ارائه روشی نوین برای محاسبه اعتماد در کاربردهای اینترنت اشیاء

بهشید شایسته[۱]، کارشناسی ارشد؛ وصال حکمی[۲]، استادیار؛ سید اکبر مصطفوی[۳]، استادیار؛ احمد اکبری ازیرانی[۴]، دانشیار

۱- دانشکده مهندسی کامپیوتر - دانشگاه علم و صنعت ایران - تهران - ایران – bshayesteh@alumni.iust.ac.ir
۲- دانشکده مهندسی کامپیوتر - دانشگاه علم و صنعت ایران - تهران - ایران – vhakami@iust.ac.ir
۳- گروه مهندسی کامپیوتر - دانشگاه یزد - یزد - ایران – a.mostafavi@yazd.ac.ir
۴- دانشکده مهندسی کامپیوتر - دانشگاه علم و صنعت ایران - تهران - ایران – akbari@iust.ac.ir

چکیده: در سیستم‌های اینترنت اشیا کیفیت سرویس و اعتبار داده‌های مورد استفاده برای تصمیم‌گیری در کاربردهای مختلف اهمیت بالایی دارند. اشیاء مخرب می‌توانند با ارائه داده‌های نامعتبر موجب کاهش کیفیت و تجربه سرویس برای سایر گره‌ها در یک سیستم اینترنت اشیا شوند. یکی از راه‌کارهای ممکن برای حل این مشـــکل، مدیریت اعتماد اســـت. اغلب پژوهش‌های موجود برای محاســـبه اعتماد متمرکز بر محاســـبه اعتماد موجودیت‌های یک سیستم است. در این مقاله روشی برای محاسبه اعتماد ارائه شده است که علاوه بر محاسبه اعتماد موجودیت‌ها در یک کاربرد اینترنت اشیا، به محاسبه اعتمادپذیری داده نیز بپردازد. به این منظور، روش نوینی برای محاسبه اعتماد با در نظر گرفتن ارتباط بین اعتمادپذیری داده و اعتماد موجودیت ارائه شده است که مبتنی بر یادگیری بیزی بوده و برای محاسبه اعتمادپذیری داده از قانون ترکیب نظریه دمپستر- شیفر استفاده می‌کند. برای آزمایش روش پیشنهادی، به شبیه سازی این روش در سناریوی پارکینگ هوشمند پرداخته شده و مقدار همگرایی و زمان همگرایی اعتماد در حضور رفتارهای مخرب و میزان تطبیق‌پذیری آن ارزیابی شده است. نتایج حاصل از ارزیابی روش پیشنهادی در قیاس با روش موجود نشان می‌دهد که روش ما حتی در حضور ۷۰٪ گره مخرب در سیستم، تخمین صحیحی از اعتماد را به دست می‌دهد.

واژه‌های کلیدی: اینترنت اشیا، محاسبه اعتماد، اعتمادپذیری داده، پارکینگ هوشمند.

A Novel Trust Computation Scheme for Internet of Things Applications

B. Shayesteh[1], MSc; V. Hakami[2], Assistant Professor; S.A. Mostafavi[3], Assistant Professor; A. Akbari Azirani[4], Associate Professor

1- School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran, Email: bshayesteh@alumni.iust.ac.ir
2- School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran, Email: vhakami@iust.ac.ir
3- Department of Computer Engineering, Yazd University, Yazd, Iran, Email: a.mostafavi@yazd.ac.ir
4- School of Computer Engineering, Iran University of Science and Technology, Tehran, Iran, Email: akbari@iust.ac.ir

Abstract: Quality of service and trustworthiness of data is of high importance for decision making in Internet-of-Things (IoT) applications. Malicious nodes and devices may compromise the quality of service and experience for other nodes through providing invalid data and evaluations. Hence, a trust management system to assess the trust level of users and gathered data is deemed to be essential to every IoT system. The current approach in the literature for computing the trust level is entity-centric trust in which the trust level of end users are estimated. However, the trustworthiness of data is equally important in many applications. In this paper, we propose, Trusty, a hybrid trust computation approach, aiming at trust assessment for both entities as well as data. In our proposed approach, a Bayesian learning method is used for computing the entity trust, while Dempster-Shafer theory is exploited to data fusion and data trustworthiness assessment. We implement Trusty in a smart parking system scenario to investigate the performance of our model in the different settings for misbehavior nodes and faulty sensors. As shown by the extensive simulation experiments, Trusty outperforms the competing approaches in terms of convergence for both data trustworthiness and entity trust.

Keywords: Internet of Things, Trust Computation, Data Trustworthiness, Smart Parking.

تاریخ ارسال مقاله: ۱۳۹۷/۰۷/۰۷
تاریخ اصلاح مقاله: ۱۳۹۷/۱۰/۲۴و ۱۳۹۸/۰۳/۱۲
تاریخ پذیرش مقاله: ۱۳۹۸/۰۴/۰۴
نام نویسنده مسئول: وصال حکمی
نشانی نویسنده مسئول: ایران - تهران – رسالت – خیابان دانشگاه - دانشگاه علم و صنعت ایران - دانشکده مهندسی کامپیوتر.

۱- مقدمه

اینترنت اشیا سامانه‌ای از دستگاه‌های پردازشی هم‌بسته، ماشین‌های مکانیکی و دیجیتال، اشیا و انسان‌ها است که بدون نیاز به دخالت انسان با فراهم شدن یک شناسه یکتا دارای قابلیت ارسال اطلاعات بر روی شبکه هستند [۱]. ازآنجاکه در محیط اینترنت اشیا، ارتباطات دستگاه‌های هوشمند و موجودیت‌ها در محیط‌های ناشناخته صورت می‌گیرد، یک چالش اصلی این است که چگونه دستگاه‌ها باید به یکدیگر اعتماد کنند. در سیستم‌های اینترنت اشیا کیفیت سرویس‌های فراهم شده و معتبر بودن داده‌های مورد استفاده برای تصمیم‌گیری در کاربردهای مختلف اهمیت بالایی دارند [۲]. موجودیت‌های مخرب و اشیا می‌توانند با ارائه داده‌ها و ارزیابی‌های نامعتبر در مورد یک سرویس، باعث پایین آمدن کیفیت و تجربه آن سرویس برای سایر موجودیت‌ها شوند. یکی از راه‌کارهای ممکن برای این مسئله، مدیریت اعتماد است. بنابراین چالش عمده این است که چگونه یک سیستم مدیریت اعتماد طراحی شود که بتواند کارایی سیستم را در صورت وجود موجودیت‌ها و داده‌های مخرب بهبود بخشد [۳].

تمرکز بیش‌تر روش‌های ارائه شده برای محاسبه اعتماد در اینترنت اشیا، بر روی اعتماد موجودیت‌های یک سیستم است. این نوع محاسبه، با بررسی رفتارها و تمایلات این گره‌ها برای تشخیص گره‌های مخرب یا غیر صادق از گره‌های خوش‌رفتار و صادق انجام می شود. فرض برابری اعتمادپذیری داده با اعتماد تخمین زده شده برای موجودیت تولید کننده آن کاملاً درست نیست؛ زیرا بیشتر سیستم‌های اینترنت اشیا به جریان‌های داده بستگی دارند و جامعیت داده و اینکه چه کسی آن را تولید کرده است؛ هر دو حائز اهمیت هستند.

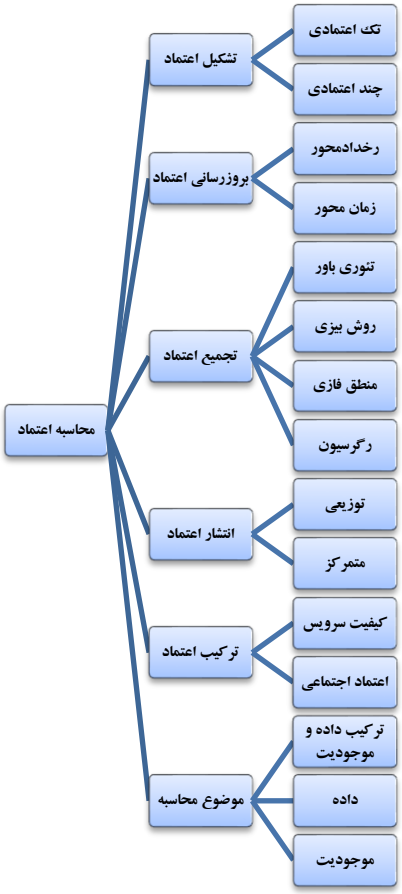
در این مقاله، یک دسته‌بندی بر اساس موضوع محاسبه اعتماد برای روش‌های ارائه شده در حوزه اینترنت اشیا ارائه شده است. بر اساس این دسته‌بندی، روش‌های ارائه شده به سه دسته تقسیم می‌شوند: روش‌هایی که تنها اعتماد موجودیت‌ها یک سیستم را محاسبه می‌کنند، روش‌هایی که تنها اعتمادپذیری داده‌های تولید شده در یک سیستم را محاسبه می‌کنند و روش‌هایی که علاوه بر محاسبه اعتمادپذیری داده، اعتماد موجودیت را نیز محاسبه می‌کنند (ترکیبی). با توجه به اینکه کارهای کمتری در زمینه محاسبه اعتماد ترکیبی انجام شده‌است؛ در این کار به ارائه مراحل محاسبه اعتماد و ارائه یک روش با رویکرد ترکیبی در اینترنت اشیا پرداخته شده است.

در روش پیشنهادی، برای محاسبه اعتماد موجودیت‌ها از یک روش مبتنی بر یادگیری بیزی و برای محاسبه اعتمادپذیری داده از قانون ترکیب نظریه دمپستر-شیفر استفاده شده‌است. با انجام مطالعه موردی پارکینگ هوشمند، صحت‌سنجی روش پیشنهادی انجام شده و درنهایت روش پیشنهادی بر اساس ملاک‌هایی مانند مقدار همگرایی اعتماد، زمان همگرایی اعتماد و تطبیق‌پذیری ارزیابی شده و با یک کار مشابه محاسبه اعتماد ترکیبی در اینترنت اشیا مقایسه شده است. هدف از انتخاب یک مطالعه موردی، نشان دادن نحوه نگاشت روش محاسباتی پیشنهادی در یک سناریوی کاربردی و بررسی کارایی روش است. با توجه به روش محاسباتی پیشنهادی، مطالعه موردی باید در کاربردی باشد که در آن کاربران بدون در نظر گرفتن ارتباطات اجتماعی به جمع‌آوری داده در یک سکوی مرکزی می‌پردازند. در این راستا، کاربرد «پارکینگ هوشمند» یکی از سناریوهای مطرح در اینترنت اشیاء برای شهر هوشمند است که با ویژگی موردنظر برای نگاشتِ روش پیشنهادی ما نیز تطابق دارد.

در این مقاله در بخش دوم به بررسی کارهای مرتبط در حوزه اعتماد در اینترنت اشیا پرداخته شده است. در بخش سوم روش محاسبه اعتماد پیشنهادی ارائه شده است و این روش در بخش چهارم بر روی مطالعه موردی پارکینگ هوشمند نگاشت شده است. در بخش پنجم نتایج ارزیابی نشان داده شده‌اند و بخش ششم به جمع‌بندی می پردازد.

۲- کارهای مرتبط

در سیستم‌های اینترنت اشیاء مدیریت اعتماد از اهمیت بسزایی برخوردار است. در ادبیات مدیریت اعتماد در اینترنت اشیا، محاسبه اعتماد به شش قسمت ترکیب اعتماد، انتشار اعتماد، تجمیع اعتماد، به‌روزرسانی اعتماد، شکل‌گیری اعتماد و موضوع محاسبه اعتماد تقسیم شده‌است.



شکل ۱: درخت روش‌های محاسبه اعتماد

ترکیب اعتماد مشخص می‌کند که در محاسبه اعتماد از چه اجزایی استفاده شود. این اجزا شامل کیفیت سرویس و اعتماد اجتماعی است. انتشار اعتماد به چگونگی انتشار شواهد اعتماد به دیگر دستگاه‌های شبکه اشاره دارد و شامل دو نوع انتشار توزیع شده و متمرکز است. تجمیع اعتماد به ترکیب شواهد اعتماد به‌دست‌آمده از طریق مشاهده‌های خود دستگاه و یا بازخورد از دستگاه‌های دیگر و به‌دست آوردن اعتماد نهایی اشاره دارد [۴]. روش‌های رایج ترکیب شواهد اعتماد شامل جمع وزن‌دار، تئوری باور، استنتاج بیزی، منطق فازی و تحلیل رگرسیون هستند [۶-۴]. محاسبه اعتماد با در نظر گرفتن هدف مورد ارزیابی محاسبه اعتماد به سه دسته محاسبه اعتماد موجودیت، محاسبه اعتمادپذیری داده و محاسبه اعتماد ترکیبی تقسیم می شود [۸-۷]. تنوع روش‌های محاسبه اعتماد را می‌توان در قالب یک ساختار درختی مانند شکل ۱ نمایش داد.

در زمینه محاسبه اعتماد ترکیبی کارهای محدودتری انجام شده است. در مرجع [۹] یک روش محاسبه اعتماد ترکیبی برای کاربرد سلامت در اینترنت اشیا ارائه شده است. معیار ترکیب اعتماد از نوع کیفیت سرویس (نرخ درستی بازخوردها) است. نوع انتشار اعتماد در این روش متمرکز است و محاسبه اعتماد در یک موجودیت مرکزی انجام می‌شود. در قسمت تجمیع اعتماد برای اعتمادپذیری داده، از روش میانگین‌گیری بین اعتماد موجودیت‌های تولیدکننده داده استفاده شده است و برای اعتماد موجودیت از جمع وزن‌دار بین معیارهای کیفیت سرویس استفاده شده است. یکی از نقص‌های این روش، تجمیع اعتمادپذیری داده است که تنها از اعتماد موجودیت‌های بازخورددهنده برای به دست آوردن اعتمادپذیری داده استفاده کرده است و از معیارهایی مانند پارامترهای زمینه بهره نبرده است.

در مرجع [۱۰] برای تأمین امنیت در اینترنت اشیا، یک طرح کلی مبتنی بر سیاست، برای جمع‌آوری داده به‌صورت امن و قابل اعتماد به نام RealAlert ارائه شده است. تجمیع اعتماد در این روش با استفاده از نظریه دمپستر-شیفر انجام می‌شود؛ به‌این‌ترتیب که گزارش‌های همسایگان هر گره، که می‌تواند همراه با عدم قطعیت باشد، در آن گره ترکیب می شود. از نقص‌های این روش، می‌توان به وجود ابهام در روش تشخیص داده‌های خارج از محدوده برای محاسبه اعتمادپذیری داده و هم‌چنین، وجود ابهام در روش تشخیص رفتارهای ناهنجار یک گره اشاره کرد. هم‌چنین، در تابع ترکیب نظریه دمپستر-شیفر، نحوه تعریف وزن‌های استفاده شده که قسمت اصلی استفاده از این ترکیب است، بیان نشده است.

در مرجع [۱۱] یک چارچوب محاسبه اعتماد ترکیبی مبتنی بر کار پیشین نویسندگان [۱۲] ارائه شده است. تمرکز این کار روی افزودن اعتمادپذیری داده به کار پیشین و ارائه یک چارچوب محاسبه اعتماد ترکیبی است. معیارهای ترکیب اعتماد موجودیت در این کار شهرت و دانش و تجربه هستند. انتشار اعتماد برای اعتماد موجودیت به صورت توزیع‌شده انجام می‌شود و هریک از گره‌ها اعتماد نسبت به سایر گره‌ها را محاسبه می‌کنند. در تجمیع اعتماد برای هر دو اعتمادپذیری داده و اعتماد موجودیت از روش جمع وزن‌دار استفاده شده است. از نقص‌های این روش می‌توان به مشخص نبودن روش تعیین ضرایب در تجمیع اعتماد اشاره کرد. علاوه بر این، چارچوب ارائه شده و روش محاسبه اعتماد، مورد ارزیابی و شبیه‌سازی قرار نگرفته است.

جدول ۱: مقایسه روش‌های محاسبه اعتماد

روش محاسبه / موضوع		فاکتورهای محاسبه اعتماد				
		ترکیب اعتماد	انتشار اعتماد	تجمیع اعتماد	تشکیل اعتماد	به‌روزرسانی اعتماد
اعتماد موجودیت	[۱۳]	کیفیت سرویس	متمرکز	جمع وزن‌دار ایستا	تک اعتمادی	رخدادمحور
	[۱۴]	کیفیت سرویس	توزیعی	جمع وزن‌دار ایستا	چند اعتمادی با جمع وزن‌دار ایستا	رخدادمحور/ زمان‌محور
	[۱۵]	کیفیت سرویس	توزیعی	جمع‌وزن‌دار ایستا	چند اعتمادی با جمع وزن‌دار ایستا	رخدادمحور/ زمان‌محور
	[۱۶] [۱۰]	کیفیت سرویس	توزیعی	روش بیزی/ جمع‌وزن‌دار پویا	تک اعتمادی	رخدادمحور/ زمان‌محور
	[۱۷]	کیفیت سرویس	توزیعی	منطق فازی/ جمع وزن‌دار پویا	تک اعتمادی با جمع وزن‌دار ایستا	زمان‌محور
	[۱۰]	کیفیت سرویس	توزیعی/ متمرکز	جمع‌وزن‌دار ایستا	چند اعتمادی با جمع وزن‌دار ایستا	رخدادمحور
	[۱۸]	کیفیت سرویس	متمرکز	روش بیزی	تک اعتمادی	زمان‌محور
اعتماد پذیری داده	[۱۹]	کیفیت سرویس	توزیعی	جمع وزن‌دار	چند اعتمادی	رخدادمحور
	[۲۰]	کیفیت سرویس	توزیعی	جمع وزن‌دار	تک اعتمادی	رخدادمحور
	[۹]	کیفیت سرویس	متمرکز	جمع وزن‌دار ایستا	چند اعتمادی جمع وزن‌دار ایستا	زمان‌محور
اعتماد ترکیبی	[۱۱]	کیفیت سرویس	توزیعی/ متمرکز	جمع وزن‌دار پویا	چند اعتمادی با جمع وزن‌دار پویا	رخدادمحور
	[۱۰]	کیفیت سرویس	توزیعی	دمپستر-شیفر	تک اعتمادی	رخدادمحور

جدول ۱ به‌طور خلاصه تمامی کارهای انجام شده در زمینه محاسبه اعتماد در اینترنت اشیا را نمایش می‌دهد.

۳- روش پیشنهادی محاسبه اعتماد: Trusty

با توجه به گستردگی کاربردهای اینترنت اشیا، انواع سناریوهای تعاملات ممکن بین اشیا و بین سرویس‌ها در اینترنت اشیا به‌صورت زیر قابل دسته‌بندی است:

۱) سرویس‌گیری: در این سناریو تعدادی سرویس‌گیرنده و تعدادی فراهم‌کننده سرویس وجود دارند. سرویس‌گیرنده‌ها برای هدف و کاربرد خود، با استفاده از اعتماد از بین فراهم‌کننده‌های سرویس، موردی را انتخاب می‌کنند. سناریو های تعاملات اعتماد در کارهای [۹-۶]، [۱۶-۱۵] و [۲۶] و [۲۸] از این دسته هستند.

۲) جمع‌آوری داده در سکوی مرکزی: در این سناریو، دسته‌ای از اشیا به‌عنوان جمع‌کنندگان داده، داده‌هایی را از محیط فیزیکی جمع می‌کنند و برای سکوی سرویس به صورت جریانی یا بنا به درخواست می‌فرستند. در این سناریو سکوی مرکزی اعتماد هر یک از موجودیت‌های ارسال‌کننده داده را محاسبه می‌کند. سناریوی تعاملات اعتماد در کارهای [۴]، [۵] و [۲۰] و [۲۵] و [۲۷] از این دسته است.

۳) اعلان هشدار و رخداد: در این سناریو عده‌ای اعلان‌دهنده با ارسال اعلان به دسته‌ای شنونده باعث می شوند تا شنونده‌ها از اعلان‌ها استفاده کنند. شنونده‌ها آماده هستند تا دسته‌ای از رخدادها را که شنونده آن هستند؛ دریافت کنند. سناریوی تعاملات اعتماد در مرجع [۲۱] از این دسته است.

روش پیشنهادی Trusty، یک روش محاسبه اعتماد ترکیبی بوده و در دسته جمع‌آوری داده در سکوی مرکزی قرار می‌گیرد. به‌این‌ترتیب، محاسبه اعتماد به‌صورت مرکزی در یک سکو انجام می‌شود و بنابراین، محاسبه اعتماد سربار بر روی دستگاه‌ها ایجاد نخواهد کرد. گره‌ها تنها در قالب یک برنامه کاربردی، گزارش‌ها و درخواست‌های خود را ارسال می‌کنند و پاسخ آگاه از اعتماد را از سکوی مرکزی دریافت می نمایند. محاسبه اعتماد در سکوی مرکزی به‌صورت دوره‌ای انجام می‌پذیرد و سربار بر روی دستگاه‌ها ایجاد نمی‌کند. در ادامه، جزئیات مراحل محاسبه اعتماد در دو بخش اعتماد پذیری داده و اعتماد موجودیت تشریح شده و سپس رویکرد Trusty برای انجام هر یک از این دو بخش ارائه می‌شود. در پایان، کاربرد Trusty برای محاسبه اعتماد در یک سیستم پارکینگ هوشمند بیان می‌شود.

۳-۱- مراحل محاسبه اعتماد ترکیبی در اینترنت اشیا

در مبحث تأمین امنیت و اعتمادپذیری، طیف متنوعی از انواع حملات امنیتی قابل تصور است؛ از جمله، حملات تحریف اعتماد (حمله دروغ‌گویی، روشن-خاموش، خود ارتقایی، آراء تقلبی) [۳] و احتمال دست‌کاری داده‌ها در سکو مرکزی. لازم است تأکید شود که روش پیشنهادی در این بخش به بررسی این نوع حملات و مقابله با آن‌ها نمی‌پردازد. در واقع، فرض بر این است یک مکانیزم تشخیص نفوذ در سیستم استقرار دارد و قادر است این نوع از حملات را شناسایی کند. در عوض، تمرکز راهکار ارائه شده به‌طور خاص روی مقوله محاسبه اعتماد برای کاربردهای اینترنت اشیاء است.

در اغلب کاربردهای اینترنت اشیا جامعیت داده و اعتبار کسی که آن را تولید کرده است؛ هر دو حائز اهمیت هستند. برای مثال، به‌دست آوردن اطلاعات امن و مطمئن درباره وضعیت یک تصادف از راننده تاکسی یا مسافران آن، نسبت به کسب اطلاعات از یک مأمور پلیس اهمیت بیشتری دارد زیرا نیاز به کمک گرفتن از متخصصین پزشکی و سایر نهادهای مرتبط به سریع‌ترین نحو وجود دارد [۴]. در روش‌های محاسبه اعتماد در اینترنت اشیا متداول است که اعتمادپذیری داده، که در این مثال مطمئن و امن بودن اطلاعات تصادف است برابر با اعتماد موجودیت تولیدکننده این داده، که همان راننده تاکسی و مأمور پلیس هستند در نظر گرفته شود. با توجه به مثال ذکر شده، این فرض کاملاً درست نیست و نیاز است که اعتمادپذیری داده و اعتماد موجودیت هر دو در یک کاربرد اینترنت اشیا محاسبه شوند. در این مقاله برای محاسبه اعتماد از ترکیب اعتماد موجودیت و اعتمادپذیری داده استفاده می‌شود.

۳-۱-۱- اعتمادپذیری داده

هدف از محاسبه اعتمادپذیری داده این است که درستی یا عدم درستی یک پدیده که در مورد آن گزارش‌ها یا بازخوردهایی از موجودیت‌ها دریافت شده است؛ مشخص شود. اعتمادپذیری داده از دو قسمت اصلی وزن‌دهی گزارش‌ها و ادغام گزارش‌ها تشکیل شده است که در ادامه هر یک توضیح داده شده است.

- **وزن‌دهی گزارش:** هدف این قسمت این است که با توجه به عوامل تعیین کننده صحت یک گزارش و با تخصیص یک وزن به آن گزارش، مشخص شود که به چه میزان می‌توان به این گزارش اطمینان داشت.
- **ادغام گزارش‌ها:** هدف این قسمت این است که با توجه به میزان اطمینان هریک از گزارش‌های ارسال شده (بر اساس وزن)، با ادغام آن‌ها مشخص کند که اعتماد به پدیده مذکور چقدر است. ممکن است هدف ما در یک کاربرد تنها به دست آوردن میزان صحت یک گزارش باشد که در این صورت نیازی به استفاده از ادغام نخواهد بود و تنها به دست آوردن وزن گزارش کفایت می‌کند.

۳-۱-۲- اعتماد موجودیت

منظور از اعتماد موجودیت، اعتماد به گره‌هایی است که گزارش‌ها و بازخوردهایی را در یک سیستم اینترنت اشیا ارائه می‌دهند. در مثال گزارش دی‌اکسید نیتروژن موجود در هوا، موجودیت‌ها همان حس‌گرهای کاربران است که گزارش را ارائه می‌دهند. محاسبه اعتماد موجودیت از دو قسمت اصلی تشکیل شده‌است:

- **صحت‌سنجی گزارش‌ها:** با توجه به اینکه تعامل موجودیت مرکزی محاسبه اعتماد با کاربران تنها از طریق به اشتراک‌گذاری گزارش‌های آن‌ها ا ست؛ هدف از این ق سمت این ا ست که بتوان تعداد به ا شتراک‌گذاری‌ها یا گزارش‌های صحیح و غلط هریک از گره‌ها یا موجودیت‌ها را به دست آورد.
- **به‌روزرسانی:** با توجه به اینکه هر موجود یت چه تعداد به اشتراک‌گذاری صحیح و به اشتراک‌گذاری اشتباه دارد، مقدار اعتماد موجودیت با توجه به روش محاسباتی که برای محاسبه اعتماد موجودیت در نظر گرفته شده‌است؛ به‌روزرسانی می‌شود.

۳-۲- محاسبه اعتماد در Trusty

در این بخش به شرح جزئیات روش پیشنهادی برای محاسبه هریک از مراحل یاد شده پرداخته شده ا ست. نمادهای مورد ا ستفاده در روش پیشنهادی Trusty در جدول ۲ ارائه شده است.

جدول ۲: نمادهای استفاده شده در روش پیشنهادی

نماد	توضیح
R_i	i امین گزارش
N_k	k امین گره گزارش‌دهنده
t	زمان تولید گزارش
l	مکان تولید گزارش
$\mu_t(R_i)$	اطلاعات زمینه زمانی گزارش i ام
$\mu_l(R_i)$	اطلاعات زمینه مکانی گزارش i ام
$\mu_e(R_i, N_k)$	اطلاعات زمینه ویژگی گزارش‌دهنده گزارش i ام ارائه‌شده توسط گره k ام
$w_k^{l,t}(R_i)$	وزن گزارش R_i توسط گره N_k در زمان t و مکان l
T_d	اعتمادپذیری داده
N_f	تعداد گزارش‌های درست یک گره
N_g	تعداد گزارش‌های نادرست یک گره
σ_f	احتمال خطای منفی کاذب
σ_g	احتمال خطای مثبت کاذب
$T_e(N_k)$	اعتماد موجودیت گره N_k

با توجه به اینکه Trusty یک روش ترکیبی اســت، در دو بخش اعتمادپذیری داده و اعتماد موجودیت به بررســی جزئیات آن پرداخته شده‌است. در این روش، انتشار اعتماد به‌صورت مرکزی انجام می‌شود و عمل به‌روزرسانی اعتماد به‌صورت زمان‌محور انجام می‌شود.

۳-۲-۱- محاسبه اعتمادپذیری داده در Trusty

در روش پیشــنهادی، پارامترهای زمان (t)، مکان (l) و ویژگی‌های موجودیت (N_k) به‌عنوان عوامل زمینه تأثیرگذار بر اعتمادپذیری داده در نظر گرفته شــده‌اند. ازآنجاکه در برخی از کاربردهای اینترنت اشــیا و ضعیت یک پدیده ممکن ا ست با گذ شت زمان تغییر کند، نیاز ا ست عامل زمان به‌عنوان یکی از عوامل تأثیرگذار در نظر گرفته شــود و تأثیر بازخوردها و گزارش‌های اخیر بیش‌تر از گزارش‌های قدیمی باشــد. همچنین عامل زمینه‌ای مکان گزارش با توجه به کاربرد می‌تواند تأثیرگذار باشــد. عامل مهم زمینه‌ای دیگر، ویژگی موجودیت اســت. با توجه به کاربرد، هر موجودیت با توجه به نوع یا مرتبه آن ممکن اســت گزارش دقیق‌تری ارائه دهد. برای مثال، ممکن است موجودیت موردنظر دارای حس‌گرهای مجهزتر و به‌روزتری باشــد یا در طبقه‌بندی موجودیت‌ها در طبقه بالاتری قرار گیرد.

برای تولید اطلاعات زمینه، قســمتی تحت عنوان پیش‌پردازش وجود دارد که اطلاعات خام مانند زمان (t)، مختصات جغرافیایی یا هر مقداری که نشــان‌دهنده مکان تولید گزارش یا بازخورد باشــد (l) و شناسه موجودیت تولیدکننده این گزارش یا بازخورد (N_k) را به‌عنوان ورودی می‌گیرد و عملیات اســتنتاج زمینه را انجام می‌دهد. برای هر پدیده، گزارش i ام در مورد آن با R_i مشــخص شــده اســت. اطلاعات زمینه استنتاج شده برای عامل زمان گزارش R_i با $\mu_t(R_i)$، عامل مکان گزارش R_i با $\mu_l(R_i)$ و عامل ویژگی موجودیت گزارش R_i که توســط گره N_k ارائه شده، با $\mu_e(R_i, N_k)$ مشخص شده است.

وزن دهی گزارش: با توجه به اینکه اعتماد موجود یت و عامل زمینه‌ای ویژگی موجودیت (μ_e)، وابسته به رفتار و ویژگی گره هستند؛ و عوامل زمینه مکان و زمان، با توجه به کاربرد، به شــرایط زمینه آن کاربرد وابســته می‌شــوند؛ در Trusty برای محاســبه وزن و تجمیع این عوامل از تابع جمع وزن‌دار ا ستفاده شده ا ست. $w_k^{l,t}(R_i)$ وزن گزارش R_i اســت که توســط گره N_k در زمان t و در مکان l ارائه شــده اســت. اعتماد موجودیت برای گره k ام که گزارش R_i را ارائه کرده اســت، با $T_e(N_k)$ مشخص شده است.

رابطه (۱) نشــان‌دهنده وزن حاصــل از تجمیع عوامل زمینه و اعتماد موجودیت برای گزارش R_i ارائه شده توسط گره N_k است.

$$w_k^{l,t}(R_i) = \alpha\big(T_e(N_k) * \mu_e(R_i, N_k)\big) + \beta\big(\mu_l(R_i)\big) + \gamma\big(\mu_t(R_i)\big) \quad (۱)$$

بدیهی ا ست که $\alpha + \beta + \gamma = 1$ و با توجه به اهمیت بالاتر اعتماد موجودیت نسبت به عوامل زمینه، باید رابطه $\alpha > \beta + \gamma$ برقرار باشد.

ادغام گزارش‌ها: بعد از تعیین وزن هر یک از گزارش‌ها، برای به دســت آوردن اعتمادپذیری داده باید تمامی گزارش‌های مربوط به آن پدیده با توجه به وزن محاسبه شده برای آن‌ها با یکدیگر ترکیب شوند. در کاربردهای اینترنت ا شیا ح سگرها دارای دقت‌های متفاوت ه ستند که این امر زمینه‌ســاز عدم قطعیت در داده‌ها خواهد بود. با توجه به اینکه نظریه دمپستر-شیفر برای کاربردهای دارای عدم قطعیت مناسب ا ست، از این نظریه در Trusty ا ستفاده شده ا ست. در نظریه دمپستر-شــیفر هنگامی‌که یک موجودیت بازخوردی مبنی بر قابل اعتماد بودن یک پدیده ارائه می‌دهد، به این معنا ست که این پدیده در صورت قابل اعتماد بودن موجودیت (بالا بودن مقدار $w_k^{l,t}(R_i)$)، قابل اعتماد ا ست

و در غیر این صورت لزوماً غیرقابل‌اعتماد نیست. درواقع نظریه دمپستر-شیفر یک بازه عدم قطعیت باور و مقبولیت ارائه می‌دهد.

فرمول (۲) نشان‌دهنده ترکیب وزن گزارش‌های مختلف با استفاده از قانون ترکیب نظریه دمپستر-شیفر است [۲۲].

$$w_{1,2}(T) = (w_1 \oplus w_2)(T) = \frac{\sum_{R \cap R' = T} w_1^{l,t}(\mathrm{R})\, w_2^{l,t}(R')}{1 - \sum_{R \cap R' = \emptyset} w_1^{l,t}(\mathrm{R})\, w_2^{l,t}(R')} \quad (۲)$$

در فرمول (۲) $w_{1,2}(T)$ مشخص‌کننده وزن قابل‌اعتماد بودن یا تأیید پدیده موردنظر است که از ترکیب وزن گزارش‌های R و R' که به ترتیب توسط گره ۱ و گره ۲ در زمان t و در مکان l ارائه شده‌اند، به دست می‌آید. درصورتی‌که گزارش‌های R و R' هر دو مبنی بر تأیید پدیده یا قابل اعتماد بودن آن باشند، صورت این کسر برابر با حاصل‌ضرب وزن‌های $w_1^{l,t}(R)$ و $w_2^{l,t}(R')$ است. درصورتی‌که اشتراک گزارش‌های R و R' تهی باشد، مخرج ترکیب دمپستر-شیفر برای نرمال کردن برابر حاصل‌ضرب وزن‌های $w_1^{l,t}(R)$ و $w_2^{l,t}(R')$ است. به همین ترتیب $w_{1,2}(\bar{T})$ برای غیر قابل‌اعتماد بودن یا رد پدیده موردنظر محاسبه خواهد شد. همین‌طور $w_{1,2}(U)$ نشان‌دهنده عدم وجود دانش کافی یا حالت ندانستن وضعیت پدیده موردنظر خواهد بود. با توجه به نرمال شدن مقادیر به‌دست‌آمده، بدیهی است که حاصل جمع $w_{1,2}(T)$ و $w_{1,2}(\bar{T})$ و $w_{1,2}(U)$ که به ترتیب نشان‌دهنده وزن صحت، عدم صحت و عدم وجود دانش کافی در مورد یک پدیده هستند، برابر با یک خواهد بود. فرمول (۲) نشان‌دهنده ترکیب دمپستر- شیفر برای گزارش‌های دو گره است. به همین ترتیب $w_{1,2}(T)$ با گزارش گره‌های بعدی ترکیب خواهد شد تا درنهایت تمامی گزارش‌های مربوط به پدیده با یکدیگر ترکیب شده و اعتمادپذیری داده یا T_d برای این پدیده محاسبه گردد.

در مرجع [۱۲] روشی برای هموارسازی نتایج حاصل از استفاده از نظریه دمپستر-شیفر ارائه شده است. در این کار یک جریمه برای تغییرات زیاد در ورودی در نظر گرفته شده است. این جریمه باید بر روی وزن محاسبه شده برای هر گزارش یا بازخورد یک موجودیت در مورد یک پدیده اعمال شود تا نوسان نتیجه نهایی کاهش یابد.

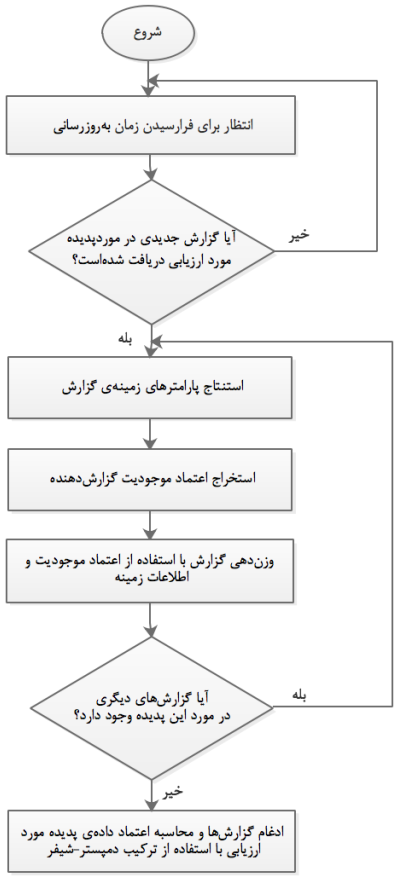
درصورتی که با توجه به کاربرد، امکان وقوع این تغییرات در ورودی‌ها وجود داشته باشد، می‌توان پس از وزن‌دهی، از فرمول (۳) برای به دست آوردن مقدار جریمه و هموار کردن نتیجه استفاده کرد. $d(R_i, R_{i-1})$ نشان‌دهنده اختلاف دو گزارش یا بازخورد متوالی یک موجودیت است که به بیشینه این مقدار نرمال شده است و با ضرب در مقدار قبلی وزن محاسبه شده تشکیل جریمه را می‌دهد. این اختلاف فاصله اقلیدسی بین گزارش‌ها است. این مقدار جریمه از مقدار وزن محاسبه شده $w_k^{l,t}(R_i)$ کسر می‌شود.

$$penalty = \left[w_k^{l,t}(R_i) \times \frac{d(R_i, R_{i-1})}{\max\left(d(R_i, R_{i-1})\right)} \right] \quad (۳)$$

شکل ۲ نشان‌دهنده نمودار روند محاسبه اعتمادپذیری داده در روش پیشنهادی است.

۳-۲-۲- محاسبه اعتماد موجودیت در Trusty

روش‌های متنوعی برای تجمیع اعتماد وجود دارد که از جمله متداول‌ترین آن‌ها می‌توان به روش جمع وزن‌دار (با وزن‌های ایستا یا پویا)، استنتاج بیزی، نظریه باور و روش فازی اشاره کرد. مزیت روش جمع وزن‌دار سادگی کارکرد آن است ولی نارسایی آن در این است که در حضور رفتارهای مخرب با درصد بالا عملکرد مناسبی نخواهند داشت. روش فازی در موقعیت‌های دارای ابهام که ارائه یک مقدار عددی دقیق، دشوار است، با استفاده از متغیرهای زبانی، فرآیند تصمیم‌گیری را تسهیل می‌کند و می‌تواند برای کاربرد اعتماد مناسب باشد، اما چالش اصلی آن، ارائه تابع عضویت است. در روش نظریه باور، مشخص کردن جرم باور پایه یکی از چالش‌ها است. هم‌چنین روش‌های مبتنی بر نظریه باور مانند دمپستر- شیفر بیش‌تر برای به دست آوردن اعتماد در حالتی که تعامل مستقیم وجود ندارد مورد استفاده قرار می‌گیرد.



شکل ۲: جریان کاری محاسبه اعتمادپذیری داده در Trusty

در کارهای انجام شده در اینترنت اشیا، برای محاسبه اعتماد موجودیت‌ها که تعامل مستقیم با آن‌ها وجود دارد، بیش‌تر از روش‌های بیزی استفاده شده‌است. در Trusty با توجه به اینکه رفتار گره‌ها در

کاربردهای ذکر شده محدود به ارسال و ارائه اطلاعات است؛ برای محاسبه اعتماد موجودیت از روش ارائه شده در مرجع [۲۳] که مبتنی بر یادگیری بیزین برای شبکه‌های دارای همیاری است، استفاده شده است. در این روش شهرت هر یک از موجودیت‌ها با توجه به رفتار قبلی آن‌ها در طی زمان یاد گرفته می‌شود.

در این روش l سطح از شهرت در نظر گرفته شده است. مجموعه شهرت‌ها با $\mathbb{R}$ نشان داده می‌شود و دارای l عضو است؛ هر یک از سطوح شهرت با $\mathbb{R}_l$ مشخص می‌شود. N_g و N_f به ترتیب نشان‌دهنده تعداد گزارش‌های صحیح و تعداد گزارش‌های غلط ارائه شده توسط گره مورد ارزیابی در مورد یک پدیده است. برای تشخیص اینکه آیا یک گزارش صحیح بوده یا اشتباه، از اعتمادپذیری داده پدیده موردنظر که در قسمت قبل بررسی شد استفاده می‌شود.

در این روش، احتمال هر یک از l سطح شهرت با استفاده از فرمول (۴) محاسبه می شود. در اینجا، $P_{N_k}^t(r=\mathbb{R}_l)$ نشان‌دهنده احتمال برابری شهرت با سطح $\mathbb{R}_l$ برای گره N_k در زمان به‌روزرسانی t ام است و برای هریک از سطوح این احتمال محاسبه می‌شود. با توجه به اینکه به‌روزرسانی اعتماد در Trusty زمان‌محور است، $P_{N_k}^{t-1}(r=\mathbb{R}_l)$ نشان‌دهنده احتمال محاسبه شده برای این سطح از شهرت گره N_k در به‌روزرسانی قبلی است.

فرمول (۴) احتمال اینکه سطح شهرت گره N_k در زمان به‌روزرسانی t ام برابر با $\mathbb{R}_l$ باشد را نشان می‌دهد.

(۴)

$$P_{N_k}^t(r=\mathbb{R}_l)=\frac{P_{N_k}^{t-1}(r=\mathbb{R}_l)\left[\mathbb{R}_l{\sigma_f}^{N_f}(1-\sigma_f)^{N_g}+(1-\mathbb{R}_l){\sigma_g}^{N_g}(1-\sigma_g)^{N_f}\right]}{\sum_{\mathbb{R}_l\in\mathbb{R}}P_{N_k}^{t-1}(r=\mathbb{R}_l)\left[\mathbb{R}_l{\sigma_f}^{N_f}(1-\sigma_f)^{N_g}+(1-\mathbb{R}_l){\sigma_g}^{N_g}(1-\sigma_g)^{N_f}\right]}$$

پس از محاسبه $P_{N_k}^t(r=Rep_l)$ برای هر یک از سطوح شهرت، با استفاده از یک جمع وزن‌دار که وزن‌ها برابر با سطوح شهرت هستند، مقدار اعتماد N_k به یکی از l سطح شهرت همگرا شده و اعتماد موجودیت محاسبه می‌شود. فرمول (۵) نشان‌دهنده نحوه محاسبه اعتماد موجودیت با استفاده از احتمال هر یک از سطوح شهرت، برای گره N_k است.

$$T_e(N_k)=\sum_{Rep_l\in Rep}Rep_l.P_{N_k}^t(r=Rep_l) \qquad (۵)$$

در هر بار به‌روزرسانی، اعتماد موجودیت برای تمامی موجودیت‌ها به ازای گزارش یا اندازه‌گیری‌های جدیدی که ارائه کرده‌اند محاسبه می‌شود. روندنمای نشان دهنده شیوه محاسبه اعتماد موجودیت در شکل ۳ نشان داده شده است.

۴- مطالعه موردی: محاسبه اعتماد در پارکینگ هوشمند

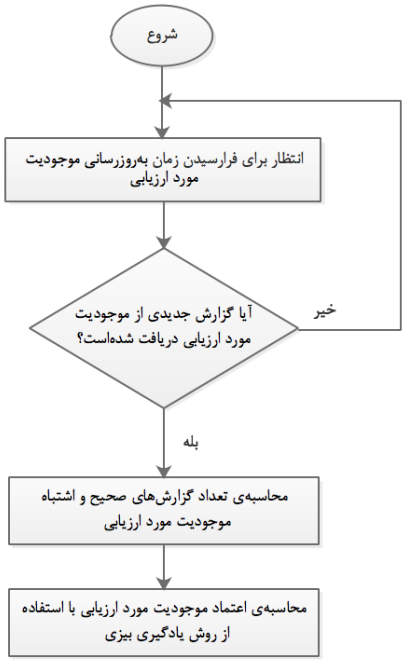
یکی از سرویس‌های کلیدی که در شهر باید مدیریت شود، امکانات پارکینگ و ترافیک است. برای مدیریت پارکینگ، حسگرهای هوشمند جهت نصب در فضای پارکینگ جهت اعلام وضعیت فضای اشغال شده مورد نیاز است. هم‌چنین می‌بایست داده‌های جمع‌آوری شده برای به دست آوردن دید عملی پردازش شوند [۲۴].

۴-۱- مشخصات پارکینگ هوشمند

در پارکینگ هوشمند موردنظر، تعدادی جایگاه پارک مجهز به حس‌گر بی‌سیم وجود دارند. علاوه بر این، تعدادی کاربر که دارای خودرو هستند، به‌عنوان موجودیت‌های سیستم در نظر گرفته شده‌اند. حس‌گرهایی که در هر جایگاه تعبیه شده‌اند، با ورود/خروج ماشین به/از جایگاه، تغییر وضعیت را به‌صورت داده دودویی موجودیت مرکزی اطلاع می‌دهند. هر کاربر پیش از رسیدن به مقصد، با کمک یک برنامه کاربردی مقصد خود را مشخص کرده و درخواستی برای پیدا کردن جایگاه پارک مناسب برای موجودیت مرکزی ارسال می‌کند. موجودیت مرکزی با بررسی این درخواست؛ لیستی از جایگاه‌های مناسب به همراه ویژگی آن‌ها را به کاربر ارائه می‌دهد تا کاربر با توجه به ترجیحات خود، یک جایگاه را انتخاب کند. در این پژوهش سه ویژگی دسترس‌پذیری، ایمنی و سهولت پارک به‌عنوان ویژگی‌های یک جایگاه در نظر گرفته شده‌اند.

۴-۲- کاربرد اعتماد در پارکینگ هوشمند

ممکن است کاربران بدخواهی وجود داشته باشند که گزارش‌های غیرواقعی در مورد ویژگی‌های جایگاه‌ها ارائه دهند. بنابراین نیاز است که اعتماد برای هر یک از موجودیت‌ها محاسبه شود.



شکل ۳: روندنمای محاسبه اعتماد موجودیت در Trusty

علاوه بر ضرورت وجود اعتماد موجودیت، به دلیل اینکه داده‌ها و گزارش‌های تولید شده توسط کاربران در مورد هر یک از ویژگی‌های جایگاه‌ها، ممکن است نادرست باشند و موجودیت مرکزی با استناد به همین گزارش‌ها در مورد کیفیت ویژگی‌های جایگاه‌ها استنتاج انجام می‌دهد، نیاز است تا اعتماد به داده‌های استنتاج شده توسط موجودیت مرکزی محاسبه شود. اعتمادپذیری داده باید برای تمامی ویژگی‌های

یک جایگاه محا سبه شود. مدل رفتاری کاربران بدخواه در این سناریو به این صورت است که این کاربران در نواحی که رفت‌وآمد بیش‌تری دارند، برای حفظ نظم یا یافتن جای پارک سریع‌تر، رفتار بهتری دارند ولی در سایر نواحی، همواره رفتار خصمانه داشته و بازخوردهای غیرواقعی می‌دهند.

۴-۳- اطلاعات زمینه‌ای در محاسبه اعتماد

در این سناریو عوامل زمینه‌ای مکان و ویژگی های موجودیت در محاسبه اعتماد مورد استفاده قرار می‌گیرند. تابع ضابطه‌ای محاسبه مکان برای گزارش R_i توسط کاربر N_k در فرمول (۶) نشان داده شده است.

$$\mu_l(R_i,N_k)=\begin{cases}1, & l\in home(N_k)\\ 0.2, & l\notin home(N_k)\end{cases} \quad (۶)$$

عامل ویژگی موجودیت برای سناریو پارکینگ هوشمند به صورت یک ماتریس تعریف شده است که در آن کاربران بر اساس نوع گواهی نامه و ابعاد ماشین خود به پنج کلاس تقسیم‌بندی شده‌اند و موجودیت هر کلاس، که همان کاربران هستند؛ دارای ویژگی‌های متفاوتی خواهند بود. جدول ۳ نشان‌دهنده عامل زمینه‌ای ویژگی موجودیت در سناریو پارکینگ هوشمند است. نکته‌ای که باید در رابطه با تنظیم مقادیر عددی برای پارامترهای زمینه‌ای روش پیشنهادی به آن توجه داشت این است که فرض بر این بوده که در هر سناریوی کاربردی که قرار به استفاده از راهکار پیشنهادی باشد، می‌توان مقادیر مناسب را بر اساس دانش موجود در حوزه مربوطه و نیز کسب آراء افراد خبره به نحو تجربی تعیین نمود. کلیت و چارچوب روش پیشنهادی فارغ از مقادیر پارامترهای ثابت آن، قابل به‌کارگیری است و در عمل، تنها نیاز به تعیین موردی آن‌ها می‌باشد.

جدول ۳: کلاس‌های عامل زمینه‌ای ویژگی‌های موجودیت

	دسترس‌پذیری	ایمنی	سهولت پارک
کلاس ۱	۰/۸	۰/۸	۰/۸
کلاس ۲	۰/۸	۰/۸	۱
کلاس ۳	۰/۸	۰/۸	۰/۶
کلاس۴	۰/۸	۰/۶	۰/۶
کلاس۵	۱	۱	۰/۶

در قدم بعدی باید ضرایب تابع تشکیل وزن اعتمادپذیری داده مشخص شود. تابع تشکیل وزن اعتمادپذیری داده در فرمول (۷) نشان داده شده است.

$$w_k(R_i)=0.7*\left(T_e(N_k)*\mu_e(R_i,N_k)\right)+0.3*\left(\mu_l(R_i,N_k)\right) \quad (۷)$$

۴-۴- محاسبه اعتماد موجودیت

برای محاسبه اعتماد موجودیت در روش پیشنهادی از یک روش مبتنی بر یادگیری بیزی استفاده شده است که سطوح مختلفی از شهرت را در نظر می‌گیرد. در این سناریو، سه سطح شهرت در نظر گرفته شده است: شهرت بالا که به‌منزله قابل اعتماد بودن موجودیت است برابر با ۰/۹۵، شهرت پایین که به‌منزله غیرقابل‌اعتماد بودن موجودیت است برابر با ۰/۰۵ و شهرت متوسط که نشان‌دهنده حالت بی‌طرفی است برابر با ۰/۵۰ در نظر گرفته شده است.

۵- ارزیابی و تحلیل نتایج

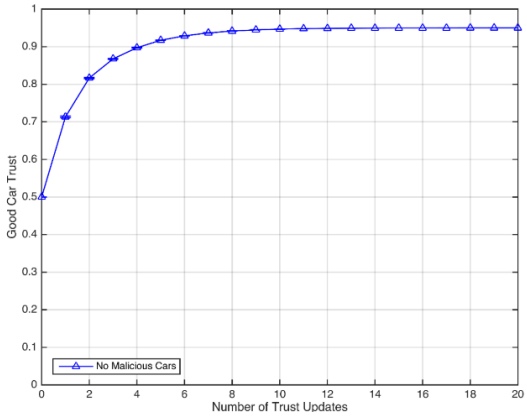
در این بخش با انجام شبیه سازی سناریوی پارکینگ هوشمند، کارایی Trusty مورد ارزیابی قرار می‌گیرد. برای رسیدن به این هدف از یک شبیه‌ساز مبتنی بر نرم‌افزار MATLAB استفاده شده و روش پیشنهادی با روش ارائه شده در مرجع [۹] مقایسه شده است. خروجی که صحت آن مورد ارزیابی قرار می‌گیرد، اعتماد پذیری داده و اعتماد موجودیت محاسبه شده با استفاده از روش Trusty است. اعتمادپذیری داده برای هر یک از سه ویژگی جایگاه‌ها محاسبه می شود. اعتماد موجودیت نیز برای کاربران محاسبه شده تا موجودیت‌های خوش‌رفتار از موجودیت های مخرب تشخیص داده شوند. نتایج با تکرار ۳۳ بار برای هر آزمایش و در بازه اطمینان ۹۵٪ به‌دست‌آمده‌اند. پارامترهای مورد استفاده در شبیه سازی سناریوی پارکینگ هوشمند برای روش پیشنهادی و روش مقایسه در جدول ۴ ارائه شده است.

جدول ۴: پارامترهای شبیه‌سازی

متغیر	مقدار
تعداد کاربرها	۴۰
تعداد جایگاه‌ها	۱۰۰
تعداد ناحیه‌ها	۴
درصد کاربرهای مخرب	[٪۷۰-۰]
درصد جایگاه‌های غیرامن	[٪۲۰-۰]
درصد جایگاه‌های دشوار برای پارک	[٪۳۰-۰]
درصد جایگاه‌های دارای حس‌گر مختل	[٪۲۰-۰]
آستانه اعتماد	۰/۶
تعداد به‌روزرسانی‌های اعتماد	۵۰
مقدار σ_f و σ_g	۰/۲
مقدار α	۰/۷
مقدار β	۰/۳

۵-۱- نمایش صحت کارکرد Trusty

هدف از این آزمایش، نمایش صحت کارکرد روش پیشنهادی بدون حضور رفتارهای مخرب و با فرض مناسب بودن تمامی جایگاه‌های پارک است. به این منظور، نمودارهای مربوط به اعتماد موجودیت و اعتماده داده محاسبه شده، آورده شده‌است. در شکل ۴ اعتماد موجودیت که همان اعتماد ماشین‌های خوش‌رفتار است نشان داده شده است. شکل ۴ نشان دهنده میانگین اعتماد تمامی ماشین‌های خوش‌رفتار سیستم است. مقدار اولیه اعتماد برای تمامی گره‌ها ۰/۵۰ در نظر گرفته شده است. همان‌طورکه در شکل ۴ مشاهده می‌شود، در حالتی که هیچ رفتار مخربی وجود ندارد اعتماد محاسبه شده برای ماشین‌ها از مقدار ۰/۵ به ۰/۹۵ همگرا می‌شود.



شکل ۴: اعتماد ماشین‌ها بدون حضور رفتارهای مخرب

۵-۲- تأثیر رفتارهای مخرب بر همگرایی اعتماد

هدف از این آزمایش، نمایش عملکرد روش پیشنهادی در حضور رفتارهای مخرب و میزان دقت همگرایی روش با در نظر گرفتن رفتارهای مخرب است. به این منظور، با در نظر گرفتن میزان متفاوتی از رفتارهای مخرب و همچنین با در نظر گرفتن میزان متفاوتی از جایگاه‌های نامناسب (غیرامن، مجهز به حسگر دارای نقص، دشوار برای پارک) به بررسی کارکرد روش پیشنهادی پرداخته شده است.

۵-۲-۱- اعتماد موجودیت

در این قسمت اعتماد موجودیت برای ماشین‌های خوش‌رفتار و ماشین‌های مخرب محاسبه شده است. نتایج نشان داده شده در این قسمت، به ازای حالتی که ۳۰٪ از جایگاه‌ها نامناسب هستند و ۱۰٪ الی ۷۰٪ از ماشین‌ها رفتار مخرب دارند، به‌دست‌آمده است. شکل ۵ نشان‌دهنده اعتماد ماشین‌های خوش‌رفتار در حضور رفتارهای مخرب است.

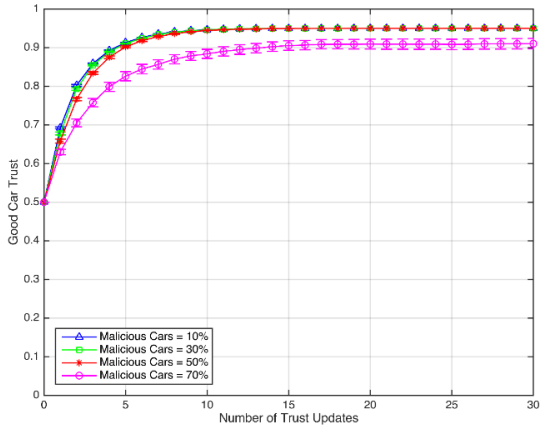
در شکل ۵، تا زمانی که ۵۰٪ رفتار مخرب در سیستم وجود دارد، مقدار اعتماد ماشین‌های خوش‌رفتار دقیقاً به مقدار ۰/۹۵ که سطح بالای اعتماد در نظر گرفته شده است همگرا می‌شود. در حالتی که ۷۰٪ رفتار مخرب در سیستم وجود دارد، به مقداری بالاتر از ۰/۹ همگرا می‌شود که قابل قبول است. دلیل اینکه روش پیشنهادی در حضور بیشترین تعداد گره‌های مخرب نیز مقدار اعتماد را به‌درستی محاسبه می‌کند، تنظیمی است که برای پارامترهای σ_f و σ_g در نظر گرفته شده‌است. اگر مقدار σ_f و σ_g بیشتر از مقدار تعیین شده باشند، به این معنا است که احتمال خطای مثبت کاذب و منفی کاذب در تشخیص صحت گزارش‌ها بیشتر است، بنابراین اعتماد موجودیت به مقدار کمتری همگرا خواهد شد.

با شرایط ذکر شده، شکل ۶ نشان‌دهنده اعتماد ماشین‌های مخرب در حضور رفتارهای مخرب است. در شکل ۶ تا حالتی که ۵۰٪ رفتار مخرب در سیستم وجود دارد، مقدار اعتماد ماشین‌های مخرب دقیقاً به مقدار ۰/۰۵ که سطح پایین اعتماد در نظر گرفته شده است همگرا می‌شود. در حالتی که ۷۰٪ رفتار مخرب در سیستم وجود دارد، به مقداری کم‌تر از ۰/۱ همگرا می‌شود که قابل قبول است.

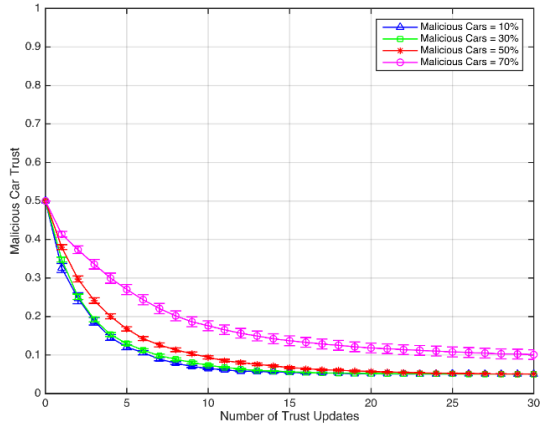
۵-۲-۲- اعتمادپذیری داده

در این قسمت اعتمادپذیری داده برای سه ویژگی در نظر گرفته شده محاسبه می‌شود. برای هر یک از ویژگی‌ها، یک نمودار نشان‌دهنده اعتماد به وجود این ویژگی، برای جایگاه‌هایی که این ویژگی را دارند، و یک نمودار نشان‌دهنده بی‌اعتمادی به وجود این ویژگی، برای جایگاه‌هایی که این ویژگی را ندارند، در نظر گرفته شده است. نتایج این قسمت، به ازای حالتی که ۳۰٪ از جایگاه‌ها نامناسب هستند و ۱۰٪ الی ۷۰٪ از ماشین‌ها رفتار مخرب دارند، به‌دست‌آمده است.

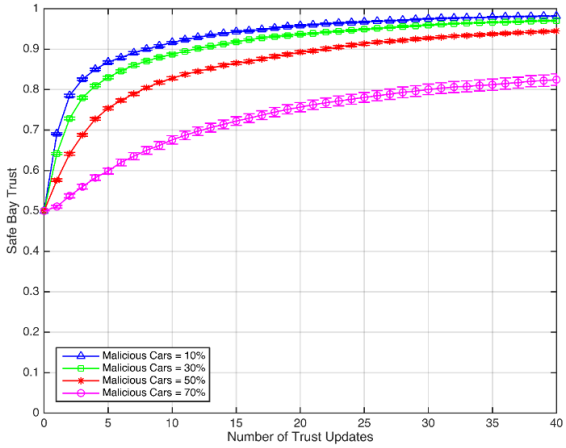
شکل ۷ نشان‌دهنده اعتماد پذیری داده ویژگی ایمنی برای جایگاه‌های امن در حضور رفتارهای مخرب است. با توجه به شکل ۷، مقدار همگرایی اعتمادپذیری داده محاسبه شده برای ویژگی ایمنی جایگاه‌های امن با افزایش در صد حضور رفتارهای مخرب در سیستم، کاهش پیدا می‌کند. در بیش‌ترین حالت رفتارهای مخرب یعنی با حضور ۷۰٪ رفتار مخرب مقدار همگرایی نزدیک به ۰/۸ است. با توجه به اینکه آستانه در نظر گرفته شده برای اعتماد برابر با ۰/۶ است می‌توان گفت که محاسبه اعتمادپذیری داده برای این ویژگی کارکرد مناسبی در حضور رفتارهای مخرب دارد.



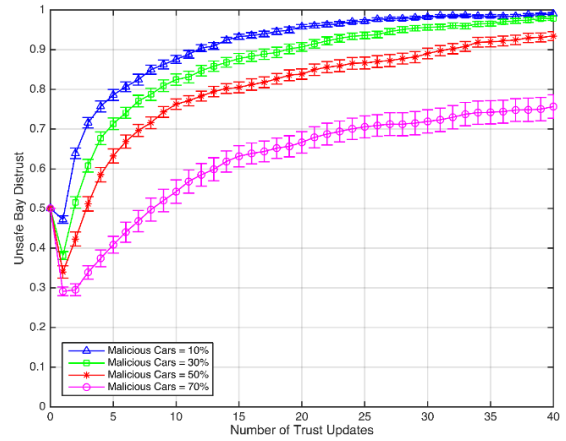
شکل ۵: اعتماد ماشین‌های خوش‌رفتار در حضور رفتارهای مخرب



شکل ۶: اعتماد ماشین‌های بدرفتار در حضور رفتارهای مخرب



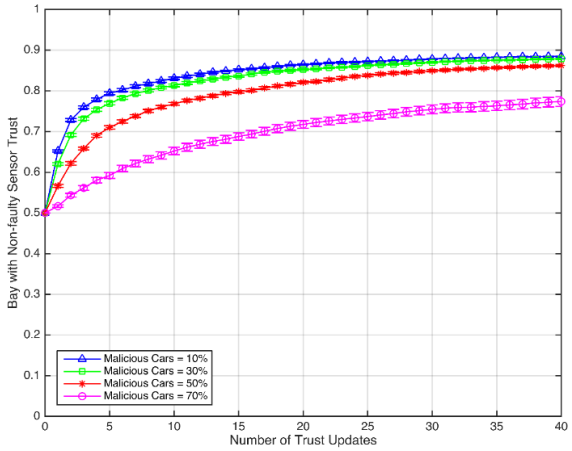
شکل ۷: اعتمادپذیری داده ویژگی ایمنی برای جایگاه‌های امن در حضور رفتارهای مخرب



شکل ۸: اعتمادپذیری داده ویژگی ایمنی برای جایگاه‌های ناامن در حضور رفتارهای مخرب

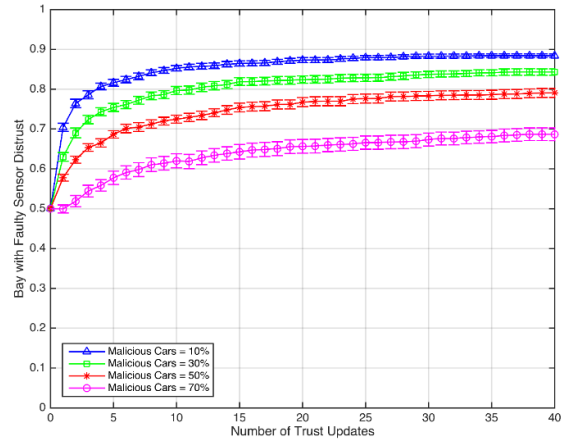
شکل ۸ نشان‌دهنده اعتماد پذیری داده ویژگی ایمنی برای جایگاه‌های ناامن در حضور رفتارهای مخرب است. با توجه به شکل ۸، مقدار همگرایی بی‌اعتمادی محاسبه شده برای ویژگی ایمنی جایگاه‌های ناامن با افزایش درصد حضور رفتارهای مخرب در سیستم، کاهش پیدا می‌کند. در بیش‌ترین حالت رفتارهای مخرب مقدار همگرایی نزدیک به ۰/۷۵ است. با توجه به اینکه آستانه در نظر گرفته شده برای اعتماد برابر با ۰/۶ است می‌توان گفت که محاسبه اعتمادپذیری داده برای این ویژگی کارکرد مناسبی در حضور رفتارهای مخرب دارد.

دومین ویژگی مورد بررسی دسترس‌پذیری جایگاه است. شکل ۹ نشان‌دهنده اعتمادپذیری داده ویژگی دسترس‌پذیری برای جایگاه‌های مجهز به حس‌گرهای سالم در حضور رفتارهای مخرب است. با توجه به شکل ۹، مقدار همگرایی اعتمادپذیری داده محاسبه شده برای ویژگی دسترس‌پذیری برای جایگاه‌های مجهز به حس‌گرهای سالم با افزایش درصد حضور رفتارهای مخرب در سیستم، کاهش پیدا می‌کند. در بیش‌ترین حالت رفتارهای مخرب یعنی با حضور ۷۰٪ رفتار مخرب مقدار همگرایی نزدیک به ۰/۸ است؛ با توجه به اینکه آستانه در نظر گرفته شده برای اعتماد برابر با ۰/۶ است می‌توان گفت که محاسبه اعتمادپذیری داده برای این ویژگی کارکرد مناسبی در حضور رفتارهای مخرب دارد.



شکل ۹: اعتمادپذیری داده ویژگی دسترس‌پذیری برای جایگاه‌های مجهز به حس‌گرهای سالم در حضور رفتارهای مخرب

شکل ۱۰ نشان‌دهنده اعتمادپذیری داده ویژگی دسترس‌پذیری برای جایگاه‌های مجهز به حس‌گرهای معیوب در حضور رفتارهای مخرب است.

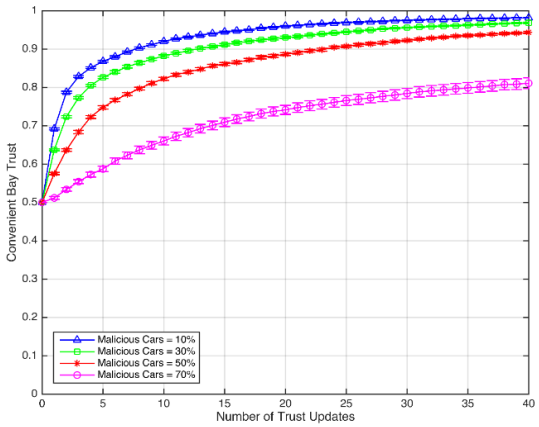


شکل ۱۰: اعتمادپذیری داده ویژگی دسترس‌پذیری برای جایگاه‌های مجهز به حس‌گرهای معیوب در حضور رفتارهای مخرب

با توجه به شکل ۱۰، مقدار همگرایی بی‌اعتمادی محاسبه شده برای ویژگی دسترس‌پذیری جایگاه‌های مجهز به حس‌گرهای معیوب با افزایش درصد حضور رفتارهای مخرب در سیستم، کاهش پیدا می‌کند. در بیش‌ترین حالت رفتارهای مخرب مقدار همگرایی نزدیک به ۰/۶۵ است؛ با توجه به اینکه آستانه در نظر گرفته شده برای اعتماد برابر با ۰/۶ است می‌توان گفت که محاسبه اعتمادپذیری داده برای این ویژگی کارکرد مناسبی در حضور رفتارهای مخرب دارد.

سومین ویژگی مورد بررسی، سهولت پارک در جایگاه است. شکل ۱۱ نشان‌دهنده اعتماد پذیری داده ویژگی سهولت پارک برای جایگاه‌های با اندازه استاندارد در حضور رفتارهای مخرب است. با توجه به شکل ۱۱، مقدار همگرایی اعتمادپذیری داده محاسبه شده برای ویژگی سهولت پارک برای جایگاه‌های با اندازه استاندارد با افزایش درصد حضور رفتارهای مخرب در سیستم، کاهش پیدا می‌کند. در

بیش‌ترین حالت رفتارهای مخرب مقدار همگرایی نزدیک به ۰/۸ ا ست؛ با توجه به اینکه آســـتانه در نظر گرفته شـــده برای اعتماد برابر با ۰/۶ اســـت می‌توان گفت که محاســـبه اعتمادپذیری داده برای این ویژگی کارکرد مناسبی در حضور رفتارهای مخرب دارد.



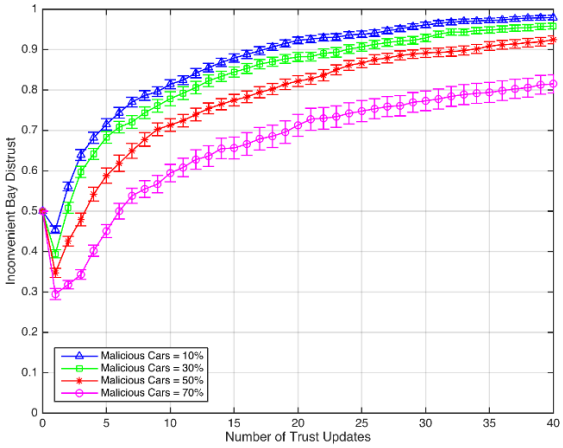
شکل ۱۱: اعتمادپذیری داده ویژگی سهولت پارک برای جایگاه‌های با اندازه استاندارد در حضور رفتارهای مخرب

شکل ۱۲ نشان‌دهنده اعتمادپذیری داده ویژگی سهولت پارک برای جایگاه‌های با اندازه غیراســتاندارد در حضــور رفتارهای مخرب اســت. با توجه به شــکل ۱۲، مقدار همگرایی بی‌اعتمادی محاســبه شــده برای ویژگی سهولت پارک جایگاه‌های با اندازه غیراستاندارد با افزایش درصد حضور رفتارهای مخرب در سیستم، کاهش پیدا می‌کند. در بیش‌ترین حالت رفتارهای مخرب مقدار همگرایی نزدیک به ۰/۸ ا ست؛ با توجه به آ ستانه در نظر گرفته شده برای اعتماد (برابر با ۰/۶) می‌توان گفت که محا سبه اعتمادپذیری داده برای این ویژگی کارکرد منا سبی در حضور رفتارهای مخرب دارد.

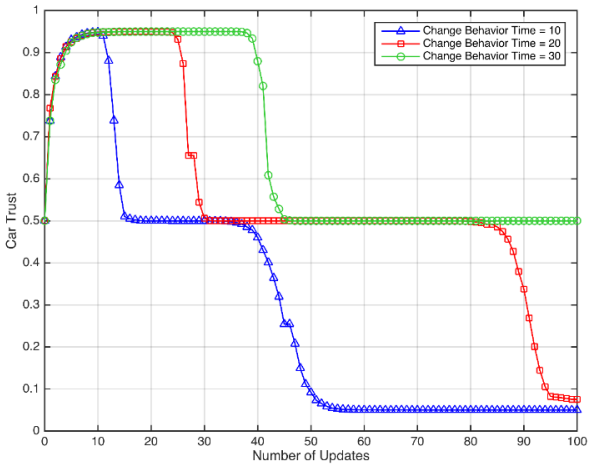
۵-۳- بررسی تطبیق‌پذیری اعتماد موجودیت با تغییر رفتار

یکی از پارامترهایی که میزان انعطاف‌پذیری یک روش محاســبه اعتماد را مشخص می‌کند، میزان تطبیق‌پذیری آن با تغییر شخصیت است؛ به این معنا که گره موردنظر رفتار خود را از مخرب به خوش‌رفتار و یا برعکس تغییر دهد. ســرعت این تطبیق و دقت مدل محاســبه اعتماد نسبت مستقیم دارند. به این منظور، در این بخش یک گره خوش‌رفتار در نظر گرفته شده است که یک‌بار بعد از گذشت ۱۰ مرتبه به‌روزرسانی، یک‌بار پس از گذشت ۲۰ مرتبه به‌روزرسانی و یک‌بار پس از گذشت ۳۰ مرتبه به‌روزرسانی به یک گره مخرب تغییر شخصیت داده است. شکل ۱۳ نشـــان‌دهنده میزان تطبیق پذیری اعتماد موجودیت با تغییر شخصیت است.

با توجه به شـــکل۱۳، در حالتی که تغییر رفتار پس از ۱۰ مرتبه به‌روزرسانی صورت می‌گیرد، به‌سرعت در به‌روزرسانی بعدی این تغییر رفتار تشخیص داده شده و مقدار اعتماد با کاهش به یک سطح پایین‌تر یعنی سطح متوسط(۰/۵) می‌رسد. این آزمایش برای حالاتی که تغییر رفتار پس از ۲۰ مرتبه و پس از ۳۰ مرتبه به‌روزرســانی صــورت بگیرند نیز تکرار شده است. با توجه به شکل ۱۳، با افزایش زمان تغییر رفتار، مدت زمان بیش‌تری طول می‌کشـــد تا مقدار اعتماد با این تغییر شـــخصـــیت تطبیق پیدا کند. دلیل این اختلاف در زمان تطبیق، نحوه کارکرد روش محاسبه اعتماد موجودیت است. در روش محاسبه اعتماد، با هر بار به‌روزرسانی، احتمال یک سطح به یک نزدیک‌تر می شود؛ این بدان معناســت که احتمال دو ســطح دیگر در هر به‌روزرســانی به صــفر نزدیک‌تر می شوند. بنابراین در مورد ۲۰ بار به‌روزرسانی، زمان بیشتری لازم اســت تا به احتمال مربوط به یک ســطح اعتماد جدید برســیم. با نتایج به‌دست‌آمده می‌توان گفت، روش محاسبه اعتماد موجودیت ارائه شده در Trusty با تغییر شخصیت گره‌ها تطبیق‌پذیر است.



شکل ۱۲: اعتمادپذیری داده ویژگی سهولت پارک برای جایگاه‌های با اندازه غیراستاندارد در حضور رفتارهای مخرب



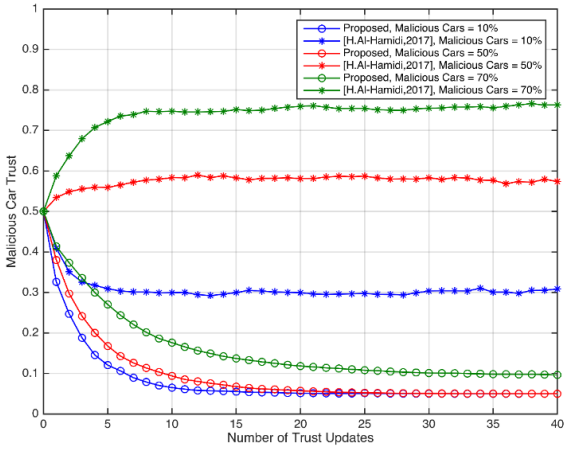
شکل ۱۳: میزان تطبیق پذیری اعتماد موجودیت با تغییر شخصیت

۵-۴- مقایسه Trusty با سایر روش‌ها

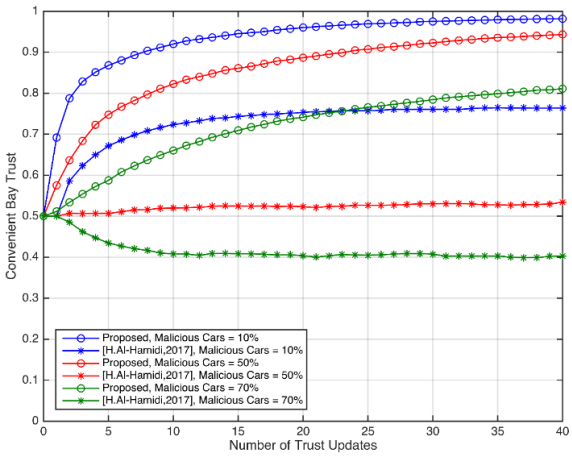
در این آزمایش، ســناریوی پارکینگ هوشــمند با اســتفاده از روش ارائه شده در مرجع [۹] نیز پیاده‌سازی شده و نتایج حاصل از شبیه‌سازی با نتایج محاسبه اعتماد در روش Trusty مقایسه شده است. در شکل ۱۴ اعتماد گره‌های مخرب در حضــور رفتارهای مخرب توســط هر دو روش محاسبه شده و مورد مقایسه قرار گرفته است.

با توجه به شــکل ۱۴، Trusty حتی در حالتی که ۷۰٪ گره مخرب در سیستم وجود دارد، عملکرد مناسبی خواهد داشت. با افزایش درصد گره‌های مخرب در سیستم، در حالتی که این مقدار به ۵۰٪ می‌رسد؛

مقدار همگرایی اعتماد در روش مرجع [۹] نزدیک به ۰/۶ خواهد بود و در حالتی که در صد گره‌های مخرب سیستم به ۷۰٪ می‌رسد؛ مقدار همگرایی بالاتر از آستانه اعتماد به نزدیک ۰/۸ می‌رسد که نشان‌دهنده کارکرد غیر مناسب این روش در حضور رفتارهای مخرب است.



شکل ۱۴: مقایسه اعتماد موجودیت Trusty و روش مرجع [۹]



شکل ۱۵: مقایسه اعتمادپذیری داده Trusty و روش مرجع [۲۰] در حضور رفتارهای مخرب

در شکل ۱۵ اعتماد پذیری داده ویژگی سهولت پارک برای جایگاه‌های با اندازه استاندارد، در حضور رفتارهای مخرب توسط هر دو روش مورد مقایسه قرار گرفته است. با توجه به شکل ۱۵، Trusty حتی در حضور ۷۰٪ گره مخرب در سیستم عملکرد مناسبی خواهد داشت. با افزایش درصد گره‌های مخرب در سیستم به ۵۰٪ مقدار همگرایی در روش [۹] از آستانه اعتماد نیز پایین‌تر آمده و نزدیک به ۰/۵ خواهد بود و در حالت ۷۰٪ درصد گره مخرب به ۰/۴ می‌رسد که نشان‌دهنده کارکرد غیر مناسب این روش در مقایسه با Trusty در حضور رفتارهای مخرب است.

۶- نتیجه‌گیری

در این مقاله به ارائه یک روش محاسبه اعتماد برای کاربرد در اینترنت اشیا پرداخته شده است که علاوه بر محاسبه اعتماد برای موجودیت‌ها در یک کاربرد، اعتمادپذیری داده‌های تولید شده را نیز محاسبه می‌کند. روش پیشنهادی برای محاسبه اعتماد، یک رویکرد ترکیبی است که از قانون ترکیب نظریه دمپستر-شفر برای ترکیب اعتماد موجودیت و اعتمادپذیری داده استفاده می‌کند. برای محاسبه اعتماد موجودیت از یک روش مبتنی بر یادگیری بیزی و برای محاسبه اعتمادپذیری داده از جمع وزن‌دار گزارش‌ها استفاده شده است. عملکرد مناسب روش پیشنهادی در قیاس با روش‌های موجود در سناریوی کاربردی پارکینگ هوشمند نشان دهنده اثربخشی رویکرد ارائه شده است.

۷- مراجع

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2356, 2015 .

[2] J.-H. Cho, K. Chan and S. Adali, "A survey on trust modeling," ACM Computing Surveys, vol. 48, no. 2, p. 28, 2015 .

[3] J. Guo and I.-R. Chen, "A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems," in IEEE International Conference on Services Computing, 2015 .

[4] A. Jøsang, R. Ismail and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007 .

[5] I.-R. Chen, J. Guo and F. Bao, "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.

[6] Y. Wang, Y.-C. Lu, I.-R. Chen, J.-H. Cho, A. Swami and C.-T. Lu, "LogitTrust: A logit regression-based trust model for mobile ad hoc networks," in 6th ASE International Conference on Privacy, Security, Risk and Trust, 2014 .

[7] S. A. Soleymani, A. H. Abdullah, W. H. Hassan, M. H. Anisi, S. Goudarzi, M. A. Rezazadeh Baee and S. Mandala, "Trust management in vehicular ad hoc network: a systematic review," EURASIP Journal on Wireless Communications and Networking , vol. 146, 2015.

[8] X. Yao, X. Zhang, H. Ning and P. Li, "Using trust model to ensure reliable data acquisition in VANETs," Ad Hoc Networks, vol. 55, pp. 107-118, 2017.

[9] 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.

[10] W. Li, H. Song and F. Zeng, "Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities," IEEE Internet of Things Journal , vol. PP, no. 99, p. 1, 2017 .

[11] U. Jayasinghe, A. Otebolaku and T.-W. Um, "Data centric trust evaluation and prediction framework for IOT," in ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K), 2017 .

[12] R. Böck, S. Glüge and A. Wendemuth, "Dempster-Shafer Theory with Smoothness," in International Symposium on

Integrated Uncertainty in Knowledge Modelling and Decision Making, 2013 .

[13] Y. Saied, A. Olivereau, D. Zeghlache and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," Computers & Security, vol. 39, pp. 351-365, 2013 .

[14] F. Bao and I.-R. Chen, "Dynamic Trust Management for Internet of Things Applications," in Proceedings of the international workshop on Self-aware internet of things, 2012 .

[15] Z. Chen, R. Ling, C. Huang and X. Zhu, "A scheme of access service recommendation for the Social Internet of Things," International Journal of Communication Systems., vol. 29, no. 4, pp. 694-706, 2016 .

[16] Bao, Fenye, I.-R. Chen and J. Guo, "Scalable, Adaptive and Survivable Trust Management for Community of Interest Based Internet of Things Systems," in IEEE Autonomous Decentralized Systems, 2013 .

[17] D. Chen, G. Chang, D. Sun, J. Li, J. Jia and W. Xingwei, "TRM-IoT: A Trust Management Model Based on Fuzzy Reputation for Internet of Things," omputer Science and Information Systems, vol. 8, no. 4, pp. 1207-1228, 2011.

[18] B. Liu, Z. Xu and J. Chen, "Toward reliable data analysis for Internet of Things by Bayesian dynamic modeling and computation," in IEEE International Conference on Signal and Information Processing, 2015 .

[19] Q. Ding, X. Li, M. Jiang and X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in Wireless Communications and Signal Processing, 2010 .

[20] S. Gurung, D. Lin, A. Squicciarini and E. Bertino, "Information-Oriented Trustworthiness Evaluation in Vehicular Ad-hoc Networks," in International Conference on Network and System Security, 2013 .

[21] M. Nitti, R. Girau and L. Atzori, "Trustworthiness Management in the Social Internet of Things," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 5, pp. 1253 - 1266, 2014.

[22] R. Talreja, S. Sathish and K. Nenwani, "Trust and behavior based system to prevent collision in IoT enabled VANET," in Signal Processing, Communication, Power and Embedded System, 2016 .

[23] G. Shafer, A mathematical theory of evidence, Princeton University Press, 1976 .

[24] C. Jiang, Y. Ren, H.-H. Chen and M. Guizani, "Information Sharing in Cooperative Networks: a Generic Trustworthy Issue," in IEEE International Conference on Communications, 2016 .

[25] Y. Zheng, S. Rajasegarar and C. Leckie, "Parking Availability Prediction for Sensor-Enabled Car Parks in Smart Cities," in IEEE International Conference on Intelligent Sensors, Sensor Networks and Information Processing, 2015.

[۲۶] جمیل جنتی، داریوش نظرپور، «مدیریت انرژی پارکینگ هوشمند خودروهای برقی در یک زیرشبکه با در نظر گرفتن اثرات برنامه پاسخگویی بار»، مجله مهندسی برق تبریز، جلد ۴۷، شماره ۲، صفحه ۴۵۵-۴۶۷، ۱۳۹۶

[۲۷] رحیم بجانی، محمد کلانتری، امیرمسعود افتخاری مقدم، «ارائه چهارچوبی مبتنی بر نظریه بازیها برای جلب مشارکت گره‌ها در فرآیند شناسایی گره‌های مخرب در شبکه‌های حسگر بی سیم»، مجله مهندسی برق تبریز، جلد ۴۷، شماره ۴، صفحه ۱۳۲۹-۱۳۴۲، ۱۳۹۶

[28] L. Gu, J. Wang, and B. Sun, “Trust management mechanism for Internet of things”, China Communications, vol. 11, no. 2, pp. 148-156, 2014

[29] H. Pohls, V. Angelakis, S. Suppan, K. Fischer, “RERUM: building a reliable IoT upon privacy and security enabled smart objects”, IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2014, pp. 122-127

[30] A. Rezvanian, A.M. Saghiri, S.M. Vahidipour, M.R. Meybodi, “Recent Advances in Learning Automata”, Springer, 2018