌آید.

۷- تحلیل مدل‌های اعتماد از منظر حملات

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

۱-۷- انواع حملات به اعتماد در شبکه اینترنت اشیا

شبکه اینترنت اشیا تعداد زیادی عنصر ناهمگن دارد که خدمات متنوعی ارائه می‌کنند. برخی از این اشیا مخرب هستند که با حملاتی نظیر خوب جلوه دادن خود، بدگویی از دیگران و یا کاهش شهرت دیگر اشیا، عملکرد سامانه را با مشکل مواجه می‌سازند. حمله‌های متعددی با هدف شکستن سامانه‌های مدیریت اعتماد طراحی شده‌اند. مطابق شکل (۳) حملات مرتبط با اعتماد در حوزه اینترنت اشیا به دو دسته اصلی تقسیم شده‌اند.



(شکل-۳): انواع حملات به اعتماد در اینترنت اشیا
(Figure-3): Types of attacks on the IOT trust

در دسته‌ای از حملات، اشیا دیگران را با دست‌کاری در رفتار خود دچار اشتباه می‌کنند و در دسته دوم رئوس مخرب شهرت دیگران را با اظهار نظر نادرست، دچار تغییر می‌کنند. نوعی از حملات نیز وجود دارند که از همکاری تعدادی رأس مخرب به‌وجود می‌آید؛ به این ترتیب که تعدادی رأس با تبانی جهت بدنام‌کردن یک رأس مشهور و یا خوش‌نام‌کردن رأس بی‌کفایت با هم به توافق می‌رسند.

حملاتی که به‌وسیلهٔ رئوس مخرب علیه سامانه‌های مدیریت اعتماد اجرا می‌شود و به‌طورعمومی با مفهوم اعتماد مرتبط هستند، در ادامه به‌اختصار شرح داده می‌شوند:

- حمله خدمت فرصت‌طلبانه[1]: رأس مخرب به‌محض این‌که متوجه می‌شود، شهرت خود را از دست داده است، کیفیت ارائه خدمت را بالا می‌برد [19].
- حمله روشن-خاموش[2]: رأس مخرب در اجرای حمله روشن-خاموش با ایجاد الگوی رفتاری که بین رفتار خوب و بد در حال تغییر است، امیدوار است تا زمان آسیب‌رسانی به‌صورت نامحسوس باقی بماند [62].
- حمله رفتار متناقض[3]: رأس مخرب به دلخواه به برخی خدمات بی‌کیفیت ارائه می‌کند، درحالی‌که رفتار متفاوتی با سایرین دارد.

حمله Sybil: در این حمله، رأس مخرب با ایجاد شماره‌های شناسایی بدل، هویت واقعی خود را مخفی می‌کند.

- حمله تازه وارد[4]: زمانی که عنصر مخرب پیشینه بد و سوء خود را پاک و به‌عنوان کاربر جدید و با شناسه متفاوت خود را معرفی می‌کند، این حمله رخ می‌دهد [62].
- حمله رفتار هوشمندانه[5]: در این حمله رأس مخرب به‌صورت هوشمندانه مطابق با آستانه قابل اعتمادماندن، با پیشنهادهای نادرست یا خدمات خوب و بد تغییر رفتار می‌دهد [37].
- حمله خوب‌گویی[6]: در این مدل حملات، شهرت رئوس بدنام با تعریف و ارائه پیشنهادهای خوب دربارهٔ آن‌ها افزایش می‌یابد و درنتیجه بخت رئوس ناشایست برای انتخاب به‌عنوان ارائه‌دهنده خدمت بالا می‌رود [63].
- حملهٔ بدگویی[7]: در این حالت رأس مخرب با ازبین‌بردن شهرت یک رأس خوش‌نام (مثلاً با ارائه پیشنهادهای بد درمورد رئوس خوب) باعث کاهش محبوبیت آن رأس شده و شانس انتخاب این رأس به‌عنوان خدمت‌دهنده را کاهش می‌دهد [63].
- حملهٔ رفتار انتخابی[8]: عنصر مخرب از روی عمد درباره برخی رئوس گزارش غلط ارائه می‌دهد؛ در صورتی که با سایر اجزای شبکه چنین رفتاری از خود نشان نمی‌دهد [37].
- حمله وابسته به زمان[9]: در این مدل حمله نحوه ارائه بازخورد رأس مخرب با تغییر زمان متفاوت می‌شود؛ به‌طوری‌که به دنبال فرصت مناسب برای امتیازدهی ناعادلانه است [37].
- حمله وابسته به مکان[10]: در این حمله، نحوه ارائه بازخورد رأس مخرب با تغییر مکان متفاوت می‌شود؛

[1] Opportunistice Service Attack
[2] On-off Attack
[3] Conflicting Behavior Attack
[4] Newcomer Attack
[5] Intelligent Behavior attack
[6] Good-mouthing Attack
[7] Bad-mouthing Attack
[8] Selective Behavior Attack
[9] Time-dependent Attack
[10] Location-dependent Attack

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

به‌طوری‌که به‌دنبال موقعیت فیزیکی مناسب برای امتیازدهی ناعادلانه است [37].

از آنجایی که در دنیای واقعی اینترنت اشیا، رئوس مخرب در تلاش برای کاهش کارآیی و آسیب‌رسانی به عناصر شبکه هستند، مقالات ارائه‌شده در حوزه مدیریت اعتماد در اینترنت اشیا متناسب با الگوریتم تخمین اعتماد، روش‌های مقابله با حملات را نیز ارائه کرده‌اند.

۲-۷- روش‌های مقابله با حملات در مدل‌های اعتماد

در [20] با فیلترکردن شاهدان به‌وسیله متریک‌های **اعتبار**، مدل در برابر حملات بدگویی و خوب‌گویی مقاوم شده است. به‌علاوه، ابر مرکزی کارآیی ارائه‌دهنده خدمت را برای مقابله با حمله خود بزرگ‌نمایی از طریق جمع وزن‌دار توانمندی‌های ارائه‌دهنده خدمات محاسبه می‌کند که در این رابطه وزن‌ها، اعتبار درخواست‌کننده خدمت هستند.

در مقاله [21] مطابق با رابطه (۱۳) برای مقابله با **بازخورد دروغین پیشنهاددهندگان**، از اعتبار پیشنهاددهندگان به‌عنوان وزن نظرات استفاده می‌شود.

در مقالات [17]، [22] و [24]، برای مقابله با حملات به‌منظور اعتباردهی به نظر پیشنهاددهنده و تجارب قدیمی از وزن γ استفاده شده است. (رابطه ۲۱) γ از فرمول $\frac{\beta D_{ik}^{x}(t)}{1+\beta D_{ik}^{x}(t)}$ به‌دست می‌آید و با ضریب $\beta \geq 0$ نرمالیزه می‌شود که اثر پیشنهادها غیرمستقیم نام‌گذاری شده است. اگر β عدد کوچکی انتخاب شود، آن‌گاه مقدار γ نیز کوچک خواهد شد و این به آن معنی است که تجارب گذشته نسبت به نظر پیشنهاددهنده وزن بیشتری دارد؛ درحالی‌که اگر β عدد بزرگی انتخاب شود، آن‌گاه مقدار γ به سمت یک میل می‌کند و در محاسبه اعتماد، نظر پیشنهاددهنده وزن بیشتری به خود اختصاص می‌دهد. درواقع با انتخاب β از **حمله‌های خوب‌گویی** و **بدگویی** جلوگیری می‌شود؛ چون که اگر k رأس بدی باشد، می‌توان β را نزدیک به صفر انتخاب کرد تا حمله بدگویی رخ ندهد و اگر k رأس خوبی باشد β بزرگ انتخاب می‌شود.

مقاله [18] اعتماد را به‌صورت به‌طورکامل متمرکز محاسبه می‌کند و با دادن وزن به بازخوردها با پارامترهای قابل تنظیم به‌طوری‌که اثر نظر منفی در مقایسه با مثبت و خنثی دو برابر باشد، مدل را نسبت به **حملات خوب گویی، بدگویی** و **روشن-خاموش** مقاوم کرده است.

مدل عینی محاسبه اعتماد در مقاله [23] به‌صورت نیمه‌متمرکز عمل می‌کند و به‌منظور جلوگیری از **اعمال بازخورد ناصحیح** به‌وسیله رئوس مخرب هر بازخورد توسط پارامتر اعتبار که در رابطه ۲۴ نشان داده شده است، وزن‌دار می‌شود. به این ترتیب رئوسی که پیوندهای ارتباطی قوی دارند، خیلی باهوش هستند و تعداد زیادی تراکنش برقرار کرده‌اند پتانسیل رفتار مخرب را دارند؛ از اعتبار کمتری برخوردار می‌شوند.

$$C_{ij} = \frac{(1-\gamma-\delta)T_i + \gamma(1-F_{ij}) + \delta(1-I_i)}{1+log(N_{ij}+1)} \qquad (۲۴)$$

در مقاله [37] مطابق با رابطه (۲۲)، وزن اعتماد مستقیم (ω_d) و غیرمستقیم (ω_i) به‌صورت پویا براساس کمیت و کیفیت تراکنش‌های مشاهده‌شده به‌وسیله رئوس ارزیابی‌شونده محاسبه می‌شود. اگر رأس ارزیابی‌کننده اطلاعات کافی درباره ارزیابی‌شونده داشته باشد، وزن اعتماد مستقیم مساوی یا بزرگتر در نظر گرفته می‌شود. در مقابل اگر رأس ارزیابی‌کننده قادر به قضاوت درباره ارزیابی‌شونده نباشد، وزن بیشتری به اعتماد غیرمستقیم داده می‌شود. با توجه به اینکه محاسبه اعتماد غیرمستقیم با جمع‌آوری نظرات همسایه‌ها به‌دست می‌آید و از طرفی همه نظرات قابل اعتماد نیستند، ایده فیلترکردن پیشنهادها مبتنی بر خوشه‌بندی در این مدل ارائه شده است و رئوس بر اساس سه معیار مقدار اطمینان[1]، میزان انحراف[2] و اندازه نزدیکی[3] خوشه‌بندی می‌شوند. به این ترتیب مدل ارائه‌شده با خوشه‌بندی به تشخیص و حذف پیشنهادهای غلط کمک می‌کند و مدل را در برابر **حملات خوب‌گویی** و **بدگویی** مقاوم می‌کند.

در مقاله [19] اعتماد نهایی از ترکیب اعتماد مستقیم و غیرمستقیم با استفاده رابطه (۲۵) حاصل می‌شود. در این رابطه $0 \leq \mu \leq 1$ پارامتر وزن است که به‌صورت پویا انتخاب می‌شود تا الگوریتم در برابر **حملات خوب‌گویی، بدگویی** و **بزرگ نشان‌دادن خود**، مقاوم باشد. در این مدل انتخاب μ به‌گونه‌ای خواهد بود که فاصله بین اعتماد کل و آخرین تجربه کاربر (رابطه ۲۵) را کمینه می‌کند تا الگوریتم در برابر حملات مقاوم باشد.

$$MSE(\mu) = \sum_i \left(\mu.t_{x,i}^{d} + (1-\mu).t_{x,i}^{r} - \overline{f_{x,i}^{(new)}}\right)^2 \qquad (۲۵)$$

[1] Confidence Value
[2] Deviation Value
[3] Closeness Value

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

در مقاله [25] برای مقابله با **حملاتی** نظیر **خوب‌گویی** یا **بدگویی** وقتی از سایر رئوس راجع به یک رأس نظرخواهی می‌شود، نظر پیشنهاددهندگان در مقدار عددی میزان اطمینان خدمت‌دهنده به پیشنهاددهنده ضرب می‌شود که به این ترتیب رأسی که از نظر خدمت‌گیرنده مطمئن‌تر است از اعتبار بیشتری برخوردار است. مقدار عددی اطمینان نسبت به پیشنهاددهنده نیز در این مقاله ترکیبی از میزان اعتماد به پیشنهاددهنده، اعتماد به مالک (مرکزیت و تعداد دوستان مشترک)، قدرت محاسباتی و فاکتور ارتباط است.

در مقاله [58] با تنظیم پارامتر پویای تبعیض، اشیای تبعیض‌گذار تشخیص داده می‌شوند و الگوریتم در برابر حمله **تبعیض اجتماعی و خوب‌گویی و بدگویی** مقاوم است.

مطابق با جدول (۲) اگر در پژوهش‌های پیشین به صراحت اعلام شده باشد که الگوریتم در برابر حمله مقاوم است، از علامت √ استفاده شده و در غیر این‌صورت با اشاره‌نشده (x) علامت‌گذاری شده است. جدول (۲) نشان می‌دهد که مقالات [17]، [22]، [37] و [24] با وزن‌دهی به نظرات مستقیم و غیرمستقیم سعی در مقابله با حملات خوب‌گویی و بدگویی داشته‌اند. مقاله [19] در کنار حملات خوب‌گویی و بدگویی با وزن‌دهی پویا توانسته با حمله خودبزرگ‌نمایی نیز مقابله کند. در مقاله [18] به‌دلیل متمرکزبودن الگوریتم و حفظ کلیه داده‌ها در برابر حملات روشن-خاموش، خدمت فرصت‌طلبانه و بدگویی مقاوم است. در مقاله [21] و [23] خدمت‌دهندگان بد و رئوسی که بازخورد غلط می‌دهند، شناسایی می‌شوند. در مقاله [37] نیز رئوس خودخواه و دسته‌ای از رئوس را که با تبانی شهرت دیگران کم یا زیاد می‌کنند، شناسایی می‌شوند. در مقالات [21]، [18]، [23] و [25] متقلبان شناسایی و تنبیه می‌شوند تا شهرت آن‌ها کاهش پیدا کرده و الگوریتم در برابر حملات مقاوم شود. در [20] فیلترکردن شاهدان به‌وسیله متریک‌های اعتبار، مدل در برابر حملات خودبزرگ‌نمایی، بدگویی و خوب‌گویی مقاوم شده است.

۸- محدودیت‌های عناصر اینترنت اشیا

از آنجایی که عناصر تشکیل‌دهنده شبکه اینترنت اشیا بسیار متنوع هستند و محدودیت‌هایی نظیر انرژی و حافظه دارند، مقالات سعی در ارائه مدل‌های متناسب با محدودیت‌های اشیا کرده‌اند.

۸-۱- آگاهی از موضوع

تنوع ارائه خدمات به‌وسیلهٔ اشیا در شبکه اینترنت اشیا سبب شده است که اعتماد به موضوع وابسته باشد. همان‌طورکه در جدول (۲) نشان داده شده است، مدل‌های [20]، [25] و [49] اعتماد را با آگاهی از موضوع محاسبه می‌کنند.

۸-۲- محدودیت انرژی

در مقاله [18] و [58] میزان انرژی شیء از معیارهای انتخاب نامزد ارائه خدمت در نظر گرفته شده است.

۸-۳- قدرت محاسباتی

در مقالات [21] و [23]، از مفهومی به نام هوش استفاده شده که درواقع قدرت محاسباتی شیء است و براساس فرضیات، هر چه بیشتر باشد توانمندی شیء در ایجاد حملات بیشتر است.

در مقاله [18] قدرت پردازش نیز به‌عنوان معیار انتخاب نامزد ارائه خدمت فرض شده است.

۸-۴- محدودیت فضای حافظه

در مقاله [17] با توجه به اینکه شبکه اینترنت اشیا بسیار وسیع و ناهمگن است، هر رأس فقط مقدار عددی اعتماد تعدادی رأس را که بیشترین اعتماد به آن‌ها دارد، نگهداری می‌کند.

در مقاله [18] یکی دیگر از معیارهای انتخاب نامزد ارائه خدمت میزان حافظه شیء است.

در مقالات [22]، [19] و [25] با درنظرگرفتن این‌که فضای حافظه در عناصر سامانه اینترنت اشیا محدود است از استراتژی مدیریت حافظه استفاده کرده است. وقتی رأس i مقدار اعتماد نسبت به j را محاسبه می‌کند:

- اگر فضای حافظه پر نباشد و یا رأس i با رأس j درقبل تراکنش داشته است، به‌راحتی در فضای حافظه قرار می‌گیرد.
- درصورتی‌که فضای حافظه پر باشد، رأس i مقدار اعتماد نسبت به j را در مکانی از حافظه جایگزین می‌کند که هم از زمان تراکنش آن زمان زیادی گذشته و هم اعتماد آن از نصف کمتر باشد. به‌علاوه وقتی دو رأس با یکدیگر تراکنش انجام می‌دهند، می‌توانند اطلاعات اعتماد ذخیره‌شده خود را به اشتراک بگذارند.

در جدول (۲) محدودیت‌های عناصر اینترنت اشیا که در مدل فرض شده‌اند، با علامت √ در ستون مربوطه نشان داده شده‌اند.

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

۹- روش‌های ارزیابی مدل‌های اعتماد

یکی از مهم‌ترین بخش‌های هر پژوهش، دفاع از عملکرد مدل ارائه‌شده است؛ لذا در این بخش روش‌های مختلف ارزیابی مدل‌های پیشنهادی بیان شده‌اند. در شکل (۴)، این روش‌ها به‌اختصار نمایش داده شده‌اند.

(شکل-۴): روش‌های ارزیابی مدل‌های اعتماد
(Figure-4): Trust evaluation methods

۹-۱- نرخ موفقیت

معیار ارزیابی عملکرد مدل ارائه‌شده در مقالات [21]، [23] و [58] نسبت تعداد تراکنش‌های موفق به تعداد کل تراکنش‌ها است که با عنوان **نرخ موفقیت**[1] از آن نام برده شده است.

۹-۲- سرعت و دقت رسیدن به سطح اعتماد ذاتی[2]

در مقالات [17] و [24] با تغییر ضریب تضعیف اثر زمان، ضریب تأثیر پیشنهادهای غیرمستقیم و افزایش درصد رئوس مخرب؛ **سرعت و دقت رسیدن به سطح اعتماد ذاتی** بررسی شده است.

نتایج در مقاله [22] نشان می‌دهد با وجود این‌که رئوس نمی‌دانند به کدام انجمن علاقمندی تعلق دارند، مقدار عددی اعتماد به سمت توافق انجمن همگرا می‌شود و ارزش واقعی اعتماد برای هر رأس، **سطح اعتماد ذاتی** آن در نظر گرفته شده است.

برای ارزیابی مدل [18] میزان کیفیت یک رأس تصادفی در حضور رئوس مخرب با وجود الگوریتم و بدون آن بررسی شده است. در مرحله بعد برای ارزیابی الگوریتم، **سطح اعتماد** یک رأس با افزایش تعداد تراکنش‌ها در حضور رئوس مخرب و وجود حملات خوب‌گویی، بدگویی و روشن-خاموش بررسی شده است. در این مقاله هدف ارائه سامانه مدیریت اعتماد با قابلیت آگاهی از مفهوم برای اینترنت اشیا است و به دو سؤال ۱) تاریخچه عملکرد داوطلب ارائه خدمت چه بوده است؟ و ۲) برای کدام خدمت مناسب است؟ پاسخ داده می‌شود.

برای بررسی توانمندی، کارآیی و قابلیت اطمینان الگوریتم ارائه‌شده در مقاله [25] شبیه‌سازی در حضور رئوس مخرب صورت گرفته و سطح مطلوب اعتماد برای رأس خوب عدد یک و رأس مخرب عدد صفر فرض شده است. عملکرد پروتکل ارائه‌شده با افزایش تعداد تراکنش‌ها و با مقایسه سرعت و دقت هم‌گرایی الگوریتم به سطح مطلوب مورد بررسی قرار گرفته است.

در مقاله [19] **هم‌گرایی، دقت و انعطاف‌پذیری** پروتکل اعتماد ارائه‌شده در مقابل حملات مخرب مورد بررسی قرار گرفته است. سطوح رضایت کاربر از دریافت خدمت بر اساس یک مجموعه داده واقعی مطابق با مرجع [64] به‌عنوان معیار اعتماد ذاتی در نظر گرفته شده و به این ترتیب هم‌گرایی، دقت و انعطاف‌پذیری الگوریتم در حضور رئوس مخرب (رئوسی که بازخورد غلط می‌دهند) و با تغییر درصد آنها در مقایسه سطح اعتماد ذاتی ارزیابی شده است.

الگوریتم مدیریت اعتماد مقاله [20] در رستوران‌های هوشمند پیاده‌سازی و زمان انتظار سرویس متریک ارزیابی فرض شده است؛ به‌طوری‌که دقت، هم‌گرایی و انعطاف‌پذیری مقدار اعتماد برای یک رأس خوب و بد با گذشت زمان مورد بررسی قرار گرفته است؛ همچنین، زمان انتظار و درصد انتخاب ارائه‌دهندگان خدمت نامطلوب در طول زمان و با سناریوهای مختلف تجزیه و تحلیل شده است.

۹-۳- مقایسه با روش‌های پیشین

مدل‌های اعتماد ذهنی و عینی در مقالات [21] و [23] با مدل ارائه‌شده در مقاله [65] و با معیار نرخ موفقیت مقایسه شده‌اند. در مقاله [19]، مقایسه‌ای بین مدل ارائه‌شده و دو الگوریتم پایه‌ای EigenTrust [66] و Peer-Trust [65] صورت گرفته است. در مقاله [58] نحوه ارتباط اجتماعی کاربران و حرکت آن‌ها نیز از مجموعه‌داده location-based Social Network متعلق به SNAP استخراج شده و یکی از معیارهای ارزیابی این مدل بررسی هم‌گرایی به اعتماد ذاتی و مقایسه آن با مدل‌های پیشین است.

[1] Success Rate
[2] Ground Truth

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

(جدول-۲): مقایسه مقاومت الگوریتم‌ها در مقابل حملات، محدودیت‌های عناصر اینترنت اشیا و روش‌های ارزیابی الگوریتم اعتماد

(Table-2): Comparison of algorithms' resistance to attacks, limitations of IoT elements and methods of evaluating trust algorithms

روش‌های ارزیابی الگوریتم اعتماد	محدودیت‌های عناصر اینترنت اشیا				تنبیه	مقاومت در برابر حملات							منابع
	قدرت محاسبا	انرژی	حافظه	آگاهی از موضوع		سایرین	حمله Sybil	حمله‌ی رفتار متناقض	حمله روشن-خاموش	حمله خدمت فرصت طلبانه	حمله خوب گویی	حمله بدگویی	حمله خودبزرگ نمایی	
نرخ موفقیت	√	×	×	×	√	ارائه خدمت بد، بازخورد منفی	×	×	×	×	×	×	×	[21]
سرعت و دقت رسیدن به سطح اعتماد ذاتی	×	×	×	×	×	---	×	×	×	×	√	√	×	[17]
سرعت و دقت رسیدن به سطح اعتماد ذاتی بین گروهی و داخل گروهی	×	×	√	×	×	---	×	×	×	×	√	√	×	[22]
کیفیت پیشنهادها، سطح اعتماد در حضور حملات	√	√	×	√	√	---	×	×	√	√	×	√	×	[18]
تهدیدات امنیتی برنامه‌های موبایل	×	×	×	×	×	---	×	×	×	×	×	×	×	[49]
نرخ موفقیت	√	×	×	×	√	ارائه خدمت بد، بازخورد منفی	×	×	×	×	×	×	×	[23] ذهنی
	√				×									[23] عینی
توان عملیاتی شبکه و ازدست‌دادن بسته پیشنهادهای تقلبی کشف‌شده، منفی اشتباه و مثبت اشتباه در حضور حملات بدگویی و خوب‌گویی	×	×	×	×	×	رأس خودخواه، تبانی	×	×	×	×	√	√	×	[37]
همگرایی، دقت و انعطاف‌پذیری الگوریتم در رسیدن به ذاتی، اعتماد مقایسه با روش‌های EighenTrust و PeerTrust	×	×	√	×	×	---	×	×	×	×	√	√	√	[19]
همگرایی و دقت الگوریتم در رسیدن به اعتماد ذاتی	×	×	×	×	×	---	×	×	×	×	√	√	×	[24]
همگرایی الگوریتم در رسیدن به اعتماد ذاتی، مقایسه با روش‌های [17] و [22]	√	×	√	√	√	بازخورد غلط، تبانی	×	×	×	×	×	×	×	[25]
سرعت و دقت همگرایی الگوریتم در رسیدن به اعتماد ذاتی برای رئوس خوب و بد، زمان انتظار و درصد سرویس‌های استفاده شده نامطلوب نسبت به زمان	×	×	×	√	---	حمله عدم همکاری و حمله گزارش جعلی	×	×	×	×	√	√	√	[20]
سرعت و دقت همگرایی الگوریتم در رسیدن به اعتماد ذاتی، نرخ موفقیت	×	√	×	√	---	---	×	×	×	√	√	√	√	[58]

۴-۴-۹- پیشنهادهای تقلبی کشف‌شده، منفی اشتباه و مثبت اشتباه

برای ارزیابی فرضیات ارائه‌شده در مقاله [37]، کارآیی مدل در کل شبکه با دو پارامتر توان عملیاتی شبکه و ازدست‌دادن بسته در حضور رئوس مخرب مورد ارزیابی قرار گرفته است.

مقدار اعتماد یک رأس خوب با وجود حمله بدگویی اندازه‌گیری می‌شود تا اثر حمله در حضور الگوریتم و بدون آن بررسی شود. مقدار اعتماد یک رأس بد با وجود حمله خوب‌گویی اندازه‌گیری می‌شود تا نشان داده شود چگونه حمله‌کنندگان می‌توانند مقدار اعتماد این رأس را تحریف کنند. کارآیی مدل ارائه‌شده با معیارهای **پیشنهادهای تقلبی کشف‌شده، منفی اشتباه و مثبت اشتباه** در حضور حملات بدگویی و خوب‌گویی بررسی شده است.

۵-۹- پیاده‌سازی برروی کاربردهای اینترنت اشیا

در مقاله [49] برای آزمایش و آزمون الگوریتم، شش عدد برنامه کاربردی موبایل انتخاب و مصادیقی از محرمانگی شامل IMEI[1]، محتویات پیام کوتاه، پیام چندرسانه‌ای، فهرست تماس‌ها، موقعیت‌ها، اطلاعات سیم‌کارت، دفتر

[1] International Mobile Equipment Identity

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

تلفن و وقایع ثبت‌شده سامانه درنظر گرفته شده‌اند. برنامه‌های مورد نظر به برخی از این اطلاعات محرمانه دسترسی دارند که در الگوریتم با عنوان حمله مخرب نام‌گذاری شده‌اند. پس از اجرای الگوریتم، قابل اعتمادترین برنامه مشخص و نیز نشان داده شده که بیشترین حمله با درصد ۸۱٪/۱۴ به IMEI صورت گرفته است و باید کاربران نسبت به سوء استفاده برنامه‌ها از این ویژگی هوشیار باشند. معیارهای بیان‌شده به‌اختصار در جدول (۲) نشان داده شده‌اند.

۶-۹- استخراج معیارها و ارائه روش‌های عددی با هدف ارزیابی الگوریتم‌های اعتماد با تکیه بر مفهوم استحکام

از آنجایی که بررسی صحت عملکرد الگوریتم‌های مدیریت اعتماد در اینترنت اشیا ضروری است، در این بخش با معرفی معیارهای عددی، شیوه‌هایی برای مقایسه کمی الگوریتم‌های محاسبه اعتماد ارائه خواهد شد. برای رسیدن به این هدف دو الگوریتم [23] (Nitti et.al) و [19] (Ing-Ray et.al) برای شبیه‌سازی انتخاب شده‌اند و سپس با معیارهایی که در ادامه به آن‌ها اشاره خواهدشد، مقایسه می‌شوند. علت انتخاب این دو مقاله شباهت‌هایی است که مقایسه این دو مدل را امکان‌پذیر ساخته و از طرفی با استفاده از تفاوت‌های موجود در محاسبه اعتماد، علاوه‌بر ارائه روش عددی مقایسه، برتری‌های این دو مدل نسبت به یکدیگر آشکار خواهد شد. در جداول (۱ و ۲) شباهت‌ها و تفاوت‌های این دو مدل از منظر نحوه محاسبه اعتماد و مقابله در برابر حملات نشان داده شده است.

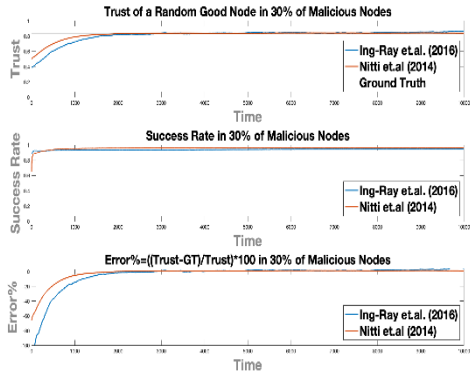
نرم افزار شبیه‌سازی متلب انتخاب شده است و در جدول (۳) پارامترهای مفروض در شبیه‌سازی شبکه اینترنت اشیا مفروض نشان داده شده‌اند.

در این شبیه‌سازی دویست رأس متعلق به چهل کاربر، در فضای مربعی که به ۲۵۶ مربع یکسان تقسیم شده است، مطابق با الگوریتم حرکتی SWIM در حرکت هستند. گراف دوستی بین صاحبان اشیا مطابق با الگوریتم مستقل از مقیاس باراباسی-آلبرت ایجاد شده است که درجه رئوس از توزیع power-law پیروی می‌کند. گذشت زمان در این مدل به مفهوم سپری‌شدن زمان بر حسب ثانیه نیست و به این معنی است که در هر بازه زمانی ۲۰٪ از رئوس قابلیت تراکنش و یا به عبارتی توانایی ارائه و دریافت خدمت دارند. اشیا در این مدل توان محاسباتی متفاوت دارند، محاسبات و ذخیره داده‌های اشیای هر کاربر می‌تواند توسط یکی از اشیا با توان محاسباتی بالا نظیر تلفن همراه، تبلت یا لپ‌تاپ انجام و با سایر اشیای متعلق به کاربر به اشتراک گذاشته شود. رئوس مخرب با حملات خوب‌گویی و بدگویی در مراحل مختلف شبیه‌سازی ۳۰٪، ۵۰٪ و ۷۰٪ کل رئوس شبکه را شامل می‌شوند. کلیه شبیه‌سازی‌ها پنجاه مرتبه تکرار شده‌اند و زمان پایداری الگوریتم ده‌هزار بازه زمانی درنظر گرفته شده است.

(جدول-۳): پارامترهای شبیه‌سازی
(Table-3): Simulation parameters

پارامتر	مقدار
تعداد کاربران	۴۰
الگوریتم دوستی کاربران	باراباسی-آلبرت
تعداد اشیا	۲۰۰
تقسیم‌بندی مکانی	۱۶*۱۶
الگوریتم حرکت	SWIM
نوع حمله	خوب‌گویی و بدگویی
درصد رئوس مخرب	۳۰٪ و ۵۰٪
زمان نهایی	۱۰،۰۰۰
تکرار مونت کارلو	۵۰

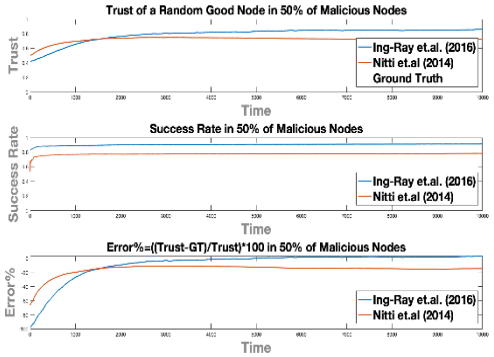
شکل (۵) سرعت و دقت رسیدن به اعتماد ذاتی یک رأس خوب تصادفی، نرخ موفقیت و درصد خطا را در حضور ۳۰٪ رئوس مخرب نشان می‌دهد. شکل (۵) نشان می‌دهد که در حضور ۳۰٪ رئوس مخرب الگوریتم [23] عملکرد بهتری دارد؛ به‌طوری‌که سرعت و دقت رسیدن به اعتماد ذاتی بهتر، نرخ موفقیت بیشتر و خطای الگوریتم نیز کمتر است.



(شکل-۵): مقایسه دو مدل در حضور ۳۰٪ رأس مخرب
(Figure-5): Comparion of two models with 30% of malicious nodes

شکل (۶) نیز همین شبیه‌سازی‌ها را با حضور ۵۰٪ رئوس مخرب نشان می‌دهد. با این تفاوت که نتایج شبیه‌سازی نشان می‌دهد الگوریتم [19] در حضور ۵۰٪ از رئوس مخرب عملکرد بهتری دارد.

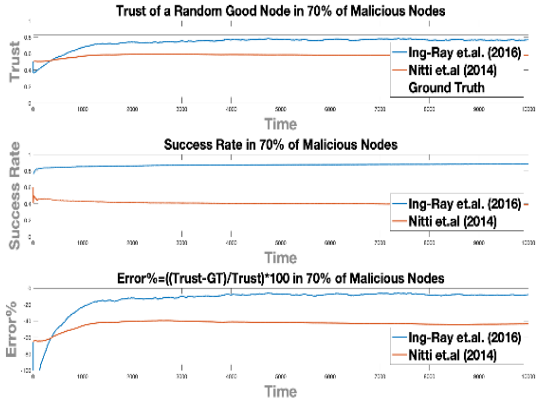
[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]



(شکل-۶): مقایسه دو مدل در حضور ۵۰٪ رأس مخرب

(Figure-6): Comparion of two models with 50% of malicious nodes

در شکل (۷) درصد رئوس مخرب به ۷۰٪ رسیده است. نتایج نشان می‌دهد که هر دو مدل در برابر حملات نودهای مخرب تاب‌آوری خود را از دست داده و به اعتماد ذاتی نمی‌رسند، درحالی که باز هم الگوریتم [19] بهتر عمل می‌کند.



(شکل-۷): مقایسه دو مدل در حضور ۷۰٪ رأس مخرب

(Figure-7): Comparion of two models with 70% of malicious nodes

جدول (۴) با هدف مقایسه این دو الگوریتم از زمان شروع تا انتهای شبیه‌سازی ارائه شده است. با توجه به مرجع [64] اعتماد ذاتی رأس خوب تصادفی ۰/۸۳ درنظرگرفته شده است؛ بنابراین یکی از روش‌های مقایسه دو مدل بررسی زمان رسیدن به این مقدار است. جدول (۴) نشان می‌دهد که الگوریتم [23] با درصد رئوس مخرب پایین‌تر زودتر به این مقدار همگرا می‌شود؛ درحالی‌که با بالارفتن درصد رئوس مخرب تا پایان زمان شبیه‌سازی همگرا نمی‌شود؛ به‌علاوه اعداد جدول (۴) کاهش عملکرد هر دو الگوریتم را با افزایش حملات به‌خوبی نشان می‌دهد، هرچند که الگوریتم [19] با افزایش حملات از [23] عملکرد بهتری دارد. مقایسه مقادیر نهایی در هر دو مدل گواه این نتیجه‌گیری است. (با هدف سهولت در مقایسه، عملکرد بهتر در جداول به‌صورت خانه‌های حاشیه‌دار نمایش داده شده‌اند.)

(جدول-۴): نتایج کمی حاصل از شبیه‌سازی

(Table-4): Quantitive simulation results

زمان رسیدن به اعتماد ذاتی			
درصد رئوس مخرب	٪۳۰	٪۵۰	٪۷۰
Ing-Ray et.al.	۲۸۳۱	۴۹۳۱	---
M. Nitti	۱۹۳۵	---	---
خطای میانگین مربعات اعتماد			
Ing-Ray et.al.	۰/۰۸۶۷	۰/۱۰۳۶	۰/۱۱۷۸
M. Nitti	۰/۰۵۴۹	۰/۱۱۳۹	۰/۲۵۲۴
مقدار نهایی اعتماد، (t=10000)			
Ing-Ray et.al.	۰/۸۶	۰/۸۳۲۸	۰/۷۷
M. Nitti	۰/۸۴۰۴	۰/۷۲۵۸	۰/۵۷۸۴
مقدار نهایی نرخ موفقیت، (t=10000)			
Ing-Ray et.al.	۰/۹۴۴۷	۰/۹۱۱۹	۰/۸۸۱۳
M. Nitti	۰/۹۶۴۷	۰/۷۸۳۹	۰/۳۹۰۵
مقدار نهایی خطا، (t=10000)			
Ing-Ray et.al.	۳/۴۸۸۴٪	۴/۸۸۸۴٪	-۷/۷۹۲۲٪
M. Nitti	۱/۲۳۲۳٪	۱۴/۳۶۳۴٪	-۴۳/۵۰۳۵٪

در ادامه مقایسه، زمان شبیه‌سازی به دو حالت گذرا و پایدار تقسیم می‌شود. به این ترتیب که از ابتدا تا رسیدن به اعتماد ذاتی، زمان گذرا و پس از آن زمان پایدار الگوریتم در نظر گرفته می‌شود و مقایسه عددی این دو الگوریتم در زمان پایداری در جدول (۵) نشان داده شده است. هدف از این مقایسه آن بررسی پایداری الگوریتم بعد از رسیدن به اعتماد ذاتی است، نکته‌ای که در پژوهش‌های گذشته به آن توجهی نشده بود.

جدول (۵) نشان می‌دهد زمانی که درصد رئوس مخرب ۳۰٪ باشد الگوریتم [23] خطای کمتری دارد، درحالی‌که با افزایش درصد حملات، به پایداری نمی‌رسد و بنابراین اعدادی برای مقایسه وجود نخواهد داشت. با درنظرگرفتن جداول (۱ و ۲) (ویژگی‌های دو مدل) و نتایج عددی حاصل از شبیه‌سازی‌های ارائه‌شده در جداول (۴ و ۵) نکاتی حاصل می‌شود که به‌کمک آن می‌توان ضعف‌ها و برتری‌های الگوریتم‌ها را نسبت به یکدیگر سنجید و برای ارائه مدل بهتر مدنظر قرار داد.

الگوریتم [23]، برای محاسبه اعتماد، نظر کلیه رئوسی را که با معتمد تراکنش داشته‌اند را ترکیب وزن‌دار می‌کند؛ درحالی‌که در مدل [19] نظر تعدادی از دوستان که بیشترین شباهت به معتمد دارند به‌صورت وزن‌دار با یکدیگر ترکیب می‌شوند. با توجه به نتایج شبیه‌سازی،

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

جمع‌آوری نظرات کلیه پیشنهاددهندگان تا زمانی که رئوس مخرب ۳۰٪ و کمتر باشد بهتر عمل می‌کند.

درحالی‌که با بالا رفتن درصد رئوس مخرب فیلتر کردن نظراتی که با یکدیگر ترکیب می‌شوند اهمیت دارد؛ به همین دلیل است که الگوریتم [19] در حضور ۵۰٪ از رئوس مخرب بعد از ۴۹۳۱ ثابت زمانی به اعتماد ذاتی می‌رسد. هرچند رسیدن به اعتماد ذاتی با افزایش رئوس مخرب تا ۷۰٪ در هر دو الگوریتم حتی تا انتهای زمان پایداری رخ نمی‌دهد. با وجود اینکه هر دو مدل اثر گذشت زمان را در محاسبه اعتماد در نظر گرفته‌اند، ترکیب نظرات مستقیم و غیرمستقیم در مدل [23] ترکیب وزن‌دار با ضرایب ثابت فرض شده است، درحالی‌که الگوریتم [19] با حداقل‌کردن خطای میانگین مربعات (رابطه ۲۵) وزن ترکیب را به‌صورت پویا محاسبه می‌کند. به این ترتیب برای مقابله با حملات نحوه انتخاب و ترکیب پیشنهاددهندگان اهمیت زیادی دارد.

(جدول-۵): نتایج کمی حالت پایدار

(Table-5): Quantitive steady state simulation resuls

زمان رسیدن به اعتماد ذاتی		
درصد رئوس مخرب	٪۳۰	٪۵۰
Ing-Ray et.al.	۲۸۳۱	۴۹۳۱
M. Nitti	۱۹۳۵	---
خطای میانگین مربعات اعتماد از زمان رسیدن به اعتماد ذاتی تا انتهای زمان		
Ing-Ray et.al.	۰/۰۱۵۸	۰/۱۰۳۶
M. Nitti	۰/۰۰۹۶	---
میانگین اعتماد از زمان رسیدن به اعتماد ذاتی تا انتهای زمان		
Ing-Ray et.al.	۰/۸۴۴۲	۰/۸۴۶۴
M. Nitti	۰/۸۳۹۳	---
انحراف معیار اعتماد از رسیدن به اعتماد ذاتی تا انتهای زمان شبیه‌سازی		
Ing-Ray et.al.	۰/۰۰۷	۰/۰۰۵۱
M. Nitti	۰/۰۰۲۵	---
میانگین خطا از زمان رسیدن به اعتماد ذاتی تا انتهای زمان شبیه‌سازی		
Ing-Ray et.al.	۱/۶۷۳۲٪	۱/۹۳۶۹٪
M. Nitti	۱/۱۰۴۱٪	---
انحراف معیار خطا از زمان رسیدن به اعتماد ذاتی تا انتهای زمان شبیه‌سازی		
Ing-Ray et.al.	۰/۸۱۵۹	۰/۵۹۷
M. Nitti	۰/۲۹۷۲	---

در ادامه، با هدف بررسی استحکام الگوریتم در برابر درصد حملات خوب‌گویی و بدگویی جدول (۶) و نمودار شکل (۸) ارائه شده است.

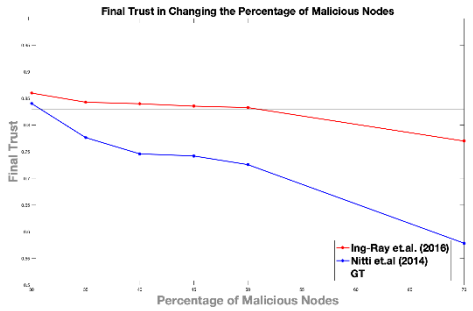
نمودار شکل (۸) مقایسه‌ای از اعتماد نهایی الگوریتم‌ها را با تغییر درصد رئوس مخرب نشان می‌دهد.

درصورتی‌که استحکام الگوریتم اعتماد در برابر حملات، رسیدن مقدار نهایی اعتماد به اعتماد ذاتی تعریف شود، استحکام الگوریتم [19] تا رسیدن رئوس مخرب به ۵۰٪، درحالی‌که این معیار برای مدل [23]، ۳۰٪ است.

(جدول-۶): مقدار نهایی اعتماد با تغییر درصد رئوس مخرب

(Table-6): Final trust values by changing malicious nodes range

مقدار نهایی اعتماد، (t=10000)		
درصد رئوس مخرب	Ing-Ray et.al.	M. Nitti
٪۳۰	۰/۸۶	۰/۸۴۰۴
٪۳۵	۰/۸۴۲۹	۰/۷۷۶۵
٪۴۰	۰/۸۴۰۰	۰/۷۴۶۰
٪۴۵	۰/۸۳۵۴	۰/۷۴۲۰
٪۵۰	۰/۸۳۲۸	۰/۷۲۵۸
٪۷۰	۰/۷۷	۰/۵۷۸۴



(شکل-۸): نمودار مقدار نهایی اعتماد نسبت به درصد رئوس مخرب

(Figure-8): Diagram of the final trust values of malicious nodes

۱۰- نتیجه‌گیری و پیشنهادها

تا به امروز پژوهش‌های محدودی در زمینهٔ محاسبهٔ اعتماد در محیط اینترنت اشیا برای تقویت امنیت انجام شده است؛ لذا در این پژوهش تلاش شد مهم‌ترین و معتبرترین مقالات چاپ شده که در ارائه مدل شباهت کمتری به یکدیگر دارند مورد بررسی قرار گیرند. مدل‌های انتخاب‌شده از چهار منظر ۱) متریک‌های عددی محاسبه اعتماد، ۲) روش‌های تجمیع آرا و مقاومت در برابر حملات، ۳) روش‌های ارزیابی الگوریتم اعتماد و ۴) محدودیت‌های اشیا مورد توجه قرار گرفتند؛ پس با ارائه معیارهایی برای ارزیابی مدل اعتماد سعی شد امکان تحلیل و ارزیابی روش‌های مطرح شده فراهم شود. با هدف مقایسه، علاوه‌بر طبقه‌بندی مدل‌ها در همه جوانب یادشده، خلاصه‌ای از عملکرد مدل‌ها در دو جدول (۱ و ۲) به‌خوبی ارائه شده است. در انتها نیز با هدف ارائه معیارهای متریکی ارزیابی و مقایسه الگوریتم‌های اعتماد،

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]
[DOI: 10.52547/jsdp.18.2.3]

دو مدل مشهور و شناخته‌شده شبیه‌سازی، ارزیابی و مقایسه شد.

بررسی کلیه مقالات و نتایج شبیه‌سازی نشان می‌دهد، پارامترهای اشاره‌شده شامل نحوه به‌روزرسانی داده‌ها با گذشت زمان، فیلترکردن پیشنهاددهندگان، ترکیب نظرات پیشنهاددهندگان با ضرایب پویا و تنبیه و تشویق پیشنهاددهندگان در استحکام الگوریتم در برابر حملات رئوس مخرب بسیار مؤثر است. با درنظرگرفتن زمان رسیدن الگوریتم به اعتماد ذاتی به‌عنوان زمان گذرا و پس از آن زمان پایداری، می‌توان عملکرد الگوریتم‌ها را با معیارهای آماری نظیر میانگین، انحراف معیار و میانگین خطای میانگین مربعات مقایسه کرد.

در ادامه پیشنهاد می‌شود، محتوا یا زمینه در محاسبات دخیل شود؛ به‌طوری‌که مقدار آستانه قابل اعتماد برای رئوس در خدمات مختلف متفاوت باشد. همچنین پارامترهایی نظیر ویژگی‌های اجتماعی و محدودیت‌های اشیا نیز به شبیه‌سازی‌ها اضافه، تا عملکرد الگوریتم‌ها با تغییر این پارامترها نیز بررسی شود. به‌علاوه مقاومت الگوریتم‌ها در برابر حملاتی نظیر حمله روشن-خاموش و تبانی نیز باید مورد بررسی قرار گیرد.

ازآن‌جایی‌که شبکه اینترنت اشیا پیوسته با مشکل پیوستن و جداشدن رئوس مواجه است، پروتکل مدیریت اعتماد باید این موضوع را در نظر بگیرد که در صورت اضافه‌شدن و یا حذف‌شدن رأسی بتواند با سرعت و دقت اعتماد را دوباره محاسبه کند و به‌عبارتی انعطاف‌پذیری الگوریتم در برابر این تغییرات نیز می‌تواند به‌عنوان یک معیار مورد بررسی قرار گیرد.

تقدیر و سپاس‌گزاری

این پژوهش تحت حمایت صندوق حمایت از پژوهش‌گران و فناوران کشور (INSF) در قالب طرح پژوهشی مصوب به شماره ۹۶۰۰۳۲۹۱ انجام شده است.

۱۱- مراجع 11- References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Comput.Syst.*, vol. 29, pp. 1645-1660,9, 2013.

[2] H. Sundmaeker, P. Guillemin, P. Friess and S. Woelfflé, "Vision and challenges for realising the Internet of Things," in *Cluster of European Research Projects on the Internet of Things—CERP IoT*, 2010.

[3] X. Li, R. Lu, X. Liang, X. Shen, J. Chen and X. Lin, "Smart community: an internet of things application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68-75, 2011.

[4] M. K. Geir, "Reflections on trust in devices: an informal survey of human trust in an internet-of-things context," *Wireless Personal Communications*, vol. 61, no. 3, pp. 495-510, 2011.

[5] T. Eder, D. Nachtmann and D. Schreckling, "Trust and Reputation in the Internet of Things," *Universit ̈at Passau, Tech. Rep.*, 2013.

[6] Z. Yan, P. Zhang and A. V. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications* , vol. 42, pp. 120-134, June 2014.

[7] S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer networks*, vol. 76, pp. 146-164, 2015.

[8] V. Suryani and and others, "A survey on trust in Internet of Things," in *Information Technology and Electrical Engineering (ICITEE), 2016 8th International Conference on*, 2016.

[9] W. Abdelghani, C. A. Zayani, I. Amous and F. Sèdes, "Trust management in social internet of things: a survey," in *Conference on e-Business, e-Services and e-Society*, 2016.

[10] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," vol. 16, no. 1, pp. 414-454, 2014.

[11] J. Guo, R. Chen and J. J. Tsai, "A survey of trust computation models for service management in internet of things systems," *Computer Communications*, vol. 97, pp. 1-14, 2017.

[12] Elizabeth J.Chang, Farookh Khadeer Hussain and Tharam S. Dillon , "Fuzzy Nature of Trust and Dynamic Trust Modeling in Service Oriented Environments," in *Proceedings of the 2005 workshop on Secure web services. ACM*, 2005.

[13] M. Blaze, J. Feigenbaum and J. Lacy, "Decentralized trust management," in *Security and Privacy, 1996. Proceedings, 1996 IEEE Symposium on*, 1996.

[14] A. Josang, C. Keser and T. Dimitrakos, "Can we manage trust?," in *iTrust*, 2005.

[15] S. Chaeikar, M. Alizadeh, M. Tadayon and A. Jolfaei, "An intelligent cryptographic key management model for secure communications in distributed industrial intelligent systems," *International Journal of Intelligent Systems, DOI:10.1002/int.22435*, 25 April 2021.

[16] D.Chen, G.Chang, D.Sun, J.Li, J.Jia and X.Wang, "TRM-IoT:A trust management model based on fuzzy reputation for Internet

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

"Two-way acknowledgment-based trust framework for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 5, p. 952905, 2013.

[29] S. Bhattacharya and A. Ghosh, "Entropy Trust based Approach against IP spoofing attacks in network," *International Journal of Computer Applications*, vol. 67, no. 23, 2013.

[30] R. A. Raje and A. V. Sakhare, "Routing in wireless sensor network using fuzzy based trust model," in *2014 Fourth International Conference on Communication Systems and Network Technologies*, 2014.

[31] Y. Gao and W. Liu, "BeTrust: a dynamic trust model based on bayesian inference and tsallis entropy for medical sensor networks," *Journal of Sensors*, vol. 2014, 2014.

[32] T. Yang, X. Xiangyang, L. Peng, L. Tonghui and P. Leina, "A secure routing of wireless sensor networks based on trust evaluation model," *Procedia computer science*, vol. 131, pp. 1156-1163, 2018.

[33] O. AlFarraj, A. AlZubi and A. Tolba, "Trust-based neighbor selection using activation function for secure routing in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-11, 2018.

[34] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothunganx, H. K. Nehemiah and A. Kannan, "An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1475-1490, 2019.

[35] W. Fang, W. Zhang, W. Chen, Y. Liu and C. Tang, "TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing," *Wireless Networks*, pp. 1-14, 2019.

[36] A. Alnasser and H. Sun, "A fuzzy logic trust model for secure routing in smart grid networks," *IEEE access*, vol. 5, pp. 17896-17903, 2017.

[37] Sh. M. Antesar, P. Keshav Dahal, S. K. Bista and I. U. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Transactions on Mobile Computing*, vol. 14, no. 10, pp. 2101-2115, 2015.

[38] V. V. Sarbhukan and L. Ragha, "Establishing Secure Routing Path Using Trust to Enhance Security in MANET," *Wireless Personal Communications*, vol. 110, no. 1, pp. 245-255, 2020.

[39] L. Wenjia, S. Houbing and Z. Feng, "Policy-based secure and trustworthy sensing for internet of things in smart cities," *IEEE Internet of Things Journal*, 27 jun 2017.

[40] X. Xu, X. Liu, Z. Xu, F. Dai, . X. Zhang and L. Qi, "Trust-oriented IoT service placement for smart cities in edge computing," vol. 7, no. of things," *Comput. Sci. Inf. Syst.*, vol. 8, pp. 1207-1228, 2011.

[17] F. Bao and I.-R. Chen, "Dynamic trust management for internet of things applications," in *Proceedings of the 2012 international workshop on Self-aware internet of things*, San Jose, California, USA, 2012.

[18] S. Yosra Ben, O. Alexis, Z. Djamal and L. Maryline, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," *Computer and Security*, vol. 39, pp. 351-365, 2013.

[19] C. Ray, F. Bao and J. Guo, "Trust management for SOA-based IoT and its application to service composition," *IEEE Transactions on Services Computing*, vol. 9, no. 3, pp. 482-495, 2016.

[20] H. Al-Hamadi, R. Chen and J.-H. Cho, "Trust management of smart service communities," *IEEE Access*, vol. 7, pp. 26362-26378, 2019.

[21] M. Nitti, R. Gira, L. Atzori, A. Iera and G. Morabito, "A subjective model for trustworthiness evaluation in the social Internet of Things," in *Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on*, 2012.

[22] B. Fenye, R. Chen and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based internet of things systems," in *Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on* , 2013.

[23] M. Nitti, R. Girau and L. Atzori, "Trustworthiness Management in the Social Internet of Things," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 26, pp. 1253-1266, 2014.

[24] Chen, Ray, Fenye Bao and Jia Guo, "Trust-based service management for social internet of things systems," *IEEE transactions on dependable and secure computing*, vol. 13, no. 6, pp. 684-696, 2016.

[25] R. Sherif Emad Abdel, A. Ayman and E. Mohamad Abou, "CBSTM-IoT: Context-based social trust model for the Internet of Things," in *Selected Topics in Mobile & Wireless Networking (MoWNeT), 2016 International Conference on*, 2016.

[26] D. Airehrour, J. Gutierrez and S. K. Ray, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things," *Future Generation Computer Systems*, vol. 93, pp. 860-876, 2019.

[27] A. Tandon and P. Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT," in *2019 Twelfth International Conference on Contemporary Computing (IC3)*, 2019.

[28] X. Anita, L. M. Martin and M. A. Bhagyaveni,

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

[51] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers and Security*, vol. 78, pp. 126-142, 2018.

[52] N. Ghosh, S. Chandra, V. Sachidananda and Y. Elovici, "SoftAuthZ: A Context-Aware, Behavior-Based Authorization Framework for Home IoT," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10773-10785, 2019.

[۵۳] جانبابایی شادی، قرائی حسین، محمدزاده ناصر، "ارائه طرح احراز اصالت سبک با قابلیت گمنامی و اعتماد در اینترنت اشیا"، پردازش علائم و داده‌ها، ۱۵ (۴)، ۱۱۱-۱۲۲، ۱۳۹۷.

[53] S. Janbabaei, H. Gharaee and N. Mohammadzadeh, "The Lightweight Authentication Scheme with Capabilities of Anonymity and Trust in Internet of Things (IoT)," *Signal and Data Processing*, vol. 15, no. 4, pp. 111-122, 2019.

[54] L. Jun, S. Zhiqi and M. Chunyan, "Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT," in *Proceedings of the 2nd International Conference on Crowd Science and Engineering*, 2017.

[55] B. Wen, Z. Luo and Y. Wen, "Evidence and Trust: IoT Collaborative Security Mechanism," in *2018 Eighth International Conference on Information Science and Technology (ICIST)*, 2018.

[56] M. Zhaofeng, W. Lingyun, W. Xiaochang, W. Zhen and Z. Weizhe, "Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4000-4015, 2019.

[57] S. Guo, Y. Dai, S. Xu, X. Qiu and F. Qi, "Trusted cloud-edge network resource management: Drl-driven service function chain orchestration for IoT," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6010-6022, 2020.

[58] B. Jafarian, N. Yazdani and M. Sayad Haghighi, "Discrimination-aware trust management for social internet of things," *Computer Networks*, vol. 178, p. 107254, 2020.

[59] B. Fenye and R. Chen, "Trust management for the internet of things and its application to service composition," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, 2012.

[60] L. Qinghua, S. Zhu and G. Cao, "Routing in socially selfish delay tolerant networks," in *NFOCOM, 2010 Proceedings IEEE*, 2010.

[61] L. Atzori, A. Iera and G. Morabito, "SIoT: 5, pp. 4084-4091, 2019.

[41] J. Guo, I.-R. Chen, D.-C. Wang, J. J. Tsai and H. Al-Hamadi, "Trust-based iot cloud participatory sensing of air quality," *Wireless Personal Communications*, vol. 105, no. 4, pp. 1461-1474, 2019.

[42] G. C. Karmakar, R. Das and J. Kamruzzaman, "IoT Sensor Numerical Data Trust Model Using Temporal Correlation," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2573-2581, 2019.

[43] Z. Liu, J. Weng, J. Ma, J. Guo, B. Feng, Z. Jiang and K. Wei, "TCEMD: A Trust Cascading-Based Emergency Message Dissemination Model in VANETs," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4028-4048, 2019.

[44] A. Alnasser, H. Sun and J. Jiang, "Recommendation-based Trust Model for Vehicle-to-Everything (V2X)," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 440-450, 2019.

[45] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang and D. Wu, "TROVE: A Context Awareness Trust Model for VANETs Using Reinforcement Learning," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6647-6662, 2020.

[46] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain and F. Hussain, "MARINE: Man-in-the-middle Attack Resistant trust model IN connEcted vehicles," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3310-3322, 2020.

[۴۷] نصیری سمیه، صدوقی فرحناز، تدین محمدحسام، دهناد افسانه، "مکانیسم‌های امنیت و حریم خصوصی اینترنت اشیا در صنعت مراقبت سلامت و غیرسلامت"، *مدیریت سلامت*، ۲۲ (۴)، ۱۰۵-۸۶، ۱۳۹۸.

[47] S. Nasiri, F. Sadoughi, M. H. Tadayon and A. Dehnad, "Security and privacy mechanisms of Internet of things in healthcare and non-healthcare industry," *Journal of Health Administration*, vol. 22, no. 4, 2019.

[48] S. Nasiri, F. Sadoughi, M. H. Tadayon and A. Dehnad, "Security requirements of internet of things-based healthcare system: a survey study," *Acta Informatica Medica*, vol. 27, no. 4, p. 253, 2019.

[49] K. Kang, , Z. Pang, , L. Da Xu, , L. Ma, and C.Wang, "An interactive trust model for application market of the internet of things," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1516-1526, 2014.

[50] H. Al-Hamadi and I.-R. Chen, "Trust-based decision making for health IoT systems," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1408-1419, 2017.

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

Giving a Social Structure to the Internet of Things," *EEE Communications Letters*, vol. 15, no. 11, pp. 1193 - 1195, 13 10 2011.

[62] Y.L. Sun, Z. Han, W. Yu and K.J.R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications*, 2006.

[63] F. Bao, I. Chen and J. Guo, "Scalable, adaptive and survivable trust management for community of interest based Internet of Things systems," in *Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on*, 2013.

[64] Z. Zibin, Y. Zhang and M. R. Lyu, "Investigating QoS of real-world web services," *IEEE Transactions on Services Computing*, vol. 1, pp. 32-39, Jan 2014.

[65] X. Li and L. Liu, "Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities," *IEEE transactions on Knowledge and Data Engineering*, vol. 7, Jul 2004.

[66] K. Sepandar D, M. T. Schlosser and H. G. Molina, "The eigentrust algorithm for reputation management in p2p networks," in *Proceedings of the 12th international conference on World Wide Web*, 2003.

مریم ابراهیمی دانشجوی مخابرات مقطع دکترا در پژوهشگاه ارتباطات و فناوری اطلاعات است. زمینه‌های پژوهشی مورد علاقه وی اینترنت اشیا و مدیریت اعتماد در اینترنت اشیا است.

نشانی رایانامه ایشان عبارت است از:

m.ebrahimi@itrc.ac.ir

محمدحسام تدین در حال حاضر دانشیار پژوهشگاه ارتباطات و فناوری اطلاعات و دارای سابقه راهنمایی پایان‌نامه‌ها و رساله‌های متعدد دانشجویان کارشناسی ارشد و دکترا است. وی سابقه مدیریت گروه پژوهشی، معاونت پژوهشکده، مشاوره به سازمان‌ها و شرکت‌ها و مجری‌گری پروژه‌های متعدد پژوهشی در حوزه امنیت اطلاعات و داده‌ها را در کارنامه خود دارد. ایشان همچنین عضو کمیته‌های علمی مختلف کنفرانس‌های معتبر و علاقه‌مند به موضوعات امنیت اطلاعات و داده‌ها، اینترنت اشیا و سامانه‌های هوشمند است.

نشانی رایانامه ایشان عبارت است از:

tadayon@itrc.ac.ir

محمد صیاد حقیقی در حال حاضر استادیار و مدیر گروه فناوری اطلاعات در دانشکده مهندسی برق و کامپیوتر دانشگاه تهران است. پیش از آن، وی استادیار در مرکز تحقیقات مخابرات ایران بود و دوره پسادکترای خود را در دانشگاه دیکن استرالیا در سال‌های ۲۰۱۲ و ۲۰۱۳ گذرانده‌اند. ایشان در کمیته‌های فنی و برگزارکننده کنفرانس‌هایی مانند IEEE DependSys, ACDC, IEEE LCN, IEEE SICK, WNS CSS, و IST حضور داشته‌اند و هم‌چنین در صنایعی همچون شرکت‌های مخابراتی، بانک‌ها و حتی سازمان‌های دولتی تا سطح مشاور ارشد و استراتژیست نیز کار کرده‌اند. ایشان عضو ارشد IEEE و رئیس لابراتوار ANSLab (Advanced Networking and Security research Laboratory) هستند.

نشانی رایانامه ایشان عبارت است از:

sayad@ut.ac.ir

[Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]

[DOI: 10.52547/jsdp.18.2.3]

[DOI: 10.52547/jsdp.18.2.3] [Downloaded from jsdp.rcisp.ac.ir on 2026-02-04]