Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 10, Number 3, Autumn 2021, pp. 36-46
Received: 28/02/2020, Revised: 04/05/2021, Accepted: 02/07/2021

# A Robust Trust Model against Malicious Attacks in Heterogeneous Internet of Things

Majid Sangbarkan[1], Amir Jalaly Bidgoly[1,*]
[1] Department of Computer Engineering, University of Qom, Qom, Iran.
[*] jalaly@qom.ac.ir

Corresponding author's address: Amir Jalaly Bidgoly, Department of Computer Engineering, University of Qom, Qom, Iran, post code: 3716146611

**Abstract-** In recent years, the Internet of Things (IoT) has gained many interest and applications in various fields from automation of industrial processes to smart environments. Despite the advantages of IoT, the reliability of connected objects is a serious challenge in these environments. The heterogeneity of objects in IoT and the imbalance of power and resources do not allow the use of a reliable trust management model in these contexts. On the other hand, the use of more general and weaker models that can be implemented in all connected objects also reduces the security of these environments. In this paper, focusing on the heterogeneity of the IoT, a two-layer trust model is proposed. In the first layer, the model allows objects to select and use a trust model appropriate to their capabilities. Then in the second layer of the model, the result of the calculations of the previous layer is aggregated and the final trust values of the objects is calculated by considering the accuracy of each object. The proposed model uses the EigenTrust algorithm to aggregate the trust from the first layer. The paper also evaluates the robustness of the proposed model compared to the base models against various attacks including dishonest behavior, on-off attack, value imbalance attack and oscillation, and the results show that the proposed model is able to identify attackers with 86% accuracy and has also improved the accuracy of the base models up to 30%.

**Keywords-** Internet of Things, Trust Management, Heterogeneous, Trust Model.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۱۰، شماره ۳، پاییز ۱۴۰۰، صفحه ۳۶-۴۶
دریافت: ۱۳۹۸/۱۲/۰۹، بازنگری: ۱۴۰۰/۰۲/۱۴، پذیرش: ۱۴۰۰/۰۴/۱۱

# ارائه یک مدل محاسبه اعتماد در شبکه اینترنت اشیا ناهمگون جهت افزایش استحکام در برابر حملات

مجید سنگ‌برکان [۱]، امیر جلالی بیدگلی [*۱]
۱- دانشکده مهندسی کامپیوتر، دانشگاه قم، قم، ایران.
[*] jalaly@qom.ac.ir

* نشانی نویسنده مسئول: امیر جلالی بیدگلی، دانشکده مهندسی کامپیوتر، دانشگاه قم، قم، ایران،کد پستی: ۳۷۱۶۱۴۶۶۱۱

**چکیده- در سال‌های اخیر اینترنت اشیاء جذابیت‌ها و کاربردهای بسیاری در حوزه‌های مختلف از خودکارسازی فرایندهای صنعتی تا هوشمندسازی محیط‌ها پیدا کرده است. در کنار این کاربردها و مزایا، مسئله قابلیت اطمینان به اشیاء متصل، چالشی جدی در این محیط‌ها است. ناهمگونی اشیاء موجود در اینترنت اشیاء و عدم توازن قدرت و منابع آن‌ها اجازه استفاده از یک مدل مطمئن مدیریت اعتماد در این بسترها را نمی‌دهد. از سوی دیگر استفاده از مدل‌های عمومی‌تر و ضعیف‌تر که امکان اجرا در همه اشیاء متصل را داشته باشند، نیز موجب کاهش امنیت این محیط‌ها می‌شود. در این مقاله با تمرکز بر ناهمگونی شبکه اینترنت اشیاء، مدلی دولایه جهت محاسبه اعتماد ارائه شده است. این مدل در لایه نخست به اشیاء اجازه می‌دهد مدل اعتمادی متناسب با توانمندی‌های خود را انتخاب و استفاده کنند. سپس در لایه دوم مدل، برآیند محاسبات لایه قبل تجمیع و با در نظر گرفتن دقت هر کدام میزان قابلیت نهایی اشیاء محاسبه می‌شود. مدل پیشنهادی از الگوریتم EigenTrust جهت تجمیع اعتماد در مدل‌های مختلف لایه اول استفاده کرده است. این مقاله استحکام مدل پیشنهادی را در مقایسه با مدل‌های پایه در برابر حملات مختلف شامل رفتارهای غیر درستکار، حمله روشن/خاموش، حمله عدم تعادل ارزش و تمایز مورد ارزیابی قرار داده است و نتایج به دست آمده نشان می‌دهد مدل پیشنهادی قادر است با دقت ۸۶٪ مهاجمین را شناسایی کند و از این دیدگاه موجب بهبود دقت در شناسایی مهاجمین بین ۸٪ تا ۳۰٪ در مقایسه با مدل‌های پایه شده است.**

**واژه‌های کلیدی:** اینترنت اشیاء، مدیریت اعتماد، ناهمگون، مدل اعتماد.

## ۱- مقدمه

اینترنت اشیاء در حال به وجود آوردن دنیایی است که در آن اشیاء به طور یکپارچه در شبکه‌های اطلاعاتی مختلف به منظور ارائه خدمات پیشرفته و هوشمند برای انسان‌ها هماهنگ شدند. ارتباط اشیاء مانند حسگرها و کنترل‌کننده‌ها تمامی زوایای مختلف و داده‌های مربوط به زندگی اجتماعی انسان را جمع‌آوری می‌کند. این داده‌ها می‌توانند پردازش و بررسی شوند و سپس جهت هوشمندسازی محیط مورد استفاده قرار گیرند. با توجه به تعاملی که اینترنت اشیاء بین عناصر و اشیای متنوع ایجاد کرده و با در نظر گرفتن این موضوع که فناوری‌های اینترنت اشیاء مختص یک صنعت نیست، به ناچار در این شبکه‌ها معمولاً شاهد حضور اشیاء با توان‌های محاسباتی متنوع هستیم از حسگرهای کم‌توانی که تنها قادر به انجام محاسبات ضعیف هستند تا دستگاه‌های کاملی که توان یک رایانه کامل را در اختیار دارند. انواع کاربردهای مختلف اینترنت اشیاء (مانند شهر هوشمند، حمل و نقل هوشمند، پیش‌بینی وضعیت

محیط‌زیست، مدیریت بلایای طبیعی و غیره) با چنین ناهمگونی و وجود اشیاء با توان مختلف روبه‌رو هستند. به طور کلی یکی از ارکان اصلی در اینترنت اشیاء برقراری ارتباط بین اشیای موجود در این سیستم است که همگی دارای ویژگی‌های خاص و ناهمگون هستند؛ از قبیل میزان مصرف انرژی، میزان حافظه، قدرت محاسبات، طول عمر مصرف و غیره[۱].

اتصال میلیاردها شیء به اینترنت در بستر اینترنت اشیاء به معنای افزایش آسیب‌پذیری‌های امنیتی بالقوه در دنیای مجازی است. تأمین امنیت در شبکه‌های اینترنت اشیاء به یکی از چالش‌های انکارناپذیر این شبکه‌ها تبدیل شده است. اعتماد به عنوان یکی از مهم‌ترین روش‌های حذف اشیای خراب‌کار از شبکه و افزایش امنیت شبکه مطرح است و در این راستا به عنوان کمکی برای افزایش امنیت شبکه‌ها شناخته می‌شود[۲]. اعتماد، برگرفته از علوم انسانی و اجتماعی است که امروزه در دستگاه‌های کامپیوتری کاربردهای روزافزونی پیداکرده است. اعتماد در فرآیند تصمیم‌گیری، زمانی که یک همکاری میان موجودیت‌های مختلف در جریان است، دخالت دارد. مدل‌های اعتماد با استفاده از دانش و تجربه‌های مستقیم و غیرمستقیم (توصیه‌ها) در تعاملات قبلی تخمینی از شیوه رفتار یک موجودیت در آینده را در اختیار قرار می‌دهند که می‌تواند به عنوان ابزاری جهت شناسایی و حذف موجودیت‌های بدخواه از محیط مورد استفاده قرار گیرد. سادگی و سبکی این مدل‌ها آن‌ها را به ابزارهای ایده‌آل برای محیط‌های توزیع‌شده و دارای دستگاه‌هایی با توان محاسباتی ضعیف تبدیل کرده است که به عنوان دو نمونه مهم می‌توان از شبکه‌های حسگر بی‌سیم[۳]، اینترنت اشیاء[۴] نام برد. مدل‌های اعتماد و شهرت علی‌رغم مزایا و کاربردهای بسیاری که دارند، چالش‌های خاص خود را نیز به همراه دارند. مهم‌ترین این چالش‌ها استحکام این مدل‌ها در برابر حملات است[۵]. حملات بر علیه سیستم‌های اعتماد و شهرت، برخلاف حملات در سایر سازوکارهای امنیتی، به معنای نفوذ و شکستن یک پروتکل امنیتی نیست، بلکه به دنباله‌ای از رفتارهای فریب‌کارانه اطلاق می‌شود که موجب گمراهی سیستم و انحراف مقدار اعتماد محاسبه‌شده به نفع مهاجمین خواهد شد. یک سیستم آسیب‌پذیر در برابر حملات نه‌تنها نمی‌تواند کمکی به بهبود امنیت یک محیط داشته باشد، بلکه به ابزاری در دست مهاجمین تبدیل خواهد شد که از آن برای شدت بخشیدن به حملات خود استفاده کنند[۶]. پژوهش‌های مختلفی در مورد ارزیابی حملات در سیستم‌های اعتماد و شهرت انجام شده است [۷-۹]، هرچند هنوز این چالش نیازمند پژوهش‌های بیشتری است.

گذشته از چالش‌های عمومی مدل‌های اعتماد و شهرت، کاربرد این مدل‌ها در اینترنت اشیاء، چالش‌های اختصاصی خود را نیز در بر دارد. یکی از این چالش‌ها موضوع ناهمگونی اشیای متصل به شبکه اینترنت اشیاء است. مدل‌هایی که طی چند سال اخیر با موضوع اعتماد ارائه و معرفی شده است، اغلب با فرض همگون بودن محیط-های اینترنت اشیاء بوده است[۴, ۱۲-۱۰]. هرچند مدل‌های مختلفی تاکنون برای محاسبه اعتماد ارائه شده است، اما بسیاری از این مدل‌ها نیاز به توانمندی محاسباتی بیش از برخی اشیاء کم‌توان در بستر اینترنت اشیاء را دارند. از سوی دیگر استفاده از مدل‌های ضعیف‌تر در اشیاء منجر به افزایش آسیب‌پذیری و کاهش استحکام در برابر حملات خواهد شد. از این‌رو، ناهمگونی چالشی جدی برای استفاده از مدل‌های اعتماد در این بستر است که در مقالات کمتر به آن توجه شده است.

هدف این مقاله ارائه‌ی روشی در جهت مدل‌سازی محاسبه اعتماد در اینترنت اشیاء با توجه به ناهمگونی در اشیای فیزیکی و همچنین افزایش استحکام در برابر حملات اعتماد است. مدل پیشنهادی، یک معماری دولایه ارائه می‌دهد که امکان استفاده از مدل‌های مختلف اعتماد را بسته به توان محاسباتی یک شیء در شبکه فراهم می‌کند. در لایه دوم مدل تلاش می‌کند برآیند خروجی مدل‌های مختلف اعتماد را به نحوی محاسبه نماید که در آن میزان دقت پایین مدل‌های ضعیف‌تر در برآیند نهایی مؤثر باشد. به این منظور روش پیشنهادی از مدل EigenTrust [13] بهره برده است. این مدل قادر است با تکرار تأثیر بردارهای مختلف اعتماد در یکدیگر درنهایت تأثیر گره‌های کمتر قابل‌اعتماد را کاهش داده و به برآیندی از بردارهای اعتماد برسد که در آن میزان قابلیت اعتماد گره‌ها نیز به صورت بازگشتی تأثیر داده شده است. در این مقاله روش پیشنهادی مورد ارزیابی قرار گرفته است و نشان داده شده است که درعین‌حال که هر دسته از اشیاء می‌توانند مدلی فراخور توان محاسباتی خود را انتخاب کنند، استحکام کل شبکه در برابر حملات نیز افزایش یابد.

مقاله به صورت زیر ادامه پیدا می‌کند. در بخش بعدی ابتدا مروری بر روی پژوهش‌ها و مقالات مرتبط در مدل‌سازی محاسبه اعتماد خواهد شد. سپس مهم‌ترین حملات بر علیه سیستم‌های اعتماد و شهرت بررسی می‌شود. در بخش چهارم و پنجم، به ترتیب مدل پیشنهادی و نتایج ارزیابی آن در سناریوهای مختلف ارائه شده است. درنهایت مقاله در بخش ششم با جمع‌بندی و کارهای آتی پایان می‌پذیرد.

## ۲- کارهای مرتبط

طی سال‌های اخیر بحث اعتماد به یکی از مسائل مهم در اینترنت اشیاء تبدیل شده است؛ به طوری که در سال ۲۰۱۱، چان برای حل چالش امنیت در اینترنت اشیاء از روش اعتماد استفاده کرد. او مدلی برای مدیریت اعتماد بر اساس رویکرد اعتبار فازی جهت اعتمادسازی و ایجاد همکاری میان اشیاء ارائه داد[۱۴]. در ادامه چندین مقاله با موضوع اعتماد در اینترنت اشیاء مطرح شد، به طوری که در سال ۲۰۱۲ چانگ و همکاران مفهوم و کاربردهای مدیریت اعتماد را برای شبکه‌های بی‌سیم و اینترنت اشیاء مورد بحث قرار دادند[۱۵]. در سال ۲۰۱۳ بن سعید و همکارانش یک رویکرد فازی برای کنترل دسترسی مبتنی بر اعتماد در اینترنت اشیاء مطرح کردند[۱۶]. در سال ۲۰۱۴ کانگ مدلی برای اعتماد تعاملی در اینترنت اشیاء پیشنهاد کرد که بر اساس تعامل بین بازار نرم‌افزار و کاربران نهایی است و اعتبارسنجی نرم‌افزار به صورت کمی از طریق شباهت بین رفتار گره‌های اینترنت اشیاء انجام می‌شود[۱۷]. در سال ۲۰۱۵ چن و همکاران برای شبکه‌های اینترنت اشیای اجتماعی، مدلی را به نام مدیریت سرویس بر اساس اعتماد ارائه کردند[۱۲]. در سال ۲۰۱۵ محسن‌زاده و همکارانش یک مدل اعتماد براساس محاسبات فازی در محیط‌های ابری مطابق با تعاملات گذشته بین موجودیت‌های ابری با توجه به ویژگی‌های اعتماد ارائه کردند[۱۸]. در سال ۲۰۱۹ کاردی و همکارانش یک الگوریتم مدیریت اعتماد مبتنی بر منطق ذهنی برای محاسبه و ارزیابی اعتماد در محیط‌های ابری پیشنهاد کرده‌اند[۱۹]. در سال۲۰۱۴ فان و پروس مقاله‌ای از ارزیابی اعتماد در محیط‌های محاسبات ابری که از هر دو رویکرد ذهنی و عینی براساس ویژگی‌های SLA(s) و QoS استفاده شده است ارائه کردند[۲۰]. در سال ۲۰۱۱ سان و همکارانش یک مدل ارزیابی اعتماد چندبعدی به نام DMTC ایجاد کردند. در این مقاله از متغیر زمان برای ارزیابی اعتماد مستقیم و از متغیر مکان برای ارزیابی اعتماد غیرمستقیم استفاده شده است[۲۱]. در سال ۲۰۱۳ کنوآل و همکارانش عوامل و معیارهای مختلف مربوط به ارزیابی اعتماد را مورد بررسی قرار دادند. براساس این معیارها، آن‌ها برای اندازه‌گیری میزان اعتماد، یک مدل کمی ارائه دادند[۲۲]. در سال ۲۰۱۶ چیرگی و نویمی‌پور مدلی جهت ارزیابی اعتماد با توجه به پنج معیار دسترس‌پذیری، قابلیت اعتماد، یکپارچگی داده، احراز هویت و توانایی در محیط‌های ابری تخمین زدند[۲۳]. در سال ۲۰۱۴ گوو و همکارانش یک بررسی جامع از مدل‌های اعتماد درIOT ارائه دادند. در این مقاله، مدل‌ها از منظر جامع بودن فرآیند اعتماد بررسی شده است. آن‌ها فرآیندهای اعتماد را به چهار دسته طبقه‌بندی کرده‌اند: تشکیل اعتماد، گسترش اعتماد، ترکیب اعتماد و به روزکردن اعتماد. همچنین استحکام مدل‌های اعتماد در برابر حملات مشهور مورد بررسی قرار گرفته است[۲۴]. در سال ۲۰۱۷ فرناندز-گاگو و همکارانش چارچوبی را پیشنهاد کردند که به توسعه‌دهندگان IOT کمک می‌کند تا موضوع اعتماد در IOT را برای سناریوهای ویژه در نظر بگیرند. این مقاله همچنین یک سطح QoS را برای محاسبات اعتماد هر یک از ارائه‌دهندگان خدمات تعریف کرده است[۲۵]. در سال ۲۰۱۴ یان و همکارانش عوامل اصلی اعتماد در محیط IOT را مورد بررسی قرار دادند و یک مدل اعتماد براساس دیدگاه لایه‌ای که شامل لایه‌ی فیزیکی، لایه‌ی شبکه و لایه‌ی کاربرداست، پیشنهاد دادند[۱۱]. باو و چن در سال ۲۰۱۲ یک پروتکل مدیریت اعتماد پویا در IOT را برای مقابله با رفتار نامناسب گره‌هایی که ممکن است رفتار آن‌ها به صورت پویا تغییر کند ارائه دادند[۱۰]. لین و همکارانش در سال ۲۰۰۴ برای تقویت امنیت شبکه یک ساختار مدیریت اعتماد ایجاد کردند. آن‌ها یک مدل اعتماد جدید را پیشنهاد کردند که قادر به ضبط انواع مختلفی از روابط اعتماد در یک شبکه است و سازوکارهایی را برای ارزیابی اعتماد و به‌روز کردن تصمیمات اعتماد فراهم می‌کند[۲۶]. در سال ۲۰۰۹ لیاو و همکارانش یک مدل اعتماد مبتنی بر منطق فازی برای محیط‌های شبکه ارائه کردند. در این مقاله، یک مدل اعتماد وابسته به زمان ارائه شده است که می‌تواند مقدار اعتماد را به‌وسیله‌ی ارزیابی فازی متغیر وزن محاسبه کند. آن‌ها بعد از ترکیب مقادیر اعتماد، درجه‌ی اعتبار هر یک از گره‌های شبکه را نیز محاسبه کردند[۲۷]. در سال ۲۰۱۶ آشتیانی و

عبداللهی مدل ارزیابی اعتماد بر اساس تئوری تقسیم کوانتومی ارائه دادند که قادر است مقادیر اعتماد اختصاص‌یافته را به بخش‌های عینی و ذهنی تقسیم کند[۲۸].

## ۳- مروری بر حملات در مدل‌های اعتماد

مهاجمان می‌توانند به شیوه‌های متنوع برای اهداف مختلف وارد سیستم شوند. در این مقاله، عمدتاً بر حملات کلی تمرکز می‌شود که می‌تواند اعتماد محلی اشیاء را زیر سؤال ببرد. در ادامه چندین حمله بر اساس رفتارهای مهاجمان بررسی خواهد شد.

### ۳-۱- حمله ساده (رفتار غیر درست‌کارانه)

این مدل حمله، ساده‌ترین نوع حمله است، گره‌های این مدل به صورت غیرهوشمندانه و ثابت، رفتار بد را از خود نشان می‌دهند. بدین‌صورت که تمامی تراکنش‌هایی که بین این گره و سایر گره‌ها انجام می‌شود به صورت نادرست است. با توجه به اینکه مدل پیشنهادی در این مقاله، بر اساس تراکنش‌های درست و واقعی میزان اعتماد هر گره را ارزیابی می‌کند به راحتی نسبت به این حمله واکنش نشان می‌دهد و اعتماد نسبت به گره‌های این مدل حمله را با درصدی پایین نشان می‌دهد.

### ۳-۲- حمله روشن/ خاموش (OFF/ON)

در حمله روشن خاموش یا حمله خیانت [۲۹, ۳۰]، مهاجم به صورت متناوب، رفتار خوب و بد از خود نشان می‌دهد. با فرض اینکه تعداد تراکنش‌های انجام شده در محیط‌های اینترنت اشیاء را در بازه‌ی محدودی در نظر بگیریم، مهاجمین این مدل در این بازه به صورت تناوب رفتار خوب و درست (m بار) و رفتار بد و نادرست (n بار) را از خود نشان می‌دهند. با این تصور، زمانی که این مهاجم رفتار خوب و درستی دارد میزان اعتماد نسبت به خود را بالا برده و باعث می‌شود که دیگر گره‌ها به نادرست، رفتار خوب گره مهاجم را به عنوان رفتار واقعاً درست در نظر بگیرند و به این گره اعتماد کنند. پس از اینکه اعتماد گره‌ها جلب شد، گره مورد نظر به عنوان مهاجم رفتار نادرست و بدی از خود نشان می‌دهد و با این روش باعث آسیب رسیدن به محیط‌های اینترنت اشیاء می‌شود.

### ۳-۳- حمله دروغ‌گویی

حمله دروغ‌گویی [۳۰, ۳۱]، همان‌گونه که از اسم آن مشخص است در این مدل، گره‌ی مخرب در مشاهدات مستقیم سایر گره‌ها نسبت به خود، تراکنش‌های مستقیم رفتاری مناسب و درست‌کارانه از خود نشان می‌دهد و مانند سایر گره‌های محیط اینترنت اشیاء رفتار می‌کند، ولی زمانی که گره‌هایی جهت ارزیابی اعتماد گره‌های دیگر، نظر و توصیه از این گره را درخواست می‌کنند به دروغ توصیه‌های غلط و نادرستی را ارائه می‌دهد و باعث گمراه نمودن گره‌های دیگر می‌شود.

### ۳-۴- حمله عدم تعادل ارزش

در برخی از سیستم‌ها خدمات ارائه‌شده ارزش‌های متفاوتی دارند. یک سیستم اعتماد ممکن است این تفاوت ارزش را در امتیازها و محاسبه اعتماد لحاظ نکند. در این حالت حمله‌کننده می‌تواند با اجرای درست‌کارانه‌ی خدمات با ارزش پایین و اجرای غیردرست‌کارانه‌ی خدمات با ارزش بالا به سودی بیش از حد معمول دست یابد، بدون آنکه کاهش قابل‌توجهی در اعتماد داشته باشد. این رفتار به عنوان حمله عدم تعادل ارزش [33-31] شناخته می‌شود.

### ۳-۵- حمله تمایز

در حملات تمایز [۳۳]، حمله‌کننده رفتار متناقضی را با افراد مختلف در سیستم در پیش می‌گیرد. به عنوان نمونه وی ممکن است با گروه کوچکی از افراد رفتار غیردرست‌کارانه داشته باشد، در حالی که برای مابقی سیستم درست‌کار باشد. این حمله می‌تواند نتایج مختلفی داشته باشد. نخست آن‌که اگر تعداد افراد گروه اول (افرادی که حمله‌کننده با آن‌ها رفتار غیردرست‌کارانه داشته است) کم بوده و یا رای آن‌ها در سیستم وزن پایینی داشته باشد، حمله‌کننده می‌تواند بدون از دست دادن اعتماد به رفتار خود ادامه دهد. گذشته از آن، اگر سیستم از سازوکاری برای شناسایی توصیه‌های غیرصادقانه استفاده نماید، ممکن است توصیه‌های منتشرشده توسط این گروه را غیرصادقانه ارزیابی کرده و از محاسبه خارج کند. این امر خود به بالا بردن اعتماد به حمله‌کننده کمک می‌کند.

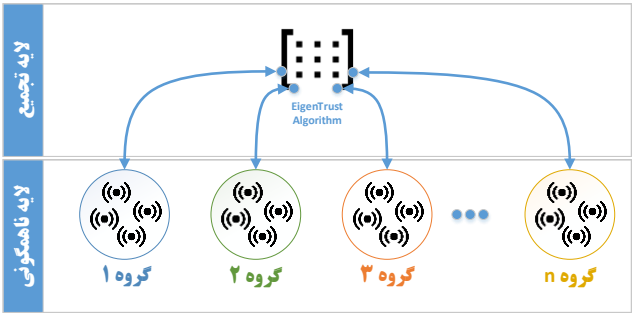
## ۴- روش پیشنهادی

رفتار یک شیء در اینترنت اشیاء یعنی میزان درستی یا نادرستی فعالیت آن در تراکنشی که با سایر گره‌های محیط اطراف خود دارد، می‌تواند برای محاسبه میزان اعتماد به آن شیء استفاده شود. با توجه به ناهمگون بودن اشیاء از نظر توانایی محاسباتی و میزان حافظه، همه اشیاء قادر نیستند به یک شیوه از محاسبه تاریخچه

رفتاری و توصیه‌های رفتاری و توصیه‌های دریافتی از سایرین، مقادیر اعتماد را تخمین بزنند. از این رو معماری پیشنهادی در این مقاله جدا کردن چالش ناهمگونی در اینترنت اشیاء از محاسبه نهایی مقادیر اعتماد است. شمای کلی این معماری در شکل (۱) نمایش داده شده است. در این معماری ابتدا به اشیا هر گروه اجازه داده می‌شود بر اساس توانمندی خود از یک مدل محلی اعتماد برای محاسبه اعتماد خود به سایرین استفاده کنند. این مدل محلی مطابق با توانمندی آن اشیاء باید باشد و می‌تواند یک مدل ضعیف یا مدل قوی با سازوکارهایی مانند تشخیص دروغ باشد. سپس در معماری پیشنهادی با اضافه کردن لایه‌ای به نام تجمیع به گره‌ها اجازه داده می‌شود، با کمک گرفتن از سایر گروه‌ها و با در نظر گرفتن میزان دقت مدل مورد استفاده توسط هر گروه، مقادیر نهایی را با تأثیر دادن خروجی همه مدل‌های محلی بسازد. این لایه بر اساس الگوریتم EigenTrust مقادیر نهایی اعتماد را تخمین و محاسبه می‌کند لازم به توضیح است نوآوری روش پیشنهادی در این مقاله استفاده از مدل لایه‌ای است که در شبکه‌های اینترنت اشیاء ناهمگون کار می‌کند. مدل‌های اعتماد ارائه شده قبلی یا یک مدل سبک‌وزن با رویکرد محاسبات پایین برای اشیاء ضعیف هستند مانند مدل بتا که ایراد این مدل‌ها استحکام پایین آن‌ها است و یا یک مدل سنگین با محاسبات پیچیده که بیشتر تمرکز آن را روی مستحکم کردن مدل است و برای اشیاء با امکانات گران استفاده می‌شود مانند مدل Subjective Logic. ایراد این مدل‌ها قابل پیاده‌سازی نبودن روی اشیاء ضعیف با امکانات ساده است. اما در روش پیشنهادی محاسبات اعتماد به دولایه تقسیم می‌شود که در لایه اول هر اشیاء براساس توان محاسباتی خود میزان اعتماد را محاسبه می‌کند برای لایه دوم ارسال می‌کند و در لایه دوم با استفاده از روش EigenTrust که این رویکرد یک روش تجمیع اطلاعات به صورت توزیع شده است اعتماد نهایی محاسبه و منتشر می‌شود.

### ۴-۱-لایه ناهمگونی

همان‌طور که گفته شد در لایه‌ی ناهمگونی، گره‌های اینترنت اشیاء به چند گروه تقسیم می‌شوند که هر گروه از روش‌های مختلفی




**شکل ۱: معماری کلی روش پیشنهادی**

جهت به دست آوردن درصد اعتماد استفاده می‌کند. در این لایه اشیاء می‌تواند از هر مدل اعتمادی به عنوان مدل محلی استفاده کنند و روش پیشنهادی در این لایه قید خاصی برای استفاده از مدل‌ها ندارد. هرچند در ادامه برای تبیین بهتر مسئله و مطالعات موردی ۴ مدل معروف اعتماد در سطوح مختلف استحکام انتخاب و برای این لایه ارائه شده است، اما مجدد تأکید می‌شود این مدل‌ها در نسخه‌های مختلف از پیاده‌سازی روش پیشنهادی می‌توانند با هر روش دیگری متناسب با شرایط محیط جایگزین شوند. در ادامه مدل‌های ارزیابی اعتماد هر گروه به صورت جداگانه شرح داده می‌شود.

#### ۴-۱-۱- مدل ارزیابی اعتماد ساده

در مدل ارزیابی اعتماد ساده ابتدا در زمان مشخصی رفتار گره‌ی مورد نظر بررسی می‌شود، به طوری که تعداد تراکنش و تبادل پیامی که بین گره‌ها انجام می‌شود در متغیرهای این مدل ذخیره می‌شود و تمامی تراکنش‌ها به دو دسته تقسیم می‌شود. بدین‌صورت که هر تراکنش درست و صحیح در متغیر R و هر تراکنش نادرست و اشتباه در متغیر S ذخیره می‌شود. این دو متغیر از جنس اعداد صحیح مثبت در نظر گرفته می‌شود که مقادیر آن تعداد تجربیات مثبت و منفی را به ترتیب نمایش می‌دهد. در مرحله دوم میزان ارزیابی اعتماد اولیه با استفاده از رابطه (۱) محاسبه می‌شود و در آرایه‌ی $N$ ذخیره می‌شود.

$$N(i) = \frac{R}{S+R} \qquad (۱)$$

که در این رابطه $N(i)$ میزان اعتماد به گره‌ی i‌ام است و R رفتار درست و S رفتار نادرست گره را مشخص می‌کند[۶].

#### ۴-۱-۲- مدل ارزیابی اعتماد بتا

این مدل هم مانند مدل قبلی از دو متغیر برای ذخیره کردن رفتار گره‌ها استفاده می‌کند؛ بدین‌صورت که رفتار درست در متغیر $\alpha$ و

رفتار نادرست در متغیر β ذخیره می‌شود، در مرحله‌ی بعدی میزان ارزیابی اعتماد اولیه با استفاده از رابطه (۲) محاسبه می‌شود و در آرایه $N$ ذخیره می‌شود.

$$N(i) = \frac{\alpha+1}{\beta+\alpha+1} \quad (۲)$$

که در این رابطه $N(i)$ میزان اعتماد مستقیم به گره iام است، α رفتار درست و β رفتار نادرست است[۳۳].

### ۴-۱-۳- مدل ارزیابی اعتماد Core

در این مدل تمام رفتارهای درست و نادرست اشیاء به همراه زمان وقوع آن ذخیره می‌شود. در این مدل رفتار درست گره برابر یک (۱) و رفتار نادرست برابر صفر (۰) در نظر گرفته می‌شود. روش ارزیابی اعتماد در این مدل به این صورت است؛ فرض کنید که در زمان $t_i$ گره $q_n$ رفتار درست دارد و در زمان $t_{i+1}$ گره $q_n$ رفتار نادرست دارد. درنهایت میزان اعتماد گره $q_j$ از رابطه (۳) به دست می‌آید.

$$N(i) = \frac{\sum_{i=1}^{new}(t_{new}-t_i)\times q_n}{\sum_{i=1}^{new} t_i} \quad (۳)$$

که در این رابطه $N(i)$ میزان اعتماد گره مورد نظر نسبت به گره iام است، $t_{new}$ زمان ارزیابی اعتماد، $t_i$ زمان انجام رفتار و $q_n$ گره‌ای است که مورد ارزیابی قرار می‌گیرد [۳۴].

### ۴-۱-۴- مدل ارزیابی اعتماد Subjective Logic

این مدل برای ارزیابی اعتماد از دو فاکتور ارزیابی اعتماد مستقیم و ارزیابی اعتماد به وسیله توصیه و پیشنهاد دیگران استفاده می‌کند. برای به دست آوردن اعتماد مستقیم ابتدا رفتارهای درست و نادرست هر گره را دریافت می‌کند و در متغیرهای (S،R) ذخیره می‌کند. در این مدل میزان اعتماد با سه فاکتور اعتقاد داشتن، اعتقاد نداشتن و شک نشان داده می‌شود؛ که هر سه فاکتور در ارزیابی اعتماد نهایی تأثیرگذار هستند و در سه متغیر (b: اعتقاد داشتن، d: اعتقاد نداشتن، u: شک) ذخیره می‌شود. برای به دست آوردن این سه فاکتور در مشاهده‌های مستقیم از رابطه‌های زیر استفاده می‌شود[۳۵].

$$b(i) = \frac{R}{S+R+2} \quad (۴)$$

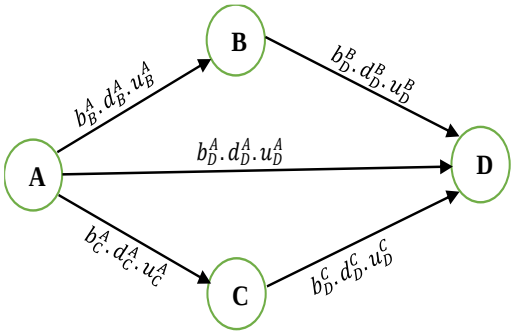
که در این رابطه $b(i)$ میزان اعتقاد به گره i، R رفتار درست و S رفتار نادرست را نشان می‌دهند.

$$d(i) = \frac{S}{S+R+2} \quad (۵)$$

که در این رابطه $d(i)$ میزان بی‌اعتقادی به گره i، R رفتار درست و S رفتار نادرست را نشان می‌دهد.

$$u(i) = \frac{2}{S+R+2} \quad (۶)$$

که در این رابطه $u(i)$ میزان شک به گره i، R رفتار درست و S رفتار نادرست را نشان می‌دهد. در مرحله بعدی، سه فاکتور اعتقاد داشتن، اعتقاد نداشتن و شک را برای مشاهده‌های غیرمستقیم محاسبه می‌کند. همان‌طور که در شکل (۱) نشان داده شده است، فرض کنید که گره‌ی A برای محاسبه اعتماد غیرمستقیم از دو گره B,C استفاده می‌کند.




**شکل ۲: رفتار انجام‌شده بین گره‌ها**

گره A جهت ارزیابی اعتقاد داشتن غیرمستقیم نسبت به گره D از گره B به صورت زیر استفاده می‌کند.

$$b_D^{A-B} = b_B^A \times b_D^B \quad (۷)$$

که در این رابطه $b_D^{A-B}$ درصد اعتقاد گره A نسبت به گره D از طریق گره B است، $b_B^A$ درصد اعتقاد گره A نسبت به گره B و $b_D^B$ درصد اعتقاد گره B نسبت به گره D است. همچنین گره A جهت ارزیابی بی‌اعتقادی غیرمستقیم نسبت به گره D از طریق گره B به صورت زیر استفاده می‌کند.

$$d_D^{A-B} = b_B^A \times d_D^B \quad (۸)$$

که در این رابطه $d_D^{A-B}$ درصد بی‌اعتقادی گره A نسبت به گره D از طریق گره B است، $b_B^A$ درصد اعتقاد گره A نسبت به گره B و $d_D^B$ درصد بی‌اعتقادی گره B نسبت به گره D است و درنهایت گره A جهت ارزیابی شک غیرمستقیم نسبت به گره D از طریق گره B به صورت زیر استفاده می‌کند.

$$u_D^{A-B} = 1 - (b_D^{A-B} + d_D^{A-B}) \quad (۹)$$

که در این رابطه $u_D^{A-B}$ درصد شک گره A نسبت به گره D از طریق گره B است، $b_D^{A-B}$ درصد اعتقاد گره A نسبت به گره D از طریق

گره B است، $d_D^{A-B}$ درصد بی‌اعتقادی گره A نسبت به گره D از طریق گره B است. گره A جهت ارزیابی اعتقاد داشتن، اعتقاد نداشتن و شک غیرمستقیم نسبت به گره D با استفاده از گره C به صورت زیر استفاده می‌کند.

$$\begin{aligned} b_D^{A-C} &= b_C^A \times b_D^{BC} \\ d_D^{A-C} &= b_C^A \times d_D^C \\ u_D^{A-C} &= 1 - (b_D^{A-C} + d_D^{A-C}) \end{aligned} \qquad (۱۰)$$

که در این رابطه $b_D^{A-C}$ درصد اعتقاد گره A نسبت به گره D از طریق گره C است، $d_D^{A-C}$ درصد بی‌اعتقاد گره A نسبت به گره D از طریق گره C است و $u_D^{A-C}$ درصد شک گره A نسبت به گره D از طریق گره C است. پس از اینکه مقادیر سه فاکتور(اعتقاد داشتن، بی‌اعتقادی و شک) از تمامی گره‌ها محاسبه شد، برای به دست آوردن فاکتور نهایی از روابط زیر استفاده می‌شود.

$$\begin{aligned} l &= u_A + u_B - u_A \times u_B \\ b^* &= \frac{b_A \times u_B - b_B \times u_A}{l} \\ d^* &= \frac{d_A \times u_B - d_B \times u_A}{l} \\ u^* &= \frac{u_A \times u_B}{l} \end{aligned} \qquad (۱۱)$$

در نهایت جهت ارزیابی اعتماد اولیه در این مدل از رابطه (۱۲) استفاده می‌شود:

$$N(i) = b_n + \frac{u_n}{2} \qquad (۱۲)$$

### ۴-۲-لایه تجمیع

در لایه تجمیع جهت ارزیابی اعتماد نهایی بین گروه‌ها از الگوریتم *EigenTrust* استفاده می‌شود. روش کار این الگوریتم به این صورت است که فرض کنید ماتریس اعتماد گروه‌ها را داریم که در آن میزان اعتماد هر گروه به گروه‌های دیگر در بازه (۰,۱) تعریف شده است. همچنین قطر این ماتریس برابر یک است یعنی درصد اعتماد هر گروه نسبت به خود مقدار یک (۱) است. بنابراین عناصر این ماتریس از تجمیع خروجی مدل‌های لایه قبل ایجاد می‌شود. ماتریس زیر را در نظر می‌گیریم که مقدار $\alpha_{i.j}$ در آن میزان اعتماد گروه $i$ به $j$ و عددی بین صفر و یک است.

$$\begin{bmatrix} \alpha_{1.1} & \alpha_{1.2} & \dots & \alpha_{1.n} \\ \alpha_{2.1} & \alpha_{2.2} & \dots & \alpha_{2.n} \\ & & \dots & \\ & & \dots & \\ & & \dots & \\ \alpha_{m.1} & \alpha_{m.2} & \dots & \alpha_{m.n} \end{bmatrix} \qquad (۱۳)$$

$$0 \le \alpha_{m.n} \le 1$$

قبل از اینکه الگوریتم EigenTrust درصد نهایی اعتماد را محاسبه کند، باید ماتریس اعتماد پیش‌پردازش شود به صورتی که جمع اعداد هر سطر از این ماتریس برابر یک شود. برای این کار با استفاده از رابطه (۱۴) مقدار هر سلول از ماتریس بر مجموع مقادیر هر سطر تقسیم می‌شود و در نهایت ماتریس زیر به دست می‌آید که مقادیر هر سطر برابر یک است.

$$C = \begin{bmatrix} \beta_{1.1} & \beta_{1.2} & \dots & \beta_{1.n} \\ \beta_{2.1} & \beta_{2.2} & \dots & \beta_{2.n} \\ & & \dots & \\ & & \dots & \\ & & \dots & \\ \beta_{m.1} & \beta_{m.2} & \dots & \beta_{m.n} \end{bmatrix} \qquad (۱۴)$$

$$\beta_{i.j} = \frac{\alpha_{i.j}}{\sum_n \alpha_{i.n}}$$

الگوریتم EigenTrust شهرت هر گروه را به دست می‌آورد. ابتدا یک بردار شهرت اولیه $t^0$ در نظر گرفته می‌شود که تمامی مقادیر آن با هم برابر است و همچنین جمع مقادیر آن باید برابر یک باشد. این مقدار اولیه به سادگی می‌تواند $1/n$ باشد که در آن $n$ تعداد موجودیت‌ها است. مفهوم مقادیر اولیه این بردار آن است که میزان شهرت اولیه همه موجودیت‌ها در ابتدا یکسان فرض شده است. همچنین می‌توان بنابر دلایلی در ابتدا برای گروه‌هایی خاصی (به عنوان نمونه گروه اشیاء دارای نظارت یا اعتبار رسمی) اعتبار اولیه بیشتری در نظر گرفته شود، باید مقدار اولیه آن‌ها در $t^0$ بیشتر از سایرین در نظر گرفته شود. در ادامه الگوریتم ماتریس پیش‌پردازش شده اعتماد گروه یا $C$، در این بردار اولیه ضرب می‌شود و مقدار به‌دست‌آمده از حاصل‌ضرب ماتریس اعتماد و بردار اولیه به عنوان $t^1$ بردار شهرت جدید در نظر گرفته می‌شود. این فرایند آن‌قدر تکرار می‌شود تا اختلاف $t^k$ و $t^{k+1}$ همگرا شود و مقدار آن تقریباً ثابت شود. در نهایت این مقدار به عنوان مقادیر اعتماد هر گروه در نظر گرفته می‌شود و برای تمامی گره‌ها ارسال می‌شود. لازم است توجه شود که مقدار اولیه بردار $t^0$ در پاسخ نهایی، تأثیرگذار است.

***TrustAggregation*** *Algorithm*
*Begin*
*Get* $\alpha_{i,j}$ *the local trust of group i to group j*
$\beta_{i,j} \leftarrow \frac{\alpha_{i,j}}{\sum_{j'} \alpha_{i,j'}}$
$C \leftarrow$ *Matrix of* $\beta_{i,j}$ *(Eq. 14).*
$t^0 \leftarrow$*Any uniform vector on groups*
*Repeat*
$t^{k+1} \leftarrow C^T \times t^k$
$\delta \leftarrow \left|t^{k+1} - t^k\right|$
*Until* $\delta < \epsilon$
*Return* $t^k$
*End*

**شکل ۳: الگوریتم *EigenTrust* جهت تجمیع مقادیر اعتماد**

## ۵- ارزیابی روش پیشنهادی

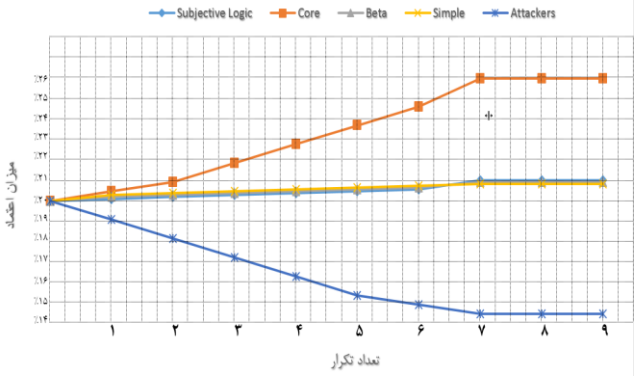
به منظور سنجش و ارزیابی مدل پیشنهادی، مدل با استفاده از شبیه‌ساز COOJA که در سیستم‌عامل Contiki قابلیت اجرا دارد، طراحی و پیاده‌سازی شده است. برای پیاده‌سازی مدل پیشنهادی به یک شبکه اینترنت اشیاء ناهمگون به همراه گره‌های مختلف نیاز است. ویژگی‌های گره‌ها در جدول (۱) مشخص شده است.

**جدول (۱): ویژگی‌های گروه‌ها - بخش اول**

| نوع گروه | ارزیابی اعتماد | نوع رفتار | توان محاسباتی | تعداد |
|---|---|---|---|---|
| **گروه اول** | ساده | ۰٪ خطا | پایین | ۳ عدد |
| **گروه دوم** | بتا | ۰٪ خطا | پایین | ۳ عدد |
| **گروه سوم** | Core | ۰٪ خطا | پایین | ۳ عدد |
| **گروه چهارم** | Subjective Logic | ۰٪ خطا | بالا | ۳ عدد |
| **گروه پنجم** | مهاجم | ۱۰۰٪ خطا | بالا | ۳ عدد |

در این پژوهش جهت آزمایش و سنجش الگوریتم پیشنهادی یکی از گروه‌ها (گروه پنجم) به عنوان گروه مخرب و مهاجم فرض شده است تا از جهات مختلف درستی/ نادرستی اجرای الگوریتم و میزان مقاوم بودن مدل پیشنهادی در برابر حملات سنجیده شود. نتایج ارزیابی اعتماد با وجود حمله غیردرستکار در شکل (۴) مشخص شده است.

همان‌طور که در شکل (۴) نمایش داده شده است، پس از اجرای الگوریتم پیشنهادی و همگرا شدن نتایج، درصد اعتماد به گروه اول ۲۱، گروه دوم ۲۱، گروه سوم ۲۶، گروه چهارم ۲۱ و گروه پنجم ۱۴درصد به دست آمده است. بر این اساس گره پنجم که گروه مهاجم است پایین‌ترین درصد و غیرقابل‌اعتماد ارزیابی شده است




**شکل (۴): ارزیابی اعتماد گره‌ها در حمله غیر درستکار**

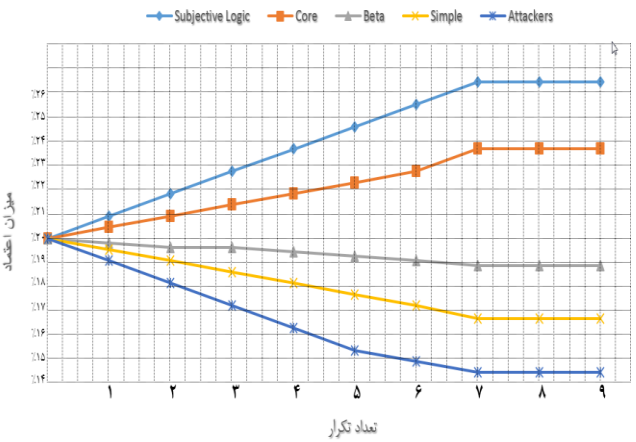
و با توجه به نتایج به دست آمده عملکرد الگوریتم در مقابل حمله غیر درستکار مقاوم بوده است. همان‌طور در ادامه این بخش ارائه خواهد شد، بدون این لایه مدل‌های ضعیف اعتمادی نزدیک به ۴۰٪ برای مهاجمین تخمین می‌زدند، این در حالی است که در مدل پیشنهادی با تجمیع دانش همه اشیاء و در نظر گرفتن دقت هر مدل، به خوبی این ضعف پوشش داده شده و حتی مدل‌های ضعیف نیز امکان تشخیص مهاجمین را دارند. همچنین در این نتایج گروه Core به عنوان قابل‌اعتمادترین مدل (به علت قدرت مدل در شناسایی) شناخته شده است.

در دومین حمله، حمله عدم تعادل ارزش ارزیابی شده است. ویژگی‌های گره‌ها در این حمله در جدول (۲) مشخص شده است.

**جدول (۲): ویژگی‌های گروه‌ها - بخش دوم**

| نوع گروه | ارزیابی اعتماد | نوع رفتار | توان محاسباتی | تعداد |
|---|---|---|---|---|
| **گروه اول** | ساده | ۵۰٪ خطا | پایین | ۳ عدد |
| **گروه دوم** | بتا | ۴۰٪ خطا | پایین | ۳ عدد |
| **گروه سوم** | Core | ۲۰٪ خطا | پایین | ۳ عدد |
| **گروه چهارم** | Subjective Logic | ۰٪ خطا | بالا | ۳ عدد |
| **گروه پنجم** | مهاجم | ۶۰٪ خطا | بالا | ۳ عدد |

نتایج ارزیابی مدل پیشنهادی در حمله عدم تعادل ارزش شکل (۵) نمایش داده شده ا ست. همان‌طور که در این شکل م شاهده می شود، پس از اجرای الگوریتم پی شنهادی و همگرا شدن نتایج، مطمئن‌ترین گروه در محیط اینترنت ا شیاء گروه چهارم با ۲۶٪ پیش‌بینی شده ا ست که بالاترین در صد اعتماد را دارد. گره پنجم که گروه مهاجم را ت شکیل می‌دهد با ۱۴٪، پایین‌ترین در صد و غیرقابل‌اعتماد ارزیابی شده است.



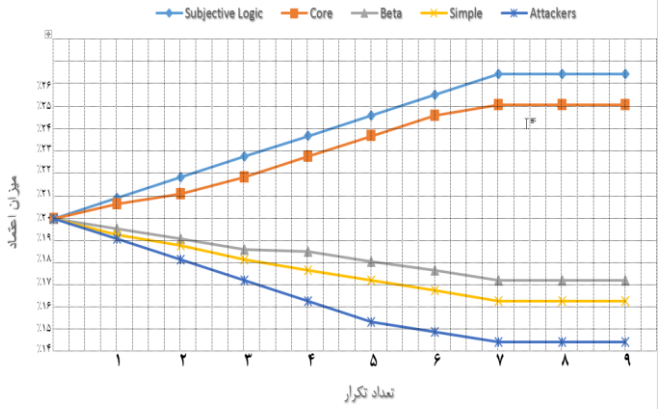

**شکل (۵): ارزیابی اعتماد گره‌ها در حمله عدم تعادل ارزش**

نتایج به دست آمده نشان می‌دهد که حتی گره‌های ضعیف هم قادر به شناسایی مهاجمین هستند. نکته جالب در این نتایج آن است که میزان اعتماد به گره‌های دارای مدل‌های محاسبه اعتماد ضعیف نیز افت کرده است. علت آن است که این گره‌ها ابزار مناسب برای تشخیص حملات تمایز را در اختیار ندارند، از این رو مقادیر محاسبه شده اعتماد آن‌ها چندان قابل‌اطمینان نیست. مدل پیشنهادی با کاهش میزان اعتماد به این گره‌ها نقش آن‌ها را در این مقابله با این حمله کم‌رنگ‌تر کرده است. مدل Subjective Logic که گره‌های آن بدون نقض فرض شده‌اند بالاترین میزان اعتماد را کسب کرده‌اند. در ادامه از حمله تمایز نیز برای ارزیابی مدل پیشنهادی استفاده شده است. این حمله در برابر گروهی از گره‌ها رفتار درست دارد و در برابر گروه دیگر رفتار نادرست از خود نشان می‌دهد. مشخصات رفتاری گره‌های مهاجم در برابر گروه‌های مختلف در جدول (۳) نمایش داده شده است.

**جدول (۳): ویژگی‌های گروه‌ها**

| نوع گروه | گروه اول | گروه دوم | گروه سوم | گروه چهارم |
|---|---|---|---|---|
| گره مهاجم | ۸۰٪ | ۷۵٪ | ۲۵٪ | ۱۵٪ |

نتایج ارزیابی مدل پیشنهادی در برابر حمله تمایز در شکل (۶) نمایش داده شده است. همان‌طور که در این شکل مشاهده می‌شود، پس از اجرای الگوریتم پیشنهادی و همگرا شدن نتایج، مطمئن‌ترین گروه در محیط اینترنت اشیاء گروه چهارم با درصد ۲۶ پیش‌بینی شده است که بالاترین درصد اعتماد را دارد. گره پنجم که گروه مهاجم را تشکیل می‌دهد با درصد ۱۴، پایین‌ترین درصد و غیرقابل‌اعتماد ارزیابی شده است به خوبی نشان‌دهنده شناسایی آن توسط همه گروه‌ها است. این نتایج با توجه به اینکه مهاجمین رفتارهای متمایزی با گروه‌های مختلف داشته‌اند، قابل‌توجه است. علی‌رغم این اختلاف در رفتار، با توجه به لایه تجمیع در روش پیشنهادی، تجربیات بدرفتاری مهاجمین تجمیع شده و همه گره‌ها اعتماد خود را به آن‌ها از دست داده‌اند.




**شکل (۶): ارزیابی اعتماد گره‌ها در حمله تمایز**

جهت مقایسه و استنتاج بهبود حاصل از مدل پیشنهادی این مقاله، روش پیشنهادی با مدل‌های نیز مقایسه و بررسی شده‌اند. در این ارزیابی فرض شده است اشیاء هر یک با توجه به توانایی خودشان مدل محاسبه اعتماد متناسب را انتخاب و بر اساس آن رفتار می‌کند. در این حالت هیچ لایه دومی جهت تجمیع دانش همه مدل‌ها نیست، هرچند هر مدل از مکانیزم‌های انتشار اطلاعات خود بهره می‌برد.

**جدول(۴):مقایسه الگوریتم پیشنهادی با سایر روش‌های ارزیابی اعتماد**

| روش ارزیابی اعتماد | مدل ساده | مدل بتا | مدل Core | مدل Subjective Logic | مدل پیشنهادی |
|---|---|---|---|---|---|
| حمله غیردرستکار | ٪۴۰ | ٪۳۵ | ٪۲۸ | ٪۲۰ | ٪۱۳ |
| حمله عدم تعادل ارزش | ٪۴۵ | ٪۳۰ | ٪۳۰ | ٪۲۷ | ٪۱۴ |
| حمله تمایز | ٪۴۵ | ٪۳۰ | ٪۲۶ | ٪۲۵ | ٪۱۴ |

نتایج ارزیابی این مدل‌ها در حملات مختلف و در مقایسه با مدل پیشنهادی در جدول (۴) نمایش داده شده است. در این جدول محتوی هر خانه میزان اعتماد محاسبه‌شده برای مهاجمین است که هر چه به صفر نزدیک‌تر باشد، نشان‌دهنده این است که مدل بهتر مهاجمین را شناسایی کرده است. همان‌طور که در این جدول

نمایش داده شده است، مدل پیشنهادی دقت همه روش‌ها را با میزان قابل‌توجهی بهبود داده است. این مدل به گره‌های ضعیف که از روش‌های ساده‌ای مانند مدل ساده یا بتا استفاده می‌کنند، کمک می‌کند مهاجمین را بهتر شناسایی کرده و میزان اعتمادی در حدود کمتر از $1/3$به آن‌ها منتسب کند. مدل پیشنهادی حتی به روش‌های قدرتمند مانند Subjective logic نیز کمک کرده و دقت آن‌ها را تا ۸٪ بهبود داده است. نتایج این مقایسه نشان می‌دهد لایه دوم پیشنهادی در این مقاله نه تنها امکان استفاده از مدل‌های مختلف اعتماد را در شبکه ناهمگون اینترنت اشیاء می‌دهد، بلکه موجب افزایش دقت حتی در مدل‌های مستحکم و قدرتمند محاسبه اعتماد نیز خواهد شد.

## ۶- نتیجه‌گیری

در این مقاله روشی جهت مدل‌سازی محاسبه اعتماد در شبکه اینترنت اشیاء با تمرکز بر ناهمگونی این شبکه ارائه شده است. در مدل پیشنهادی محاسبه اعتماد به دولایه شکسته شده است. در لایه نخست به اشیاء اجازه داده می‌شود، مدل اعتمادی را بر اساس توانمندی محاسباتی و منابع خود انتخاب کنند. سپس در لایه دوم، با استفاده از رویکرد تجمیع EigenTrust، نتایج مدل‌های اختصاصی لایه قبل تجمیع شده و برآیند میزان اعتماد به گره به دست می‌آید. لایه دوم اجازه می‌دهد نقاط ضعف مدل‌های محاسبه اشیاء پوشش داده شود و به برآیندی از دانش همه اشیاء دست یابند. نتایج ارزیابی‌های انجام‌شده نشان می‌دهد مدل پیشنهادی، می‌تواند استحکام همه اشیاء حتی اشیاء قوی را نیز در برابر حملات تا حداکثر ۳۰٪ افزایش دهد.

مدل پیشنهادشده در این مقاله، تنها به رویکرد تجمیع اعتماد به رفتار اشیاء توجه داشته است. میزان اعتماد به توصیه اشیاء فاکتور دیگری است که به عنوان کارهای آتی جهت تکمیل این مدل برنامه‌ریزی شده است. همچنین تأثیر عواملی مانند فاصله بین اشیاء، مدت حیات اشیاء و تعداد تعاملات وی در محیط از دیگر برنامه‌های تکمیلی در آینده این پژوهش است.

## مراجع


[1] Lee H-C, Lee S-W: Trust as Soft Security for Self-Adaptive Systems: A Literature Survey. In: 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC): 2017: IEEE; 2017: 523-528.

[2] Barber KS, Kim J: Soft security: Isolating unreliable agents from society. In: Workshop on Deception, Fraud and Trust in Agent Societies: 2002: Springer; 2002: 224-233.

[3] JIANG J, Guangjie H: Survey of Trust Management Mechanism in Wireless Sensor Network. Netinfo Security 2020, 20(4):12.

[4] Ahmed AIA ,Ab Hamid SH, Gani A, Khan MK: Trust and reputation for Internet of Things: Fundamentals, taxonomy, and open research challenges. Journal of Network and Computer Applications 2019, 145:102409.

[5] لادانی ت, بیدگلی ج: وارسی استحکام سامانه‌های اعتماد. دوفصل نامه علمی ترویجی منادی امنیت فضای تولید و تبادل اطلاعات ۲۰۱۵, ۳(۲):۳٤-۱۵.

[6] Bidgoly AJ, Ladani BT: Benchmarking reputation systems: A quantitative verification approach. Computers in Human Behavior 2016, 57:274-291.

[7] Bidgoly AJ, Ladani BT: Trust modeling and verification using colored petri nets. In: 2011 8th International ISC Conference on Information Security and Cryptology: 2011: IEEE; 2011: 1-8.

[8] Bidgoly AJ, Ladani BT: Modelling and quantitative verification of reputation systems against malicious attackers. The Computer Journal 2015, 58(10):2567-2582.

[9] Bidgoly AJ, Ladani BT: Modeling and quantitative verification of trust systems against malicious attackers. The Computer Journal 2016, 59(7):1005-1027.

[10] Bao F, Chen I-R: Dynamic trust management for internet of things applications. In: Proceedings of the 2012 international workshop on Self-aware internet of things: 2012; 2012: 1-6.

[11] Yan Z, Zhang P, Vasilakos AV: A survey on trust management for Internet of Things. Journal of network and computer applications 2014, 42:120-134.

[12] Chen R, Bao F, Guo J: Trust-based service management for social internet of things systems. IEEE transactions on dependable and secure computing 2015, 13(6):684-696.

[13] Kamvar SD, Schlosser MT, Garcia-Molina H: The eigentrust algorithm for reputation management in p2p networks. In: Proceedings of the 12th international conference on World Wide Web: 2003; 2003: 640-651.

[14] Chen D, Chang G, Sun D, Li J, Jia J, Wang X: TRM-IoT: A trust management model based on fuzzy reputation for internet of things. Computer Science and Information Systems 2011, 8(4):1207-1228.

[15] Chang K-D, Chen J-L: A survey of trust management in WSNs, internet of things and future internet. KSII Transactions on Internet & Information Systems 2012, 6.(۱)

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

[17] Kang K, Pang Z, Da Xu L, Ma L, Wang C :An interactive trust model for application market of the

internet of things. IEEE Transactions on Industrial Informatics 2014, 10(2):1516-1526.
[18] Mohsenzadeh A, Motameni H: A trust model between cloud entities using fuzzy mathematics. Journal of Intelligent & Fuzzy Systems 2015, 29(5):1795-1803.
[19] Kurdi H, Alfaries A, Al-Anazi A, Alkharji S, Addegaither M, Altoaimy L, Ahmed SH: A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments. The Journal of Supercomputing 2019, 75(7):3534-3554.
[20] Fan W, Perros H: A novel trust management framework for multi-cloud environments based on trust service providers. Knowledge-Based Systems 2014, 70:392-406.
[21] Sun D, Chang G, Sun L, Li F, Wang X: A dynamic multi-dimensional trust evaluation model to enhance security of cloud computing environments. International Journal of Innovative Computing and Applications 2011, 3(4):200-212.
[22] Kanwal A, Masood R, Ghazia UE, Shibli MA, Abbasi AG: Assessment criteria for trust models in cloud computing. In: 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing: 2013: IEEE; 2013: 254-261.
[23] Chiregi M, Navimipour NJ: A new method for trust and reputation evaluation in the cloud environments using the recommendations of opinion leaders' entities and removing the effect of troll entities. Computers in Human Behavior 2016, 60:280-292.
[24] Gao B, Zhang N: Configuration method and system of complex network and configuration and management module of server resources. In.: Google Patents; 2014.
[25] Fernandez-Gago C, Moyano F, Lopez J: Modelling trust dynamics in the Internet of Things. Information Sciences 2017, 396:72-82.
[26] Lin C ,Varadharajan V, Wang Y, Pruthi V: Enhancing grid security with trust management. In: IEEE International Conference onServices Computing, 2004(SCC 2004) Proceedings 2004: 2004: IEEE; 2004: 303-310.
[27] Luo J, Liu X, Fan M: A trust model based on fuzzy recommendation for mobile ad-hoc networks. Computer networks 2009, 53(14):2396-2407.
[28] Ashtiani M, Azgomi MA: A formulation of computational trust based on quantum decision theory. Information Systems Frontiers 2016, 18(4):735-764.
[29] Sun Y, Liu Y: Security of online reputation systems: The evolution of attacks and defenses. IEEE Signal Processing Magazine 2012, 29(2):87-97.
[30] Koutrouli E, Tsalgatidou A: Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers. Computer Science Review 2012, 6(2-3):47-70.
[31] Wang D, Muller T, Liu Y, Zhang J: Towards robust and effective trust management for security: A survey. In: 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications: 2014: IEEE; 2014: 511-518.
[32] Kerr R, Cohen R: Smart cheaters do prosper: defeating trust and reputation systems. In: Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 2: 2009: Citeseer; 200 :۹ .۱۰۰۰-۹۹۳
[33] Jøsang A, Golbeck J: Challenges for robust trust and reputation systems. In: Proceedings of the 5th International Workshop on Security and Trust Management (SMT 2009), Saint Malo, France: 2009: Citeseer; 2009.
[34] Milosevic Z, Josang A, Dimitrakos T, Patton MA: Discretionary enforcement of electronic contracts. In: Proceedings Sixth International Enterprise Distributed Object Computing: 2002: IEEE; 2002: 39-50.
[35] Jøsang A: Subjective logic, draft book. In.; 2011.