

الگوریتم‌های اعتماد در اینترنت اشیا: بررسی،

تحلیل و ارائه معیارهای ارزیابی



مریم ابراهیمی^۱، محمد حسام تدین^{۲*} و محمد صیاد حقیقی^۳

^۱پژوهشگاه ارتباطات و فناوری اطلاعات،

آموزشکده فنی و حرفه‌ای سما تهران، دانشگاه آزاد اسلامی، واحد تهران

^۲پژوهشگاه ارتباطات و فناوری اطلاعات،

^۳دانشکده 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 اشیا 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 علاوه بر این که 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 اشیا 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 اشیا اجتماعی، ارزیابی اعتماد

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

Maryam Ebrahimi¹, Mohammad Hesam Tadayon^{2*} & Mohammad Sayad Haghighi³

¹Iran Telecommunication Research Center, Iran,

Sama Technical and Vocational Training College, Islamic Azad University, Iran.

²Iran Telecommunication Research Center, Iran

³School 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

* نویسنده عهده‌دار مکاتبات

سال ۱۴۰۰ شماره ۲ پیاپی ۴۸

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

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 اشتراک گذاشتن 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]. اشیای 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 جمع‌آوری شده 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 سامانه 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]، علاوه بر بررسی اعتماد در حوزه اینترنت اشیا، برخی از چالش‌های پژوهشی با موضوع

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 علاوه بر این که پژوهش‌های چاپ شده 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 علاوه بر مقایسه طبقه‌بندی شده از پژوهش‌های موجود، ارزیابی کمی به همراه شبیه‌سازی مقایسه‌ای از دو مقاله را ارائه کرده است؛ به طوری که این دسته‌بندی و مقایسه در هیچ یک از ادبیات مروری مشاهده نمی‌شود. در این مقاله اقدامات انجام شده 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 علاوه بر طرح روش‌های ارزیابی اعتماد، معیارهای عددی با هدف مقایسه الگوریتم‌های محاسبه اعتماد ارائه و سپس دو مقاله شناخته شده در این حوزه شبیه‌سازی شده و نتایج حاصل مورد بررسی قرار گرفته است. بخش انتهایی نیز نتیجه‌گیری و پیشنهادها را شامل می‌شود؛ به علاوه مقایسه کلیه موارد بیان شده 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 به دلیل طبیعت فازی، پویایی و پیچیدگی اعتماد است. مفهوم فازی به معنی ناشناخته، مبهم و غیرقابل اندازه‌گیری بودن است؛ به طوری که 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 معین کردن آن وجود دارد. وقتی نتوان مفهومی را به صراحت 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 پویایی بودن آن دلالت دارد و این ویژگی‌ها **ضمنی بودن**^۱، **نامتقارن بودن**^۲، **انتقال پذیری**^۳، **تضاد**^۴، **ناهم‌زمانی**^۵ و **جاذبه**^۶ 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؛ به طوری که 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 به منظور 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 به علاوه 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^۷، 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 به دنبال 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 Transitivity

⁴ Antonymy

⁵ Asynchrony

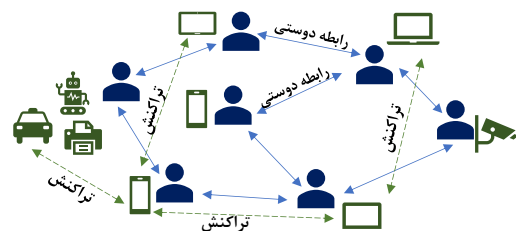
⁶ Gravity

⁷ service oriented architecture (SOA)

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.

۱-۲- 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^۱ 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 اشیا اجتماعی به‌دنبال برقراری تراکنش امن هستند تا علاوه بر 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

^۱ Wireless Sensor Networks (WSNs)

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^۲ در مقاله [36] و در شبکه‌های موردی متحرک^۳ در [37] و [38] پیاده‌سازی شده‌اند.

۳-۲- 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 می‌زند. 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 کارایی واحدهای محاسبه لبه^۴ 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 سامانه تشخیص کیفیت هوا است. این مدل متمرکز با ارائه خدمت اعتماد به‌عنوان خدمت^۵، 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.

۴-۲- شبکه اقتضایی خودرویی

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؛ به‌طوری‌که مدل در برابر حملات مقاوم و با ساختار شبکه اقتضایی وسایل نقلیه نیز سازگار است. ارزیابی اعتماد در [44]،

^۲ Smart Grid Networks

^۳ Mobile Ad-hoc Networks

^۴ Edge Computing Units (ECU)

^۵ Trust as a Service

^۶ Vehicular Ad-hoc Network (VANET)

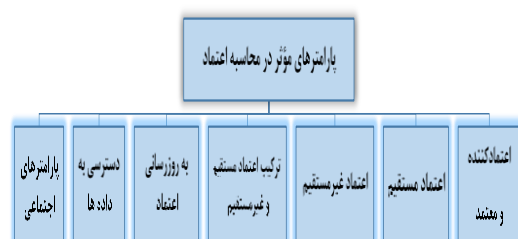
است. در این مدل عناصر شبکه اینترنت اشیا تراکنش‌های قابل اعتماد را در نواحی مجازی ایمن که حباب نام‌گذاری شده، با شناسایی و احراز هویت با قابلیت اطمینان بالا برقرار می‌کنند. چارچوب صدور مجوز مبتنی بر رفتار و آگاه از موضوع برای اینترنت اشیا خانگی نیز در [52] ارائه شده است. نویسندگان در [53] علاوه بر اینکه 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 علاوه بر سبک‌بودن از قابلیت گمنامی و اعتماد استفاده کرده و در برابر حملاتی مانند جعل هویت، تکرار و مرد میانی مقاوم است.

۷-۲- 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^۴ در اینترنت اشیا است. نویسندگان در [55] نیز یک راه حل امنیتی مبتنی بر زنجیره بلوکی برای اینترنت اشیا 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 به تفصیل مورد بحث و بررسی قرار خواهند گرفت.



(شکل ۲): پارامترهای مؤثر در محاسبه اعتماد

در اینترنت اشیا

(Figure-2): Effective parameters in trust computing

³ Blockchain

⁴ LoRaWAN

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 اقتصادی خودرویی با آگاهی از موضوع، اعتماد را تخمین می‌زند. اعتماد با استفاده از آنتروپی اطلاعات و یادگیری تقویتی^۱ محاسبه می‌شود تا وسیله نقلیه توانایی انتخاب بهترین تصمیم را داشته باشند. نویسندگان در [46]، مدل مدیریت اعتماد برای شبکه‌های اقتصادی 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.

۵-۲- اکوسیستم سلامت مبتنی بر اینترنت اشیا

با توجه به اهمیت امنیت در ابزارهای سلامت اینترنت اشیا، 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 کارایی 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 سامانه سلامت ارائه‌شده در شبکه اینترنت اشیا ارزیابی می‌شود.

۶-۲- احراز هویت اشیا

حباب اعتماد^۲ عنوان یک رویکرد جدید در مدیریت اعتماد مبتنی بر زنجیره بلوکی^۳ است که در مقاله [51] ارائه شده

¹ Reinforcement learning

² Bubbles of Trusts

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 اشیا 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.

۲-۳- 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.

۴-۳- 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.

۵-۳- 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.

۶-۳- دسترسی به داده‌ها

الگوریتم مدیریت اعتماد با توجه به نحوه دسترسی به اطلاعات می‌تواند به صورت متمرکز^۱ [18]، [20] و [49]؛ غیرمتمرکز^۲ [17]، [19]، [21]، [22]، [23]، [24]، [25] و [37] و یا حتی نیمه متمرکز^۳ [23] و [58] طراحی شود.

۷-۳- اینترنت اشیا اجتماعی^۴

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

۴- تحلیل مدل‌های محاسبه اعتماد مستقیم

۱-۴- فاکتورهای اصلی در محاسبه اعتماد مستقیم

مستقیم

۱-۴-۱- بازخورد^۵

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.

۲-۴-۱- 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 $O = \{o_0 \ o_1 \ o_2 \ \dots \ o_i\}$ دنباله‌ای از مشاهدات باشد و o_i میزان رضایتمندی خدمت‌گیرنده را در زمان i نشان دهد، آن‌گاه با استفاده از روش‌های هموارسازی نمایی^۶

¹ Centralized

² Decentralized

³ Semicentralized

⁴ Social Internet of Things (SIoT)

⁵ Feedback

⁶ Exponential smoothing Methods

• 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 رؤس، قابلیت اعتمادشان را بر تراکنش‌های ضعیف بنا نکنند، وزن در نظر گرفته شده است.

• F_{ij} : فاکتور رابطه^۲، مقداری بین صفر و یک است که بر اساس نوع رابطه بین اشیا مقداری 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^۳: اشیا^۳ مشابهی که در یک بازه زمانی و به‌وسیله یک کارخانه تولید می‌شوند.

- رابطه هم‌مکانی^۴ و همکاری^۵ 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^۶: اشیا با صاحبان یکسان.
- ارتباط اجتماعی اشیا^۷: 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.

$$T_{ij}^X(t) = (1 - \alpha)T_{ij}^X(t - \Delta t) + \alpha D_{ij}^X(t) \quad (4)$$

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

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.

$$(1) \quad \delta_i(X) = \begin{cases} 1 & \text{اگر } o_i = X \\ 0 & \text{در غیر این صورت} \end{cases} \quad \delta_i(X) = \sum_{l=0}^l r^{l-i} \delta_i(X)$$

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

۲-۴- مدل‌های ارائه‌شده محاسبه اعتماد مستقیم

۲-۴-۱- 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 اشیا^۳ 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 به‌وسیله شیء i با T_{ij} نشان داده شود رابطه (۲) نحوه محاسبه اعتماد مستقیم به روش جمع وزن‌دار ایستا را نشان می‌دهد.

$$(2) \quad T_{ij} = \sum_{i=1}^n \alpha_i P_i$$

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 اشیا^۳ اجتماعی هستند و با روش جمع وزن‌دار ایستا به‌صورت عددی بیان کرده است. (رابطه ۳)

$$(3) \quad O_{ij}^{dir} = \begin{cases} F_{ij} & \text{if } N_{ij} = 0 \\ \left(\frac{\log(N_{ij} + 1)}{1 + \log(N_{ij} + 1)} \right) (\epsilon O_{ij}^{lon} + \chi O_{ij}^{rec}) + \left(\frac{1}{1 + \log(N_{ij} + 1)} \right) F_{ij} & \text{if } N_{ij} > 0 \end{cases}$$

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

^۱ Decay Fator

^۲ Relationship Factor

^۳ Parental Object Relationship

^۴ Co-location Object Relationship

^۵ Co-work Object Relationship

^۶ Ownership Object Relationship

^۷ Social Object Relationship

• صداقت ($D_{ij}^{honesty}$): ویژگی صداقت با شمارش تجارب

تقلبی در بازه زمانی Δt و از رابطه $1 - \frac{\text{تعداد تجربه های مشکوک}}{\text{مقدار آستانه}}$ حاصل می شود.

• 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 به دست می آید.

• علاقمندی های مشترک ($D_{ij}^{community-interest}$): ویژگی علاقمندی های مشترک یا ظرفیت های یکسان نشان می دهد که اعتماد کننده و معتمد در چه تعداد انجمن های یکسانی عضو و از تقسیم تعداد انجمن هایی که هر دو رأس در آن ها عضو هستند بر مجموع تعداد انجمن هایی که دو رأس i و j به تنهایی در آن ها عضو هستند، به دست می آید. مقاله [22] نشان می دهد با وجود این که گر ها نمی دانند به کدام انجمن علاقه مندی تعلق دارند، برآورد اعتماد رؤس به سمت توافق انجمن^۱ هم گرا می شود. براساس پروتکل اعتماد ارائه شده در این مقاله، هر رأس اعتماد مستقیم را براساس سه ویژگی صداقت، مشارکت و انجمن علاقه مندی همانند مقاله [59] و رابطه (۴) می سنجد. صداقت به معنای درست کاری رأس و مشارکت مطابق با مقاله [60] به این معنی است که معتمد از نظر اجتماعی با اعتماد کننده در ارتباط است. انجمن علاقه مندی به این معنی است که اعتماد کننده و معتمد متعلق به انجمن های اجتماعی علاقه مندی نظیر هم مکانی، هم کاری یا هم خانوادگی یکسان هستند. (تعاریف مقاله [61])

در [58] هدف، ارزیابی اعتماد بین دو شیء با در نظر گرفتن لایه اجتماعی و استفاده از شواهد مستقیم و غیرمستقیم است؛ به طوری که در برابر حمله تبعیض اجتماعی مقاوم باشد. هر شخص، مالک یک یا چند شیء است و هر شیء یک یا چند سرویس ارائه می کند؛ به طوری که هر گر ممکن است، خدمت بد یا پیشنهاد غلط بدهد. اشیا بعد از گرفتن خدمت نظرات خود را در قالب بازخوردهای مثبت و منفی ذخیره می کنند و اعتماد مستقیم زمینه محور با روش جمع وزن دار ایستا و با استفاده از نظرات وزن دار با در نظر گرفتن فاکتور کاهشی زمان محاسبه می شود. در این مدل وزن ها 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 وزن دار پویا

در این روش، اعتماد مستقیم از همان رابطه (۲) به دست می آید با این تفاوت که ضرایب α_i به صورت پویا مطابق با مدل ارائه شده مقداردهی می شوند.

در مقاله [25] که هدف اصلی، ارائه مدل اعتماد اجتماعی مبتنی بر محتوا است، اعتماد مستقیم با روش جمع وزن دار پویا و از رابطه (۵) به دست می آید:

$$DT_{i,j} = \sum_1^n (DT_{i,j}^{cn} * WW_{i,j}^{cn}) \quad (5)$$

در رابطه (۵)، $WW_{i,j}^{cn}$ وزن های نرمال شده برای نشان دادن میزان اهمیت محتواها است، به طوری که $WW_{i,j}^{cn} = \frac{w_{i,j}^{cn}}{w_{Total}^{cn}}$ و $\sum WW_{i,j}^{cn} = 1$ هستند و اهمیت هر زمینه از تقسیم تعداد تراکنش های مستقیم i و j در زمینه C ($Tr_{i,j}^C$) بر تعداد کل تراکنش های صورت گرفته بین i و j در کلیه زمینه ها به دست می آید. (رابطه ۶)

$$W_{i,j}^C = \frac{Tr_{i,j}^C}{\sum_1^k Tr_{i,j}^{cn}} \quad (6)$$

مقدار $DT_{i,j}^{cn}$ در رابطه (۵) (اعتماد مستقیم بین i و j در زمینه cn) نیز از رابطه (۷) به دست می آید که در آن $DT_{i,j}^{cn(Old)}$ مقدار قدیمی اعتماد مستقیم بین i و j در زمینه cn و $\Delta DT_{i,j}^{cn}$ تغییر در اعتماد در زمینه cn است.

$$DT_{i,j}^{cn} = DT_{i,j}^{cn(Old)} + \Delta DT_{i,j}^{cn} \quad (7)$$

در رابطه بالا $\Delta DT_{i,j}^{cn}$ ، از فرمول $\Delta DT_{i,j}^{cn} = fb_{i,j}^{cn}/S$ به دست می آید که در این رابطه $fb_{i,j}^{cn}$ بازخورد i (خدمت گیرنده) نسبت به عملکرد j (خدمت دهنده) است و در محدوده $[-10, 10]$ قرار دارد. S نیز از رابطه $S = fb_{max}/MD$ حاصل می شود و منظور از fb_{max} بیشترین مقدار $fb_{i,j}^{cn}$ برای هر تراکنش یا به عبارتی 10 و MD ، بیشینه تغییری است که می تواند در مقدار اعتماد رخ دهد. به این ترتیب اعتماد مستقیم با توجه به ضرایب پویا در بازه های زمانی Δt به دست 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، دنباله ای از صفر و یک ها هستند که از توزیع برنولی پیروی می کنند. به این ترتیب احتمال موفقیت یا انتظار رضایت مندی (تابع توزیع ثانویه) به شرط داشتن دنباله ای از داده های آزمایش برنولی از توزیع بتا پیروی می کند. در این حالت اعتماد

۴-۲-۴- میانگین وزن دار

مدل ارائه شده در مقاله [18] به صورت متمرکز عمل می‌کند و ایده اصلی برای ارزیابی قابل اعتماد بودن یک شیء در شبکه، تجمیع نظرات خدمت‌گیرندگان پس از ارائه تعدادی خدمت مختلف است و به صورت توانایی یک شیء در ارائه خدمت خاص تعریف شده است. مدل ارائه شده 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 می‌کند 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 به عنوان نامزد برمی‌گزیند.

- مرحله دوم: پس از انتخاب اولیه، اشیا برای انتخاب نهایی با یکدیگر رقابت می‌کنند. در این مقاله رئیس نامزد که پتانسیل انتخاب شدن دارند با دو معیار نوع خدمت و ظرفیت مورد بررسی قرار می‌گیرند. هرچند که مجزا کردن 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 داده شده به هر بازخورد مطابق با رابطه $w_{Rij} = \lambda^{d_{ij}} \theta^{(s+1)(t_{now}-t_j)}$ با در نظر گرفتن گذشت زمان، بازخورد خدمت گیرنده (میزان رضایت از خدمت) و فاصله بین گیرنده و ارائه دهنده خدمت محاسبه شده است. پارامترهای λ و θ بین صفر و یک هستند که قابل تنظیم هستند. s نیز از رابطه $s = \frac{1}{2} * N_j$ به دست می‌آید. در صورتی که 1 یا 0 N_j شود، مقدار s برابر صفر خواهد شد؛ ولی اگر $N_j = -1$ 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 وزن دار نظرات محاسبه می‌شود و وزن نظرات همان w_{Rij} و کیفیت رأسی است که به خدمت دهنده امتیاز داده است.

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 صرف نظر کردن بسته‌ها محاسبه می‌شوند. به صورتی که اگر ρ نشان دهنده مجموع مشاهدات مثبت (بسته‌های ارسال شده) و n نشان دهنده مجموع مشاهدات منفی (بسته‌های صرف نظر شده) 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 $\alpha_{ij} = \rho + 1$ و $\beta_{ij} = n + 1$ محاسبه می‌شوند. مقدار اعتماد مستقیم بین هر دو رأس نیز با محاسبه امید ریاضی توزیع بتا $\frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}$ به روزرسانی 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 به صورت یک و صفر (دودویی) که به ترتیب به معنی رضایت‌مندی و عدم رضایت است، ذخیره می‌شود. رابطه (۹) نحوه به روز شدن $\alpha_{x,i}$ و $\beta_{x,i}$ را به روش هموارسازی نمایی نشان می‌دهد.

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

در رابطه بالا $f_{x,i}$ نشان دهنده نظر مثبت و $1 - f_{x,i}$ نشان دهنده نظر منفی است. Δt بازه زمانی است که در آن $\alpha_{x,i}$ و $\beta_{x,i}$ به روز 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] به دست می‌آید. (رابطه ۱۰)

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

- 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.

• مرحله یادگیری: زمانی که شیء گیرنده خدمت ارزیابی خود نسبت به ارائه‌دهنده را به سامانه مدیریت اعتماد بازمی‌گرداند، سامانه مدیریت اعتماد وارد مرحله یادگیری می‌شود و سطح اعتماد رؤسی را که درباره خدمت‌دهنده بازخورد داده بودند، به‌روزرسانی می‌کند. مرحله 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^۱ 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 رؤسی است که رأس j با آن‌ها تراکنش داشته است، با استفاده از رابطه (۱۱) به‌دست می‌آیند.

$$O_{ij}^{rec/lon} = \frac{\sum_{i=1}^M \sum_{l=1}^{L^{rec/lon}} f_{ij}^l \omega_{ij}^l C_{ij}^l}{\sum_{i=1}^M \sum_{l=1}^{L^{rec/lon}} \alpha} \quad (11)$$

در رابطه بالا ω_{ij}^l وزن در نظر گرفته‌شده برای هر بازخورد است تا رؤس، قابلیت اعتمادشان را بر تراکنش‌های ضعیف بنا نکنند و به‌منظور جلوگیری از اعمال بازخوردهای ناصحیح توسط رؤس 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

^۱ Distributed Hash Table (DHT)

هیچ بخش از حریم خصوصی آن‌ها وارد نشوند؛ بنابراین برداری به نام مطلوب‌ترین بردار به شکل $P_{best} = (0, 0, \dots, 0)$ ($n \in R^+$) 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.

$$T(A)_m = Jaccard(P_m, P_{best}) = \frac{|P_m \cap P_{best}|}{|P_{best}|} \times 100\% \\ = \left(1 - \frac{\sum_{i=1}^n P_i}{n}\right) \times 100\% \quad (12)$$

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 رؤسی 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 اشیا هستند که از آن‌ها راجع به داوطلب ارائه خدمت پرسیده می‌شود و درفبل 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

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

$$O_{ij}^{ind} = \frac{\sum_{k=1}^{|K_{ij}|} C_{ik} O_{kj}^{dir}}{\sum_{k=1}^{|K_{ij}|} C_{ik}} \quad (13)$$

اعتبار رأس k در نزد i (همان دوست مشترک i و j) از رابطه (۱۴) به دست 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.

$$C_{ik} = \eta O_{ik}^{dir} + \mu R_{ik} + \rho(1 - I_k) \quad (14)$$

در مقاله [19] هر کاربر می‌تواند از دوستانش بخواهد که به عنوان 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 به دست می‌آید. به این ترتیب اعتمادکننده وقتی پیشنهاددهای 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.

$$t_{x,i}^r = \sum_{u_y \in U} \frac{\text{sim}(u_x, u_y)}{\sum_{u_y \in U} \text{sim}(u_x, u_y)} \cdot t_{y,i}^d \quad (15)$$

در مقاله [25] برای محاسبه اعتماد غیرمستقیم اگر رأس i از سایر رؤس درباره j بپرسد، اعتماد غیرمستقیم از میانگین وزن‌دار اعتماد مستقیم پیشنهاددهندگان مطابق با رابطه (۱۶) به دست خواهد آمد.

$$Ind_{i,j}^e = \frac{\sum_1^M (RT_{j,k}^{cn} * X_k)}{M} \quad (16)$$

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

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

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

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

منابع	روش‌های محاسبه اعتماد									
	مدل ارتباطی		اعتماد مستقیم		اعتماد غیر مستقیم		ترکیب اعتماد		دسترسی	به روز رسانی اعتماد
	اعتمادکننده	معمده	روش محاسبه	متغیرها	روش محاسبه	متغیرها	انتخاب پیشنهاددهندگان	روش		
[21]	شیء	شیء	جمع وزن‌دار ایستا	فاکتور رابطه، نظر بلند مدت و نظر طولانی مدت مستقیم	میانگین وزن دار	نظرات غیرمستقیم و اعتبار	---	جمع وزن‌دار ایستا	غیر متمرکز	✓
[17]	شیء	شیء	جمع وزن‌دار ایستا	تجربه گذشته و مشاهدات مستقیم از صداقت، همکاری و گروه	---	نظر پیشنهاددهنده	---	جمع وزن‌دار پویا	غیر متمرکز	✓
[22]	شیء	شیء	جمع وزن دار ایستا	تجربه گذشته و مشاهدات مستقیم از صداقت، همکاری و گروه	---	نظر پیشنهاددهنده	---	جمع وزن‌دار پویا	غیر متمرکز	✓
[18]	شیء	شیء	میانگین وزن‌دار پویا	کیفیت پیشنهاددهندگان، فاصله، زمان و وزن امتیازات	---	---	شباهت موضوعی و قابلیت	---	متمرکز	✓
[49]	انسان	برنامه موبایل	ضریب شباهت Jaccard	بردار محرمانگی واقعی و بردار محرمانگی ایده‌آل	---	---	---	میانگین ریاضی	اعتماد مستقیم داوطلبان	متمرکز

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

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 شده اند.

۶- تحلیل مدل های ترکیب اعتماد مستقیم و غیرمستقیم

۶-۱- 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 روش های زیر می تواند این دو مقدار

۲-۲-۵- امید ریاضی توزیع بتا

اعتماد غیرمستقیم در مقاله [37] با استفاده از توزیع بتا محاسبه می شود، به طوری که اعتماد غیرمستقیم درواقع مشاهدات مستقیمی است که همسایه های رؤس ارزیابی کننده از ارزیابی شوند، داشته اند. با استفاده از اعتماد غیرمستقیم می توان بر مشکل ناکافی بودن اطلاعات غلبه کرد و رؤس جدید با استفاده از پیشنهاد های سایر رؤس، میزان اعتماد را پیش از انجام تراکش محاسبه کند.

۳-۲-۵- سایر روش ها

در مقالات [17]، [22] و [24] در صورتی که دو رأس تراکش مستقیم نداشته باشند، نظر پیشنهاددهنده $(R_{ij}^X(t))$ در متریک های صداقت، همکاری و علاقمندی به انجمن، اعتماد غیرمستقیم در نظر گرفته می شود.

مستقیم و غیرمستقیم با ضرایب ایستا مطابق با رابطه (۲۰) استفاده می‌کند.

$$T_{ij}^X(t) = \alpha * DT_{i,j} + \beta * IndT_{i,j} \quad (20)$$

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.

۶-۲-۲- 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.

$$T_{ij}^X(t) = (1 - \gamma)T_{ij}^X(t - \Delta t) + \gamma R_{ij}^X(t) \quad \forall j! = k \quad (21)$$

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 رؤس ارزیابی‌شونده محاسبه می‌شود.

$$T_{ij} = \omega_d * T_{ij}^d + \omega_i * T_{ij}^i, \quad \omega_d + \omega_i = 1 \quad (22)$$

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.

$$t_{x,i} = \mu . t_{x,i}^d + (1 - \mu) . t_{x,i}^r \quad (23)$$

۶-۲-۳- 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.

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.

۶-۲- مدل‌های ارائه‌شده در ترکیب اعتماد

مستقیم و غیرمستقیم

۶-۲-۱- 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 $R_{ij} = \frac{|K_{ij}|}{|N_i|}$ تعریف می‌شود، نشان‌دهنده افرادی است که دوستان مشترک زیادی دارند و به این ترتیب در بسیاری از موارد نیز هم‌عقیده هستند:

$$T_{ij} = \alpha R_{ij} + \beta I_j + \gamma O_{ij}^{dir} + \delta O_{ij}^{ind} \quad (17)$$

$$\alpha + \beta + \gamma + \delta = 1$$

در مقاله [23] زمانی که رأس i نیاز به دانستن اعتماد j دارد از DHT درباره رأس j می‌پرسد و همه رؤس 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.

$$T_j = (1 - \alpha - \beta)R_j + \alpha O_j^{lon} + \beta O_j^{rec} \quad (18)$$

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

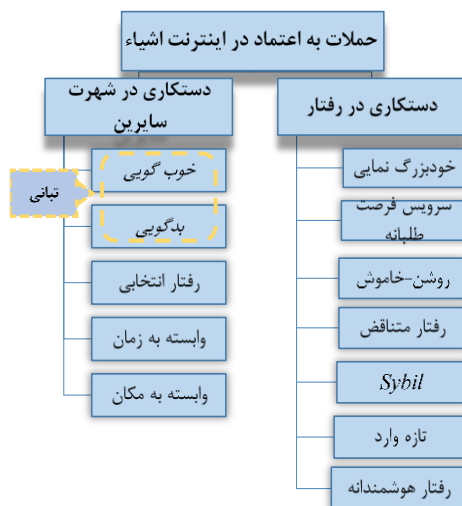
$$R_j = \frac{(A_j + H_j)}{(Q_j + A_j + H_j)} \quad (19)$$

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

۷- تحلیل مدل‌های اعتماد از منظر حملات

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 رئیس مخرب شهرت دیگران را با اظهار نظر نادرست، دچار تغییر می‌کنند. نوعی از حملات نیز وجود دارند که از همکاری تعدادی رئیس مخرب به‌وجود می‌آید؛ به این ترتیب که تعدادی رئیس با تبانی جهت بدنام کردن یک رئیس مشهور و یا خوش‌نام کردن رئیس بی‌کفایت با هم به توافق می‌رسند. حملاتی که به‌وسیله رئیس مخرب علیه سامانه‌های مدیریت اعتماد اجرا می‌شود و به‌طورعمومی با مفهوم اعتماد مرتبط هستند، در ادامه به‌اختصار شرح داده می‌شوند:

- حمله خدمت فرصت‌طلبانه^۱: رئیس مخرب به‌محض این‌که متوجه می‌شود، شهرت خود را از دست داده است، کیفیت ارائه خدمت را بالا می‌برد [19].

- حمله روشن-خاموش^۲: رئیس مخرب در اجرای حمله روشن-خاموش با ایجاد الگوی رفتاری که بین رفتار

^۱ Opportunistic Service Attack

^۲ On-off Attack

خوب و بد در حال تغییر است، امیدوار است تا زمان آسیب‌رسانی به‌صورت نامحسوس باقی بماند [62].

- حمله رفتار متناقض^۳: رئیس مخرب به دلخواه به برخی خدمات بی‌کیفیت ارائه می‌کند، درحالی‌که رفتار متفاوتی با سایرین دارد.

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

- حمله تازه وارد^۴: 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^۵: در این حمله رئیس مخرب به‌صورت هوشمندانه مطابق با آستانه قابل اعتمادماندن، با پیشنهادهای نادرست یا خدمات خوب و بد تغییر رفتار می‌دهد [37].

- حمله خوب‌گویی^۶: در این مدل حملات، شهرت رئیس بدنام با تعریف و ارائه پیشنهادهای خوب درباره آن‌ها افزایش می‌یابد و درنتیجه بخت رئیس ناشایست برای انتخاب به‌عنوان ارائه‌دهنده خدمت بالا می‌رود [63].

- حمله بدگویی^۷: در این حالت رئیس مخرب با ازبین‌بردن شهرت یک رئیس خوش‌نام (مثلاً با ارائه پیشنهادهای بد درمورد رئیس خوب) باعث کاهش محبوبیت آن رئیس شده و شانس انتخاب این رئیس به‌عنوان خدمت‌دهنده را کاهش می‌دهد [63].

- حمله رفتار انتخابی^۸: عنصر مخرب از روی عمد درباره برخی رئیس گزارش غلط ارائه می‌دهد؛ در صورتی که با سایر اجزای شبکه چنین رفتاری از خود نشان نمی‌دهد [37].

- حمله وابسته به زمان^۹: در این مدل حمله نحوه ارائه بازخورد رئیس مخرب با تغییر زمان متفاوت می‌شود؛ به‌طوری‌که به دنبال فرصت مناسب برای امتیازدهی ناعادلانه است [37].

- حمله وابسته به مکان^{۱۰}: در این حمله، نحوه ارائه بازخورد رئیس مخرب با تغییر مکان متفاوت می‌شود؛

^۳ Conflicting Behavior Attack

^۴ Newcomer Attack

^۵ Intelligent Behavior attack

^۶ Good-mouthing Attack

^۷ Bad-mouthing Attack

^۸ Selective Behavior Attack

^۹ Time-dependent Attack

^{۱۰} Location-dependent Attack

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

از آنجایی که در دنیای واقعی اینترنت اشیا، رؤس مخرب در تلاش برای کاهش کارایی 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.

۷-۲- 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 کارایی 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 خوب‌گویی، 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 رؤس مخرب هر بازخورد توسط پارامتر اعتبار که در رابطه ۲۴ نشان داده شده است، وزن‌دار می‌شود. به این ترتیب رؤسی که پیوندهای ارتباطی قوی دارند، خیلی باهوش هستند و تعداد زیادی تراکنش برقرار کرده‌اند پتانسیل رفتار مخرب را دارند؛ از اعتبار کمتری برخوردار می‌شوند.

$$C_{ij} = \frac{(1 - \gamma - \delta)T_i + \gamma(1 - F_{ij}) + \delta(1 - I_i)}{1 + \log(N_{ij} + 1)} \quad (24)$$

در مقاله [37] مطابق با رابطه (۲۲)، وزن اعتماد مستقیم (w_d) و غیرمستقیم (w_i) به‌صورت پویا براساس کمیت و کیفیت تراکنش‌های مشاهده‌شده به‌وسیله رؤس 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 رؤس بر اساس سه معیار مقدار اطمینان^۱، میزان انحراف^۲ و اندازه نزدیکی^۳ 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.

$$MSE(\mu) = \sum_i \left(\mu \cdot t_{x,i}^d + (1 - \mu) \cdot t_{x,i}^r - \overline{f_{x,i}^{(new)}} \right)^2 \quad (25)$$

¹ Confidence Value

² Deviation Value

³ Closeness Value

در مقاله [25] برای مقابله با حملاتی نظیر **خوب‌گویی** یا **بدگویی** وقتی از سایر رؤوس 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 $\sqrt{}$ استفاده شده و در غیر این صورت با اشاره نشده (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] به دلیل متمرکز بودن الگوریتم و حفظ کلیه داده‌ها در برابر حملات روشن-خاموش، خدمت فرصت‌طلبانه و بدگویی مقاوم است. در مقاله [21] و [23] خدمت‌دهندگان بد و رؤوسی که بازخورد غلط می‌دهند، شناسایی می‌شوند. در مقاله [37] نیز رؤوس خودخواه و دسته‌ای از رؤوس 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 به‌وسیله اشیا در شبکه اینترنت اشیا سبب شده است که اعتماد به موضوع وابسته باشد. همان‌طور که 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 z را محاسبه می‌کند:

- اگر فضای حافظه پر نباشد و یا رأس i با رأس z درقبل تراکنش داشته است، به‌راحتی در فضای حافظه قرار می‌گیرد.

- در صورتی که فضای حافظه پر باشد، رأس i مقدار اعتماد نسبت به z 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 $\sqrt{}$ در ستون مربوطه نشان داده شده‌اند.

۹- روش‌های ارزیابی مدل‌های اعتماد

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



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

۹-۱- نرخ موفقیت

معیار ارزیابی عملکرد مدل ارائه شده در مقالات [21]، [23] و [58] نسبت تعداد تراکنش‌های موفق به تعداد کل تراکنش‌ها است که با عنوان **نرخ موفقیت**^۱ از آن نام برده شده است.

۹-۲- سرعت و دقت رسیدن به سطح اعتماد ذاتی^۲

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

نتایج در مقاله [22] نشان می‌دهد با وجود این که رؤس 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 رؤس 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 رؤس مخرب و وجود حملات خوب‌گویی، بدگویی

و روشن‌خاموش 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، کارایی و قابلیت اطمینان الگوریتم ارائه شده در مقاله [25] شبیه‌سازی در حضور رؤس مخرب صورت گرفته و سطح مطلوب اعتماد برای رأس خوب عدد یک و رأس مخرب عدد صفر فرض شده است. عملکرد پروتکل ارائه شده 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 ارائه شده 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] به عنوان معیار اعتماد ذاتی در نظر گرفته شده و به این ترتیب هم‌گرایی، دقت و انعطاف‌پذیری الگوریتم در حضور رؤس 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؛ به طوری که 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 ارائه شده در مقاله [65] و با معیار نرخ موفقیت مقایسه شده‌اند. در مقاله [19]، مقایسه‌ای بین مدل ارائه شده 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 مجموعه داده 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

(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

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

کنند. کارایی مدل ارائه‌شده با معیارهای پیشنهادهای تقلبی کشف‌شده، منفی اشتباه و مثبت اشتباه در حضور حملات بدگویی و خوب‌گویی بررسی شده است.

۵-۹- پیاده‌سازی بر روی کاربردهای اینترنت اشیا

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

¹ International Mobile Equipment Identity

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

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

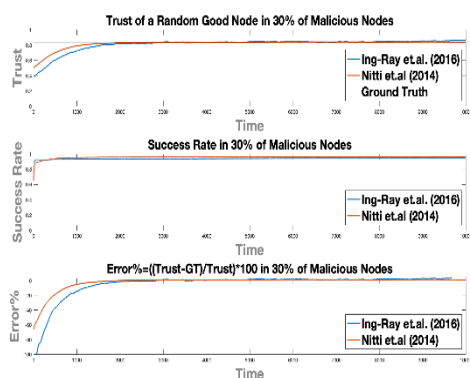
مقدار اعتماد یک رأس خوب با وجود حمله بدگویی اندازه‌گیری می‌شود تا اثر حمله در حضور الگوریتم و بدون آن بررسی شود. مقدار اعتماد یک رأس بد با وجود حمله خوب‌گویی اندازه‌گیری می‌شود تا نشان داده شود چگونه حمله‌کنندگان می‌توانند مقدار اعتماد این رأس را تحریف

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. رؤس مخرب با حملات خوب‌گویی و بدگویی در مراحل مختلف شبیه‌سازی ۳۰٪، ۵۰٪ و ۷۰٪ کل رؤس شبکه را شامل می‌شوند. کلیه شبیه‌سازی‌ها پنجاه مرتبه تکرار شده‌اند و زمان پایداری الگوریتم ده‌هزار بازه زمانی در نظر 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 رؤس مخرب	۳۰٪ و ۵۰٪
زمان نهایی	۱۰۰۰۰
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٪ رؤس مخرب نشان می‌دهد. شکل (۵) نشان می‌دهد که در حضور ۳۰٪ رؤس 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): Comparision of two models with 30% of malicious nodes

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

تلفن و وقایع ثبت‌شده سامانه در نظر 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.

۹-۶- 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 خواهد شد، 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، علاوه بر 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 رؤس 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 رؤس 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

(جدول ۴-): نتایج کمی حاصل از شبیه سازی

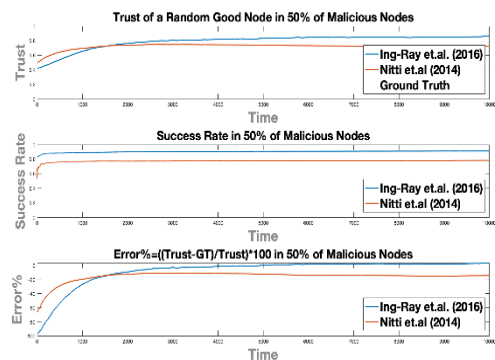
(Table-4): Quantitive simulation results

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	۰/۹۴۴۷	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 شبیه سازی به دو حالت گذرا و پایدار تقسیم می شود. به این ترتیب که از ابتدا تا رسیدن به اعتماد ذاتی، زمان گذرا و پس از آن زمان پایدار الگوریتم در نظر گرفته می شود 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، نکته ای که در پژوهش های گذشته به آن توجهی نشده بود.

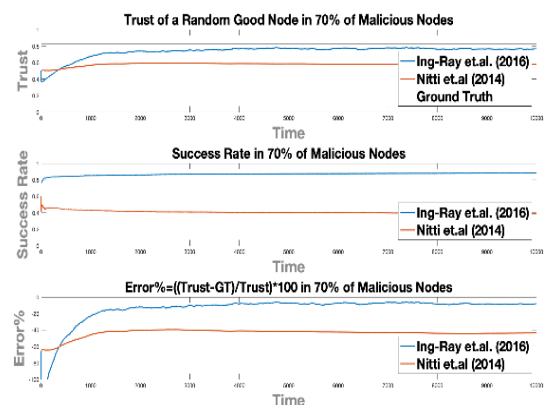
جدول (۵) نشان می دهد زمانی که درصد رئوس مخرب ۳۰٪ باشد الگوریتم [23] خطای کمتری دارد، درحالی که با افزایش درصد حملات، به پایداری نمی رسد و بنابراین اعدادی برای مقایسه وجود نخواهد داشت. با در نظر گرفتن جداول (۱ و ۲) (ویژگی های دو مدل) و نتایج عددی حاصل از شبیه سازی های ارائه شده در جداول (۴ و ۵) نکاتی حاصل می شود که به کمک آن می توان ضعف ها و برتری های الگوریتم ها 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 داشته اند را ترکیب وزن دار می کند؛ درحالی که در مدل [19] نظر تعدادی از دوستان که بیشترین شباهت به معتمد دارند به صورت وزن دار با یکدیگر ترکیب می شوند. با توجه به نتایج شبیه سازی،



(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 می دهد که هر دو مدل در برابر حملات نودهای مخرب تاب آوری خود را از دست داده و به اعتماد ذاتی نمی رسند، درحالی که باز هم الگوریتم [19] بهتر عمل می کند.



(شکل ۷-): مقایسه دو مدل در حضور ۷۰٪ رأس مخرب
(Figure-7): Comparion of two models with 70% of malicious nodes

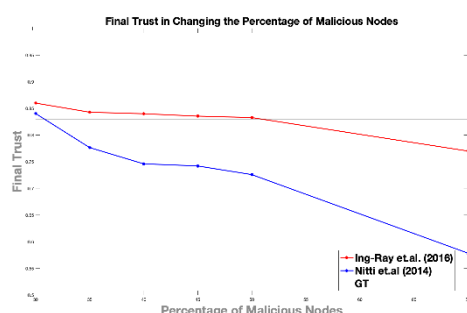
جدول (۴) با هدف مقایسه این دو الگوریتم از زمان شروع تا انتهای شبیه سازی ارائه شده است. با توجه به مرجع [64] اعتماد ذاتی رأس خوب تصادفی ۰/۸۳ در نظر گرفته شده است؛ بنابراین یکی از روش های مقایسه دو مدل بررسی زمان رسیدن به این مقدار است. جدول (۴) نشان می دهد که الگوریتم [23] با درصد رئوس مخرب پایین تر زودتر به این مقدار همگرا می شود؛ درحالی که با بالا رفتن درصد رئوس مخرب تا پایان زمان شبیه سازی همگرا نمی شود؛ به علاوه اعداد جدول (۴) کاهش عملکرد هر دو الگوریتم را با افزایش حملات به خوبی نشان می دهد، هرچند که الگوریتم [19] با افزایش حملات از [23] عملکرد بهتری دارد. مقایسه مقادیر نهایی در هر دو مدل گواه این نتیجه گیری است. (با هدف سهولت در مقایسه، عملکرد بهتر در جداول به صورت خانه های حاشیه دار نمایش داده شده اند).

در صورتی که استحکام الگوریتم اعتماد در برابر حملات، رسیدن مقدار نهایی اعتماد به اعتماد ذاتی تعریف شود، استحکام الگوریتم [19] تا رسیدن رئوس مخرب به ۵۰٪، در حالی که 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 زمینه محاسبه 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، علاوه بر 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،

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

در حالی که 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، در حالی که الگوریتم [19] با حداقل کردن 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): Quantitative steady state simulation results

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	۰/۰۰۳۶
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.

- [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," *Universität 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 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

دو مدل مشهور و شناخته شده شبیه سازی، ارزیابی و مقایسه شد.

بررسی کلیه مقالات و نتایج شبیه سازی نشان می دهد، پارامترهای اشاره شده شامل نحوه به روزرسانی داده ها با گذشت زمان، فیلتر کردن پیشنهاددهندگان، ترکیب نظرات پیشنهاددهندگان با ضرایب پویا و تنبیه و تشویق پیشنهاددهندگان در استحکام الگوریتم در برابر حملات رئیس مخرب بسیار مؤثر است. با در نظر گرفتن زمان رسیدن الگوریتم به اعتماد ذاتی به عنوان زمان گذرا و پس از آن زمان پایداری، می توان عملکرد الگوریتم ها را با معیارهای آماری نظیر میانگین، انحراف معیار و میانگین خطای میانگین مربعات مقایسه کرد.

در ادامه پیشنهاد می شود، محتوا یا زمینه در محاسبات دخیل شود؛ به طوری که مقدار آستانه قابل اعتماد برای رئیس در خدمات مختلف متفاوت باشد. همچنین پارامترهایی نظیر ویژگی های اجتماعی و محدودیت های اشیا نیز به شبیه سازی ها اضافه، تا عملکرد الگوریتم ها با تغییر این پارامترها نیز بررسی شود. به علاوه مقاومت الگوریتم ها در برابر حملاتی نظیر حمله روشن-خاموش و تبانی نیز باید مورد بررسی قرار گیرد.

از آنجایی که شبکه اینترنت اشیا پیوسته با مشکل پیوستن و جدا شدن رئیس مواجه است، پروتکل مدیریت اعتماد باید این موضوع را در نظر بگیرد که در صورت اضافه شدن و یا حذف شدن رأسی بتواند با سرعت و دقت اعتماد را دوباره محاسبه کند و به عبارتی انعطاف پذیری الگوریتم در برابر این تغییرات نیز می تواند به عنوان یک معیار مورد بررسی قرار گیرد.

تقدیر و سپاس گذاری

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

11- References

۱۱- مراجع

- [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.

- "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. Djamel 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,

- [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. Janbabaie, 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، دهنداد 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.

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 پسادکتری 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

Giving a Social Structure to the Internet of Things," *IEEE 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

دکتر 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

