



# برقراری اعتماد در شبکه‌های بین خودروبی

## مبتنی بر زنجیرهٔ قالبی با بهره‌گیری از استنتاج فازی و ساختار Chord

نیلوفر خسروی راد<sup>۱</sup>، رضا احسن<sup>۲\*</sup>، احمد شریف<sup>۳</sup>، علی کریمی<sup>۴</sup>  
 دانشجوی دکتری، مهندسی کامپیوتر، آزاد اسلامی، قم، ایران  
 استادیار دانشکدهٔ مهندسی کامپیوتر، واحد قم، دانشگاه آزاد اسلامی، قم، ایران\*  
 استادیار دانشکدهٔ مهندسی کامپیوتر، واحد قم، دانشگاه آزاد اسلامی، قم، ایران  
 دانشجوی دکتری، مهندسی کامپیوتر، آزاد اسلامی، قم، ایران

### چکیده

با پیشرفت فناوری در حوزهٔ اینترنت اشیا، شبکهٔ بین خودروبی<sup>۱</sup> تحولی در دنیای فناوری ایجاد کرده‌است. در این شبکه‌ها، گره‌ها به‌عنوان مسیر یاب و میزبان فعالیت کرده و اطلاعات مسیر را بین وسایل نقلیه و RSU به اشتراک می‌گذارند. چالش اصلی این شبکه، اعتماد به پیام‌های مبادله‌شده است که نیاز به صحت‌سنجی گره‌ها پیش از ارتباط دارد. در طرح پیشنهادی، هر وسیلهٔ نقلیه به‌محض مشاهدهٔ یک رخداد، پیامی را به‌صورت همه‌پخشی ارسال می‌کند و RSU برای اعتبارسنجی، میزان اعتماد گره فرستنده را بررسی می‌کند؛ در این راستا، برای جلوگیری از تکرار رخدادها، پیام‌های تکراری منتشر نمی‌شوند؛ به‌منظور افزایش کارایی، ساختار Chord به‌جای الگوریتم‌های اجماع زمان‌بر به‌کار گرفته شده‌است. این سامانه شامل مراحل امتیازدهی به پیام‌ها، محاسبهٔ اعتماد و تشکیل گروه‌های ارزیاب به‌وسیلهٔ RSUها است. نتایج نشان می‌دهد که قابلیت اطمینان پیام‌ها در این روش شش درصد نسبت به SBTMS و یازده درصد نسبت به POW بهبود یافته‌است. این پژوهش با ترکیب VANET، فناوری زنجیرهٔ قالبی و منطق فازی، مدلی کارآمد برای افزایش قابلیت اعتماد در شبکه‌های بین خودروبی ارائه می‌دهد.

واژگان کلیدی: شبکهٔ بین خودروبی، زنجیرهٔ قالبی، ساختار Chord، استنتاج فازی، قابلیت اعتماد.

## Presenting a model for establishing trust in inter-vehicle networks based on blockchain using fuzzy inference and Chord structure

Niloufar Khosravi Rad<sup>1</sup>, Reza Ahsan<sup>2\*</sup>, Ahmad Sharif<sup>3</sup>, Ali Karimi<sup>4</sup>  
 Ph.D. Candidate, Department of Computer Engineering, Islamic Azad University, Qom Branch, Qom, Iran<sup>1&2</sup>  
 Assistant Professor, Faculty of Computer Engineering, Islamic Azad University, Qom Branch, Qom, Iran<sup>2\*&3</sup>

### Abstract

With the swift advancement of the Internet of Things (IoT), Vehicular Ad Hoc Networks (VANETs) have become a crucial component in enabling smart transportation systems by supporting real-time communication between vehicles and roadside units (RSUs). In these networks, vehicles function as mobile nodes that generate and transmit data across the system. A major challenge in VANETs is ensuring the integrity and trustworthiness of shared messages, as any malicious or inaccurate information could severely impact safety and system performance. This research introduces a trust management framework that integrates VANET with blockchain technology and fuzzy logic to improve the reliability of vehicle-to-vehicle communication. When an event is detected, a vehicle instantly broadcasts a corresponding message. RSUs then evaluate the sender's trust level and verify the message before validation. To minimize communication overhead and avoid duplication, repeated messages are filtered prior to distribution. Unlike conventional trust models that depend on computationally heavy consensus mechanisms such as Proof of Work (PoW), the proposed system adopts a Chord-based distributed architecture. This approach significantly lowers processing times and boosts scalability. The framework utilizes a multi-phase trust evaluation process involving message scoring, dynamic trust

<sup>1</sup> VANET

\* Corresponding author

\* نویسندهٔ عهده‌دار مکاتبات

calculation, and formation of evaluator groups by RSUs. Simulations reveal notable gains in message credibility: a 6% increase compared to the Score-Based Trust Management System (SBTMS) and an 11% improvement over PoW-based approaches. These results underline the effectiveness of the proposed model in achieving a balance between security, scalability, and low latency in VANET environments. By merging VANET architecture with decentralized trust mechanisms and soft computing techniques, this study presents an innovative and pragmatic solution to one of the key challenges in vehicular communications—facilitating secure, efficient, and trustworthy message exchange in highly dynamic, distributed networks.

**Keywords:** Blockchain, Chord structure, fuzzy inference, Inter-vehicle network, reliability.

## ۱- مقدمه

با پیدایش شبکه‌های رایانه‌ای با هدف ارتباط داشتن به صورت توزیع شده، شبکه‌های موردی مطرح شد، یک شبکه سیار موردی، شامل مجموعه‌ای از گره‌های توزیع شده است که بدون هیچ زیرساخت و مدیریت مرکزی، یک شبکه موقت را تشکیل می‌دهد [۱، ۲]. در این نوع شبکه‌ها، به علت ساختار پویا، بستری برای همکاری گره‌ها ایجاد خواهد شد؛ درواقع گره‌های موجود در این شبکه هم به عنوان مسیریاب و هم به عنوان میزبان فعالیت دارند [۳]؛ در این راستا ساختاری پویا از شبکه‌های بین خودرویی با عنوان VANET<sup>۱</sup> مطرح شد، که نوع خاصی از شبکه‌های سیار MANET هستند و در آن وسایل نقلیه به صورت پویا و بدون در نظر گرفتن زیرساختی با یکدیگر ارتباط برقرار می‌کنند [۴].

حمل و نقل هوشمند موضوعی است که بعد از معرفی VANET، دنیای فناوری را متحول کرد؛ هوشمندسازی وسایل نقلیه و استفاده از امکانات جدید فناوری می‌تواند یک سامانه حمل و نقل هوشمند را رقم بزند [۵، ۶]. سامانه حمل و نقل هوشمند، به سامانه‌ای گفته می‌شود که دارای ویژگی‌هایی همچون فناوری‌های ارتباطی، کنترل و پردازش یک پارچه اطلاعات در وسایل نقلیه و زیرساخت‌های حمل و نقل است [۷، ۸]. چنین سامانه‌ای بر پایه جمع‌آوری، پردازش، یک پارچه‌سازی و انتشار اطلاعات بنا شده است. این اطلاعات در کل، از داده‌هایی به دست می‌آیند که به صورت ایستا و یا پویا، از حسگرهای روی وسایل نقلیه، حسگرهای موجود در مسیرها، ماهواره‌ها، نقشه‌های رقمی، اطلاعات ترافیکی و همچنین وضعیت هواشناسی به دست آمده‌اند؛ بنابراین استفاده از این اطلاعات باعث می‌شود از وقوع سوانح جاده‌ای جلوگیری شود؛ همچنین می‌توان از آن‌ها برای بهبود ترافیک جاده‌ای و برقراری امنیت استفاده کرد [۹]. شبکه‌های بین خودرویی متشکل از وسایل نقلیه، RSUها است که می‌تواند اطلاعات مسیر را بین اجزای موجود در شبکه به اشتراک بگذارد. بیشتر روابط موجود در VANET مبتنی بر داده‌های مشارکتی، تبادل اطلاعات بین خودروها و تبادل اطلاعاتی با زیرساخت‌های کنار جاده‌ای است [۱۰]. هر وسیله نقلیه با مشاهده هرگونه رخداد، پیامی را برای سایر اجزا منتقل می‌کند تا آن‌ها نیز از وضعیت جاده مطلع شوند؛ در نتیجه می‌توان ویژگی‌هایی همچون پویایی

شبکه، پیش‌بینی مکان خودروها، عدم محدودیت توان را برای آن نام برد [۱۱]. با توجه به اینکه عملکرد این شبکه تحت تأثیر عوامل زیادی مانند همکاری بین گره‌ها، امنیت داده‌ها، حریم خصوصی کاربر، سلامت اطلاعات مبادله شده و صحت و قابلیت اعتماد است [۹]؛ چالش‌هایی همچون ناپدید شدن سیگنال‌های ارتباطی، ارتباط پایدار، برقراری ارتباط، مسیریابی، احراز هویت گره‌ها، مقاومت بودن در برابر حملات، قابلیت اعتماد مطرح می‌شود [۱۲، ۱۳]. برقراری اعتماد در شبکه‌های بین خودرویی یکی از موضوعاتی بوده که تاکنون توسط پژوهش‌گران مورد پژوهش و بررسی قرار گرفته است، برخی از پژوهش‌گران بدون در نظر گرفتن پویایی شبکه‌ها به بررسی میزان اعتماد گره‌ها پرداخته‌اند که کارایی چندانی نداشت [۱۴]؛ همچنین برخی نیز از روش‌های دسته‌بندی یا همان کلاسترینگ استفاده کرده‌اند که این نوع نیز خود ابهاماتی را در بر دارد؛ زیرا اگر سرگروه یک کلاستر مورد حمله قرار گیرد شبکه امنیت خود را از دست می‌دهد [۱۵]. استفاده از روش‌های غیرمتمرکز و پویا که بیشتر به تعاملات بین گره‌ها اشاره دارد، روش خوبی برای برقراری ارتباط امن معرفی شده است، ارتباط امن یکی از پایه‌ای‌ترین زیرساخت‌ها در انواع شبکه است [۱۶]. در کنار استفاده از روش‌های غیرمتمرکز، استفاده از منطق فازی که بر اساس اعتماد مستقیم و غیرمستقیم، یک گره مورد اعتماد را به سایر گره‌ها معرفی می‌کند، کمک شایانی در ایجاد امنیت در شبکه‌های بین خودرویی خواهد داشت. پژوهش‌های بسیاری با هدف ارتقای قابلیت اعتماد در شبکه‌های بین خودرویی صورت گرفته است و می‌توان مدیریت اعتماد موجود در شبکه‌های بین خودرویی را به دو دسته تقسیم کرد؛ دسته نخست، رویکردهای مبتنی بر هوش مصنوعی، مبتنی بر خوشه‌بندی، یادگیری تقویتی، منطق فازی و روش‌های نظریه بازی است. دسته دوم رویکردهای مبتنی بر فناوری‌های نوظهور مبتنی بر Cloud، Fog، Edge، زنجیره قالبی و شبکه‌های تعریف شده با نرم افزار SDN هستند [۱۷]. استفاده از فناوری‌های جدید رویکرد محاسباتی، اعتماد کلاسیک را از نظر دقت، تجمیع و اشتراک ارزش‌های اعتماد بهبود می‌بخشد؛ از طرفی با توجه به حجم زیاد پیام‌هایی که در این شبکه منتقل می‌شود، ذخیره‌سازی آن‌ها در یک سامانه متمرکز صحیح نخواهد بود؛ زیرا با نفوذ به سامانه مدیریت متمرکز کل شبکه از کار خواهد افتاد؛ در نتیجه نیاز به یک سامانه ذخیره‌سازی پایدار است؛ به همین دلیل از فناوری زنجیره قالبی برای ذخیره‌سازی مانا و

<sup>۱</sup> Vehicular Ad Hoc Network

حتی در صورت هک شدن یک یا چند RSU را نیز به شدت کاهش می‌دهد.

از جمله نوآوری‌های کلیدی مدل پیشنهادی می‌توان به موارد زیر اشاره کرد:

- تعریف و محاسبه عددی میزان اعتماد گره با رویکرد فازی و تحلیل داده‌های ورودی در سطح گره؛
- تشکیل گروه‌های ارزیاب توسط RSUها برای جلوگیری از سازش و تمرکز در فرآیند اعتبارسنجی تراکنش‌ها؛
- استفاده از زنجیره قالی برای جلوگیری از تغییر در رخ داده‌ها و پیام‌های شبکه و حفظ یک پارچگی اطلاعات؛
- استفاده از ساختار Chord برای حذف نیاز به ماینینگ و افزایش محرمانگی در ذخیره‌سازی اطلاعات تراکنشی؛
- تشخیص نودهای مخرب و خارج‌سازی آن‌ها از چرخه تأثیرگذاری در تصمیم‌گیری شبکه؛
- افزایش قابلیت اعتماد به پاسخ‌های RSUها حتی در شرایطی که برخی از آن‌ها دچار اختلال یا حمله شده‌اند. در نهایت می‌توان اهداف اصلی پژوهش را به تفکیک زیر بیان کرد:

۱. مدل‌سازی کمی و کیفی مفهوم اعتماد در VANET
۲. تشخیص و ایزوله‌سازی نودهای مخرب با استفاده از منطق فازی؛
۳. پیش‌گیری از تغییر پیام‌های رخداد با بهره‌گیری از زنجیره قالی غیرقابل تغییر
۴. افزایش قابلیت اعتماد به RSUها از طریق حذف فرآیند ماینینگ و بهره‌برداری از Chord
۵. افزایش نرخ تشخیص صحیح پیام‌ها و کاهش پیام‌های کاذب با اتکا به سازوکار اعتماد توزیع‌شده؛
۶. حفظ محرمانگی و امنیت اطلاعات در طول مسیر انتقال و ذخیره‌سازی در معماری پیشنهادی.

## ۲- مفاهیم پایه

### ۲-۱- شبکه‌های بین خودروبی

شبکه‌های بین خودروبی، بخشی مهم از شبکه‌های ITS هستند که به وسیله یک ارتباط کوتاه برد در فواصل صد تا سیصد متر امکان برقراری ارتباط با دیگر وسایل نقلیه را دارند، تمام خودروها در شبکه به عنوان یک گره در نظر گرفته شده‌است [۱۵، ۲۰]. این ارتباط باعث برقراری امنیت و با ارسال پیام‌های داده‌ای از جمله میزان ترافیک جاده‌ها، ارتباطات نظیر به نظیر باعث افزایش بازدهی جاده‌ها می‌شود. هر اتصال در شبکه‌های بین خودروبی وابسته به فرکانس رادیویی است، و گره‌ها برای برقراری ارتباط باید در یک راستا قرار گیرند [۲۱]. شبکه‌های بین خودروبی دارای سه جزء اصلی تجهیزات سخت‌افزاری، کنار جاده‌ای و نرم‌افزاری هستند. درون هر خودرو

پایدار و همیشه در دسترس استفاده شده‌است. دو نوع ساختار عمومی و خصوصی برای زنجیره قالی وجود دارد. تمرکز ما در این پژوهش بر زنجیره قالی خصوصی است [۱۸]. استفاده از این فناوری باعث می‌شود که امنیت پیام‌های تولیدی حفظ شود و امکان تغییر در اطلاعات ثبت‌شده نیز وجود نداشته باشد. در پژوهش [۱۹] مدلی مبتنی بر زنجیره قالی برای شبکه‌های بین خودروبی به منظور افزایش مقیاس‌پذیری و قابلیت اعتماد ارائه شد، در این مدل برای محاسبه اعتماد از قوانین بیزین استفاده شده‌است، ضعف این مقاله نبود توجه به سازش RSUها برای تعیین مقدار اعتماد است.

در مدل پیشنهادی، تمرکز اصلی بر برقراری اعتماد در شبکه‌های بین خودروبی در شرایطی است که ممکن است واحدهای کنار جاده‌ای<sup>۱</sup> در فرآیند اجماع دچار سازش یا نفوذ امنیتی شوند. از آنجایی که حفظ یک پارچگی و صحت پیام‌ها در چنین محیط‌هایی حیاتی است، ما با تلفیق سه فناوری پیشرفته شامل VANET، زنجیره قالی و منطق فازی، یک معماری نوآورانه برای مدیریت اعتماد و تشخیص گره‌های مخرب ارائه می‌دهیم.

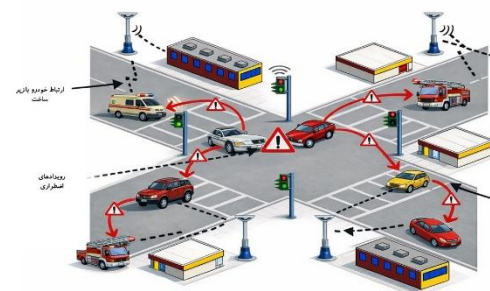
در این پژوهش، اعتماد<sup>۲</sup> به عنوان معیاری پویا و قابل محاسبه تعریف می‌شود که نشان‌دهنده میزان صحت‌سنجی رفتار یک گره (وسیله نقلیه) بر اساس تعاملات گذشته و گزارش‌های سایر گره‌ها در محیط شبکه است؛ به عبارت دقیق‌تر، اعتماد یک مقدار عددی است که از طریق تحلیل ویژگی‌هایی نظیر درست‌بودن پیام‌های ارسالی، تکرار پیام‌ها، تأخیر در ارسال و هم‌پستگی با داده‌های محیطی و سایر گره‌ها محاسبه می‌شود. برای مدل‌سازی و محاسبه میزان اعتماد، از یک سامانه استنتاج فازی استفاده می‌شود. این سامانه با دریافت ورودی‌هایی همچون میزان تأخیر، نرخ تکرار پیام‌های معتبر و اعتبار محاسبه‌شده به وسیله دیگر گره‌ها، یک مقدار نهایی اعتماد برای هر گره محاسبه می‌کند. این مقدار در قالب یک تراکنش به RSUها ارسال و پس از بررسی در یک زیرساخت مقاوم در برابر سازش، در زنجیره قالی ثبت می‌شود. برای افزایش مقیاس‌پذیری، امنیت و حفظ محرمانگی در تبادل و ذخیره‌سازی اطلاعات، از ساختار Chord بهره گرفته شد. ساختار Chord یک الگوریتم جست‌وجوی توزیع‌شده مبتنی بر جدول درهم‌سازی توزیع‌شده<sup>۳</sup> است که باعث می‌شود فرآیند مکان‌یابی اطلاعات و نگاشت کلید/مقدارها در میان نودهای شبکه با پیچیدگی زمانی  $O(\log N)$  و به شکلی امن انجام شود. به کارگیری این ساختار نه تنها نیاز به فرآیند پرهزینه ماینینگ در زنجیره‌های قالی سنتی را از میان برداشته، بلکه امکان دست‌کاری داده‌های ثبت‌شده

<sup>۱</sup> RSU

<sup>۲</sup> Trust

<sup>۳</sup> DHT

واحد سخت‌افزاری به نام OBU<sup>۱</sup> وجود دارد که خود دارای قسمت‌های مختلف اعم از واحد ورودی و خروجی جهت دریافت اطلاعات از کاربران، واحد پردازش، واحد ارتباط سیار، واسط ارتباطی با واحد الکترونیک خودرو و زیرساخت ارتباط با سامانه‌هایی همچون مکان‌یابی است [۲۰]؛



(شکل ۱- نمایش کلی از یک شبکه بین خودرویی  
(figure-1): Inter-Vehicle Network

در واقع OBUها فراهم‌کننده سرویس‌ها هستند که برای فراهم‌کردن نرم‌افزارهای مورد نیاز خود از  $AU^2$ ها استفاده می‌کنند [۲۲]. در کنار تجهیزات سخت‌افزاری که بر روی خودروها نصب می‌شوند، واحد سخت‌افزاری کنارجاده‌ای RSU نیز وجود دارد که در مکان‌هایی همچون تقاطع و یا نزدیک مکان‌های عمومی مثل پارکینگ‌ها قرار گرفته‌اند، این واحد در زیرساخت شبکه و همچنین دارای یک دستگاه شبکه جهت برقراری ارتباط کوتاه برد مبتنی بر IEEE 802.11p است [۱۱]. برقراری ارتباط در شبکه‌های بین خودرویی را می‌توان به سه دسته تقسیم کرد:

- دسته نخست، خودرو به خودرو: این نوع ارتباط از طریق یک کانال ارتباطی مستقیم جهت تبادل اطلاعات بین دو گره برقرار می‌شود. اطلاعات ارسالی شامل ترافیک موجود در مسیر، تصادف و سایر موارد است.
- دسته دوم، خودرو به زیرساخت: منظور از این ارتباط، همان تبادل اطلاعات بین خودرو و واحدهای RSU است، RSUها اطلاعات خودروها را تأمین می‌کنند.
- دسته سوم، ترکیبی: این نوع ارتباط شامل دو نوع ارتباط فوق است، ارتباط در این روش هم به صورت مستقیم و هم غیرمستقیم صورت می‌گیرد [۲۰].

## ۲-۲- زنجیره قالبی

معماری موجود در بین شبکه‌های رایانه‌ای را می‌توان به دو صورت متمرکز و توزیع‌شده دسته‌بندی کرد، معماری متمرکز قدمت و شهرت بالایی دارد و از یک پایگاه داده برای ذخیره‌سازی اطلاعات موجود در شبکه نیز استفاده می‌کند؛ در مقابل خطر این مدل نسبت به مدل توزیع‌شده بیشتر است؛

زیرا با حمله به پایگاه‌داده شبکه منحل می‌شود؛ بنابراین با گذشت زمان شبکه‌ها باتوجه به معماری توزیع‌شده ساخته شده‌اند [۲۳، ۲۴]. زنجیره قالبی یک نمونه از شبکه توزیع‌شده است، که هر گره پایگاه داده کل شبکه را در خود ذخیره کرده‌است و ارتباط بین آن‌ها به صورت p2p است [۲۵]؛ در واقع زنجیره قالبی یک دفترکل توزیع‌شده یا همان پایگاه‌داده توزیع‌شده است که تراکنش‌های صورت گرفته در آن به وسیله تمامی گره‌ها بررسی می‌شود و ذخیره آن باتوجه به نظر اجماعی از گره‌ها صورت می‌گیرد [۲۶]. یک معماری شش لایه برای زنجیره قالبی ارائه شده که هر لایه وظایفی دارد، لایه داده وظیفه ایجاد بلاک، رمزگذاری، تابع درهم‌سازی و برجسب زمانی، لایه شبکه وظیفه انتشار اطلاعات در شبکه و تأیید اعتبار داده‌ها، لایه اجماع وظیفه اجرای الگوریتم‌های اجماع که دارای الگوریتم‌هایی جهت رسیدن به یک توافق کلی بر روی یک بلاک و در شبکه‌هایی که گره‌های غیرقابل اعتماد نیز در آن وجود دارد است. لایه انگیزه وظیفه تعیین سازوکارهای توزیع، لایه قرارداد شامل قوانین، الگوریتم‌ها و قراردادهای هوشمند قابل برنامه‌ریزی است و لایه کاربرد وظیفه سناریوهای مختلف برنامه‌های کاربردی را برعهده دارد [۲۷]. باتوجه به مفاهیم ارائه‌شده، لایه اجماع و داده دو لایه مهم در این فناوری محسوب می‌شوند [۲۳، ۲۸]؛ چرا که وظیفه تأیید تراکنش‌ها و ایجاد اعتماد در لایه اجماع مورد بررسی قرار می‌گیرد. هر گره برای انجام فعالیت خود اطلاعات مورد نیاز خود را در یک تراکنش ثبت می‌کند و آن را با کلید خصوصی خود رمز و به عنوان یک تراکنش آن را برای شبکه زنجیره قالبی ارسال می‌کند [۱۷]. تمامی تراکنش‌ها در شبکه زنجیره قالبی منتشر می‌شود و گره‌های اعتبارسنج وظیفه بررسی اعتبار تراکنش‌ها و ایجاد بلاک را برعهده دارند؛ در نتیجه تراکنش‌ها درون بلاک ذخیره و با استفاده از تابع درهم‌سازی که با مقدار درهم‌سازی بلاک پیشین ترکیب شده‌است رمز می‌شوند؛ باتوجه به این فرایند اگر گرهی قصد تغییر اطلاعات در هر بلوک را داشته باشد به سرعت قابل شناسایی است [۲۹]. هر بلاک در زنجیره قالبی شامل اطلاعاتی از جمله؛ نسخه بلاک<sup>۴</sup> برای نمایش قوانین مورد استفاده در اعتبارسنجی، درخت مرکب که مقدار درهم‌سازی تمام تراکنش‌های موجود در یک بلاک را مشخص می‌کند، برجسب زمانی<sup>۵</sup> نشان‌دهنده زمان کنونی یک بلاک، فیلد N Bit که نشان‌دهنده حد آستانه هدف برای یک درهم‌سازی و سختی شبکه است، فیلد Nonce یک فیلد چهار بیتی که با صفر شروع و نسبت به سختی شبکه مقدار متفاوتی خواهد داشت. مقدار درهم‌سازی بلاک والد مقدار درهم‌سازی شده ۲۵۶ بیتی که به بلاک پیشین اشاره دارد [۳۰]، است

<sup>۳</sup> Distributed Ledger

<sup>۴</sup> Block version

<sup>۵</sup> Time stamp

<sup>۱</sup> On-Board Unit

<sup>۲</sup> Application Unit

منطق فازی اشاره به نمایش مفاهیم مبهم با یک درجه درستی و نادرستی دارد. گزاره‌های مورد استفاده در منطق فازی به‌طور کامل درست و یا نادرست نیستند، بلکه دارای درجه درستی و نادرستی هستند [۳۱]؛ برای مثال اگر یک گزاره درست باشد برای آن مقدار یک و اگر نادرست باشد مقدار صفر لحاظ می‌شود؛ در نتیجه میزان صحت یا نادرستی یک گزاره همواره بین صفر تا یک است [۳۲]. در تئوری فازی به جای استفاده از اعداد، متغیرهای زبانی<sup>۱</sup> کاربرد دارند [۳۳]؛ در واقع یک مجموعه فازی شامل اعضایی است که با یک درجه عضویت نسبی به مجموعه متعلق‌اند [۳۴]. منطق فازی دارای چهار بخش قوانین پایه است که این بخش مسئولیت کنترل تصمیم‌های یک سامانه را بر اساس یک سری قاعده، مبتنی بر اگر و آن‌گاه دارد. روند فازی‌سازی، شامل اطلاعاتی است که باید مورد پردازش قرار گیرند و به اعداد فازی تبدیل شوند. واحد استنتاج که دارای سامانه‌های متعددی، از جمله سامانه ممدانی<sup>۲</sup> که بیشتر برای پشتیبانی از تصمیم‌ها و تفسیرهای قوانین استفاده می‌شوند، سوگنو<sup>۳</sup> که در سامانه‌های کنترلی و سامانه‌هایی که نیازمند محاسبات ریاضی هستند، اشاره کرد و روند غیرفازی آخرین مرحله از فازی‌سازی است، که تمام اطلاعات فازی به اطلاعات عددی و کمی تبدیل می‌شود [۳۴]. استفاده از منطق فازی برای مدل‌سازی عدم قطعیت در داده‌ها در مطالعات مختلف مورد توجه قرار گرفته است؛ بهر حال، در یک پژوهش منتشرشده در نشریه پردازش علائم و داده‌ها، روشی برای تعیین توابع عضویت فازی بر اساس ویژگی‌های آماری داده‌ها ارائه شده است که نشان می‌دهد بهره‌گیری از این توابع می‌تواند دقت تصمیم‌گیری را در محیط‌های دارای عدم قطعیت و داده‌های نوفه‌ای به‌طور قابل توجهی بهبود دهد [۵۱]. این ویژگی، استفاده از منطق فازی را به گزینه‌ای مناسب برای ارزیابی اعتماد و اعتبار پیام‌ها در شبکه‌های VANET تبدیل می‌کند.

## ۲-۴- ساختار Chord

الگوریتم Chord یک الگوریتم هش توزیع‌شده غیرمتمرکز برای اتصال نودها در یک شبکه نظیربه‌نظیر است. این الگوریتم به‌طور یک‌نواخت یک کلید را به یک نود نگاشت می‌کند. کلیدها و نودها هرکدام دارای یک شناسه  $m$  بیتی هستند [۳۵]. نودها به‌صورت یک حلقه منطقی سازمان‌دهی می‌شوند و هر نود دارای یک مجموعه از اشاره‌گرها به نودهای همسایه خود است که در یک فضای لگاریتمی در اطراف حلقه قرار می‌گیرند؛ همچنین هر نود یک پیوند به نود بعدی و پیشین خود دارد. جدول مسیریابی Chord که در اصطلاح جدول بندانگشتی<sup>۴</sup>

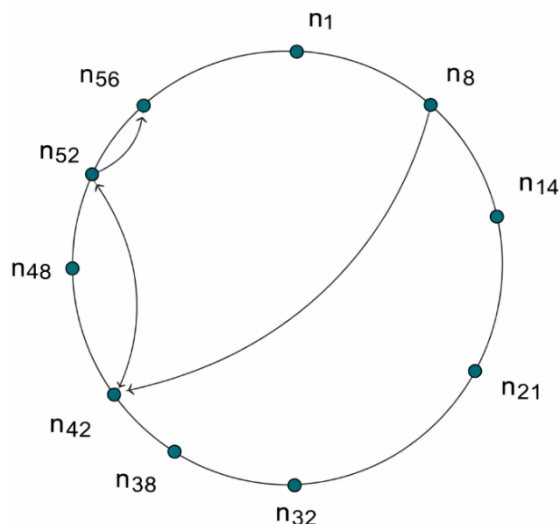
<sup>۱</sup> Linguistic Variables

<sup>۲</sup> Mamdani

<sup>۳</sup> Sugeno

<sup>۴</sup> Finger table

نام دارد، برای هر نود جداگانه ساخته می‌شود و هر نود را قادر به دسترسی به سایر نودهای دورتر در حلقه با پیمایش در جهت حرکت عقربه‌های ساعت می‌سازد [۳۶]. موقعیت هر نود در حلقه از صفر تا  $2^m - 1$  شماره‌گذاری و کلید  $k$  به  $Successor(k)$  انتصاب داده می‌شود و نودی است که شناسه آن برابر یا دنباله‌رو شناسه  $k$  است. اگر در شبکه  $N$  نود  $k$  کلید وجود داشته باشد، هر نود مسئول  $k/N$  کلید خواهد بود. شکل (۲) نمونه‌ای از حلقه Chord را نمایش می‌دهد [۳۷].



(شکل-۲): حلقه‌ای از ساختار Chord  
(Figure-2): Cord structure

در حالت پایدار، هر نود شرکت‌کننده در شبکه Chord، اطلاعاتی در حدود  $O(\log N)$  در مورد نودهای دیگر را نگهداری می‌کند و همچنین عمل جست‌وجو را از طریق  $O(\log N)$  پیام انجام می‌دهد. با ورود نودها به شبکه و یا جدایی آن‌ها از شبکه، الگوریتم Chord تضمین می‌کند که جست‌وجوی هر داده در مرتبه‌ای کمتر از  $O(\log^2 N)$  انجام می‌شود [۳۸].

## ۳- بررسی کارهای پیشین

در [۳۹] یک سامانه مدیریت اعتماد مبتنی بر فناوری زنجیره قالبی برای شبکه‌های بین‌خودرویی پیشنهاد شده است. در این سامانه وسایل نقلیه در شبکه ابتدا اطلاعات پیرامون خود را جمع‌آوری و سپس اطلاعات معتبر را در RSUهای مجاور آپلود می‌کنند. برای جلوگیری از بارگذاری پیام‌های نادرست به‌وسیله وسایل نقلیه مخرب، این مقاله یک مدل راستی‌آزمایی مبتنی بر یادگیری عمیق را طراحی کرده تا قابلیت اعتماد پیام‌های بارگذاری‌شده را محاسبه و امتیازات اعتبار خودروها را با استفاده از نتایج محاسبه‌شده به‌دست آورد و بر این اساس خودروهای مخرب را شناسایی کند؛ علاوه بر این، یک چهارچوب زنجیره قالبی عمومی با الگوریتم اجماع اثبات اعتماد<sup>۵</sup> پیشنهاد کرد. در این طرح برای وسایل نقلیه با گزارش

<sup>۵</sup> POT

اطلاعات معتبر پاداش و برای اطلاعات نامعتبر جریمه در نظر گرفته شده است. در [۴۰] یک طرح جدید برای اشتراک‌گذاری امن داده‌های ترافیکی با ادغام زنجیره قالی و الگوریتم امضای قابل ردیابی برای ایمن‌سازی پیام‌های ارسالی ارائه شد. این طرح از قرارداد هوشمند برای ردیابی وسایل نقلیه غیرقانونی و بازگرداندن نتایج به مقامات مورد اعتماد استفاده می‌کند. مقامات مورد اعتماد منبع پیام امضا را نگه می‌دارد و مجازات‌ها را تعیین می‌کند.

مقاله [۴۱] یک سامانه شهرت غیرمتمرکز را بر اساس یک کنسرسیوم زنجیره قالی و قراردادهای هوشمند به نام BRS4 VANETs توصیف می‌کند. این سامانه قابلیت اطمینان داده‌های تولیدشده به وسیله یک وسیله نقلیه را تجزیه و تحلیل، رفتارهای مخرب را شناسایی و به تصمیم‌گیری کمک می‌کند. در [۴۲] پژوهش‌گران برای حفظ حریم خصوصی مکان، در شبکه‌های خودرویی هوشمند یک مدل مدیریت اعتماد ارائه کرده‌اند که مبتنی بر زنجیره قالی است. در این طرح وسایل نقلیه می‌توانند برای درخواست LBS بدون افشای هیچ‌گونه اطلاعات شخصی از گواهی استفاده کنند. به منظور تضمین حریم خصوصی و امنیت وسایل نقلیه، یک منطقه ناشناس نیز ایجاد کرده‌اند. در [۴۳] پژوهش‌گران یک سازوکار خوشه‌بندی را پیشنهاد می‌کنند که امنیت را فراهم و کیفیت را پس از فرمول‌بندی خوشه بر اساس مؤلفه‌های ازپیش تعریف‌شده حفظ می‌کند. برای رسیدگی به حملات احتمالی در محیط VANET، سازوکار پیشنهادی از زنجیره قالی برای رمزگذاری محاسبات از مؤلفه‌های اعتماد استفاده می‌کند. درجه اعتماد خاصی از یک وسیله نقلیه به وسیله ایستگاه پایه ارزیابی می‌شود، این فرایند با رویکرد زنجیره قالی رمزگذاری و برای استفاده بیشتر به واحدهای کنار جاده‌ای منتقل می‌شود.

در [۴۴] پژوهش‌گران یک طرح احراز هویت امن را پیشنهاد کرده‌اند که به وسایل نقلیه اجازه می‌دهد تا پیام‌های ناشناس را به RSU ارسال و حریم خصوصی را حفظ کند، در این مقاله مدلی از مدیریت اعتماد پیشنهاد شده است که RSU می‌تواند قابل اعتماد بودن گره‌های خودرو و داده‌های ترافیک را تأیید کند؛ بنابراین، طرح اعتماد به RSU اجازه می‌دهد تا وسایل نقلیه مخرب ارسال‌کننده اطلاعات نادرست را شناسایی، گزارش‌های دریافتی از وسایل نقلیه را ارزیابی و فقط رویدادهای واقعی را پخش کند.

در [۴۵] یک چهارچوب مدیریت اعتماد مبتنی بر زنجیره قالی پیشنهاد شده است. هدف آن محاسبه معیار اعتماد جهانی و ذخیره‌کردن در زنجیره قالی برای هر وسیله نقلیه است. مدل پیشنهادی این مقاله بر اساس سه مرحله ارزیابی معیارهای اعتماد، تجمیع معیارهای اعتماد، تولید و اعتبارسنجی بلوک‌ها ساخته شده است. هر وسیله نقلیه معیار

اعتماد همسایگان خود را بر اساس پیام‌های دریافتی، ارزیابی می‌کند؛ سپس ماینرها معیارهای اعتماد دریافتی از وسایل نقلیه دیگر را جمع‌آوری کرده تا یک معیار اعتماد جمعی برای هر وسیله نقلیه را محاسبه کنند. معیار اعتماد جمع‌آوری‌شده در یک بلوک امضا شده به وسیله ماینر بسته‌بندی؛ در نتیجه پس از حل POW به زنجیره قالی اضافه می‌شود. با این مشکل شروع سرد نیز حل خواهد شد. در [۴۶] پژوهش‌گران زنجیره‌های قالی مختلفی را برای احراز هویت، ذخیره مقادیر اعتماد و پیام رویدادهای تأییدشده، طراحی کرده‌اند. طرح مدیریت اعتماد پیشنهادی، ارزش کل اعتماد یک وسیله نقلیه را با استفاده از تجربیات مستقیم و اطلاعات غیرمستقیم در مورد فرستندگان محاسبه می‌کند. این روش به شناسایی وسایل نقلیه مخرب و پیام‌های جعلی که تولید شده است، کمک می‌کند. در [۱۷] یک چهارچوب زنجیره قالی بیومتریک برای ایمن‌سازی اشتراک داده‌ها در بین وسایل نقلیه در VANET و حفظ داده‌های مجسمه‌ای در یک سامانه معمولی و قابل اعتماد طراحی شده است. در چهارچوب پیشنهادی، اطلاعات بیومتریک برای حفظ سابقه هویت واقعی فرستنده پیام، در نتیجه حفظ حریم خصوصی و ارائه ناشناس بودن مشروط استفاده می‌شود. رویکرد پیشنهادی امنیت و اعتماد را در بین وسایل نقلیه در VANET و همچنین قابلیت ردیابی هویت در صورت لزوم را فراهم می‌کند. در پژوهش [۱۹] مدلی مبتنی بر زنجیره قالی برای شبکه‌های بین‌خودرویی به منظور افزایش مقیاس‌پذیری و قابلیت اعتماد ارائه شد، در این مدل برای محاسبه اعتماد از قوانین بیزین و برای ذخیره‌سازی پیام‌ها از ساختار توزیع‌شده زنجیره قالی استفاده شده است؛ این پژوهش باعث افزایش مقیاس‌پذیری و قابلیت اعتماد در یک شبکه بین‌خودرویی شد، اما ضعف این مقاله بی‌توجهی به سازش RSUها برای تعیین مقدار اعتماد است؛ لذا با توجه به بررسی‌هایی که انجام شد، در این پژوهش تلاش شد تا راه‌کاری با هدف افزایش قابلیت اعتماد در شبکه‌های بین‌خودرویی مبتنی بر زنجیره قالی با بهره‌گیری از استنتاج فازی جهت محاسبه اعتماد مستقیم و غیرمستقیم و ساختار کورد جهت برقراردادن سازش بین RSUها ارائه شود. در سال ۲۰۲۵ مقاله [۴۷] ارائه شد که هدف آن ترکیب قابلیت‌های شفاف و تغییرناپذیری زنجیره قالی با قدرت پیش‌بینی مدل‌های یادگیری ماشین بود تا یک چهارچوب پویا برای مدیریت اعتماد در VANET به‌دست آورد، در این پژوهش رفتار خودروها شامل مؤلفه‌هایی مانند تأخیر پیام، کیفیت ارسال و صحت اطلاعات به وسیله مدل ML مورد بررسی نیز قرار گرفت. مقاله [۴۸] یک سامانه مدیریت اعتماد نوآورانه با نام TrCoin را برای شبکه‌های بین‌خودرویی معرفی می‌کند. TrCoin با بهره‌گیری از فناوری زنجیره قالی و یک ارز

(جدول-۱) مقایسه کارهای پیشین پژوهشگران

(Table-1): Comparison of previous works of researchers

| مقاله | عنوان                                                               | نکات کلیدی                                                                                      | ویژگی                                                       | محدودیت                                                 | نوآوری نسبت به پژوهش                                                                                |
|-------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ۳۹    | سامانه مدیریت اعتماد مبتنی بر زنجیره قالی برای شبکه‌های بین خودروبی | جمع‌آوری اطلاعات به وسیله وسایل نقلیه و بارگذاری به RSU، مدل راستی‌آزمایی مبتنی بر یادگیری عمیق | شناسایی خودروهای مخرب، سامانه پاداش و جریمه                 | نیاز به داده‌های معتبر برای عملکرد بهینه                | استفاده از یادگیری عمیق برای ارزیابی اعتماد، فاقد سامانه فازی و ساختار کمیته‌ای RSU برای اجماع سریع |
| ۴۰    | اشتراک‌گذاری امن داده‌های ترافیکی                                   | ادغام زنجیره قالی و الگوریتم امضای قابل ردیابی                                                  | استفاده از قرارداد هوشمند برای ردیابی وسایل نقلیه غیرقانونی | وابستگی به مقامات مورد اعتماد برای تعیین مجازات         | تمرکز بر ردیابی خودروها، فاقد تعامل فازی بین گروه‌ها و ساختار Chord برای بهبود امنیت و مقیاس‌پذیری  |
| ۴۱    | سامانه شهرت غیرمتمرکز (BRS4 VANETs)                                 | تجزیه و تحلیل قابلیت اطمینان داده‌ها و شناسایی رفتارهای مخرب                                    | استفاده از کنسرسیوم زنجیره قالی و قراردادهای هوشمند         | محدودیت در مقیاس‌پذیری و نیاز به همکاری بین وسایل نقلیه | مدیریت اعتماد غیرمتمرکز، اما فاقد سامانه فازی و کمیته‌های RSU برای کاهش خطا و افزایش اعتماد         |
| ۴۲    | مدل مدیریت اعتماد برای حفظ حریم خصوصی مکان                          | درخواست LBS بدون افشای اطلاعات شخصی                                                             | ایجاد منطقه ناشناس برای وسایل نقلیه                         | پیچیدگی در پیاده‌سازی و مدیریت حریم خصوصی               | تمرکز بر حفظ حریم مکان، بدون بهره‌گیری از سامانه فازی و اجماع مبتنی بر کمیته RSU                    |
| ۴۳    | سازوکار خوشه‌بندی برای امنیت در VANET                               | فرمول‌بندی خوشه بر اساس مؤلفه‌های از پیش تعریف‌شده                                              | استفاده از زنجیره قالی برای رمزگذاری محاسبات                | ممکن است در برابر حملات پیشرفته آسیب‌پذیر باشد          | استفاده از خوشه‌بندی، اما فاقد استنتاج فازی و الگوریتم Chord برای کاهش تأخیر و بهبود امنیت          |
| ۴۴    | طرح احراز هویت امن برای وسایل نقلیه                                 | ارسال پیام‌های ناشناس به RSU                                                                    | ارزیابی قابل اعتماد بودن گروه‌های خودرو                     | چالش‌های مربوط به مدیریت هویت و ناشناسی                 | تمرکز بر ناشناسی، اما فاقد سامانه فازی و کمیته‌های RSU برای اجماع و افزایش اعتماد شبکه              |
| ۴۵    | چارچوب مدیریت اعتماد مبتنی بر زنجیره قالی                           | محاسبه معیار اعتماد جهانی و ذخیره در زنجیره قالی                                                | ارزیابی اعتماد همسایگان و جمع‌آوری داده‌ها                  | نیاز به فرآیندهای محاسباتی سنگین                        | ثبت اعتماد در زنجیره قالی، اما فاقد سامانه فازی و ساختار Chord برای کاهش پیچیدگی و زمان پردازش      |
| ۴۶    | طراحی زنجیره‌های قالی مختلف برای احراز هویت                         | محاسبه ارزش کل اعتماد یک وسیله نقلیه                                                            | شناسایی وسایل نقلیه مخرب و پیام‌های جعلی                    | نیاز به تجربیات مستقیم و اطلاعات غیرمستقیم              | تمرکز بر احراز هویت، فاقد ارزیابی اعتماد غیرمستقیم با منطق فازی و کمیته‌های RSU                     |
| ۱۷    | چارچوب زنجیره قالی بیومتریک                                         | استفاده از اطلاعات بیومتریک برای حفظ هویت                                                       | امنیت و اعتماد در VANET                                     | نیاز به زیرساخت‌های بیومتریک و چالش‌های حریم خصوصی      | استفاده از بیومتریک برای امنیت، اما فاقد تعاملات فازی و ساختار Chord برای بهبود اجماع               |
| ۱۹    | مدل مبتنی بر زنجیره قالی برای افزایش مقیاس‌پذیری                    | استفاده از قوانین بیزین برای محاسبه اعتماد                                                      | افزایش مقیاس‌پذیری و قابلیت اعتماد                          | نداشتن توجه به سازش RSU در تعیین مقدار اعتماد           | افزایش مقیاس‌پذیری، اما بدون سامانه فازی و کمیته‌های RSU برای اجماع امن                             |
| ۴۷    | چارچوب یادگیری ماشین مبتنی بر زنجیره قالی برای                      | استفاده از الگوریتم ML برای ایجاد نمره                                                          | دقت بالا، انعطاف‌پذیری بالا در مواجهه با                    | نبود شفافیت در نحوه مقابله با حملات                     | استفاده از ML و زنجیره قالی، اما فاقد ساختار                                                        |

| مقاله | عنوان                                                                              | نکات کلیدی                                                                                   | ویژگی                                                                                                                                               | محدودیت                                                                                                                       | نوآوری نسبت به پژوهش                                                                       |
|-------|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
|       | مدیریت اعتماد در شبکه‌های بین خودرویی                                              | اعتماد و استفاده از زنجیره قالبی برای ثبت نمرات اعتماد                                       | رفتارهای جدید، مقیاس‌پذیری مناسب                                                                                                                    | نوظهور، ترکیب ML و زنجیره قالبی کارایی بالایی اما باید بررسی شود آیا در شرایط واقعی نیز قابل قبول است.                        | Chord و کمیته‌های RSU برای کاهش پیچیدگی و تأخیر                                            |
| ۴۸    | یک سامانه مدیریت اعتماد قوی مبتنی بر زنجیره قالبی برای VANET (TrCoin) (۲۰۲۵)       | استفاده از زنجیره قالبی برای ثبت پیام‌ها و اعتمادسازی، ترکیب ارز داخلی و سیاست پاداش و تنبیه | انعطاف‌پذیری بالا در مواجهه با حملات Sybil و نشر اطلاعات کاذب                                                                                       | استفاده از زنجیره قالبی باعث افزایش تأخیر و هزینه محاسباتی در شرایط بلادرنگ می‌شود، بی‌توجهی به همکاری چند نود برای خراب‌کاری | مقابله با حملات Sybil، اما فاقد سامانه فازی و Chord برای اجماع سریع و کاهش سر بار محاسباتی |
| ۴۹    | انتخاب نقطه دسترسی سیار چند مسیره مبتنی بر زنجیره قالبی برای VANET‌های امن G5 [۴۹] | ادغام زنجیره قالبی و انتخاب چند مسیری multi-path MAP selection                               | افزایش اعتماد بدون سرور مرکزی به علت استفاده از زنجیره قالبی، امکان گسترش برای شبکه‌های آینده‌نگر                                                   | هزینه بالای پردازش در محیط‌های واقعی، تحلیل امنیتی محدود به حمله Sybil و نداشتن تمرکز بر روی سایر حملات                       | قابلیت multi-path برای اعتماد، اما فاقد سامانه فازی و کمیته RSU برای بهبود اجماع           |
| ۵۰    | چهارچوب مدیریت اعتماد برای شبکه‌های موردی وسایل نقلیه [۵۰]                         | بهره‌گیری از دستگاه‌های ضد خراب‌کاری TPD                                                     | ارسال نکردن مداوم امتیاز اعتماد در پیام‌ها، کاهش بار شبکه، افزایش امنیت با ارزیابی قوی و سریع در مبدأ و TPD به وسیله تصمیم‌گیری هوشمند RSU به وسیله | وابستگی به سخت‌افزار خاص (TPD)                                                                                                | کاهش سر بار شبکه با TPD، اما فاقد سامانه فازی و Chord برای اجماع امن و مدیریت تراکنش‌ها    |

کاهش سر بار شبکه وجود دارد. در برخی مطالعات، ترکیب روش‌های یادگیری ماشین و منطق فازی برای تحلیل داده‌های پیچیده مورد استفاده قرار گرفته است؛ برای مثال، در [۵۲] یک مدل عصبی-فازی برای پیش‌بینی داده‌ها ارائه شده است که دقت بالایی در محیط‌های پویا نشان می‌دهد. در ادامه یک جدول از کارهای پیشین مورد مطالعه در طی سال‌های اخیر ارائه شده است.

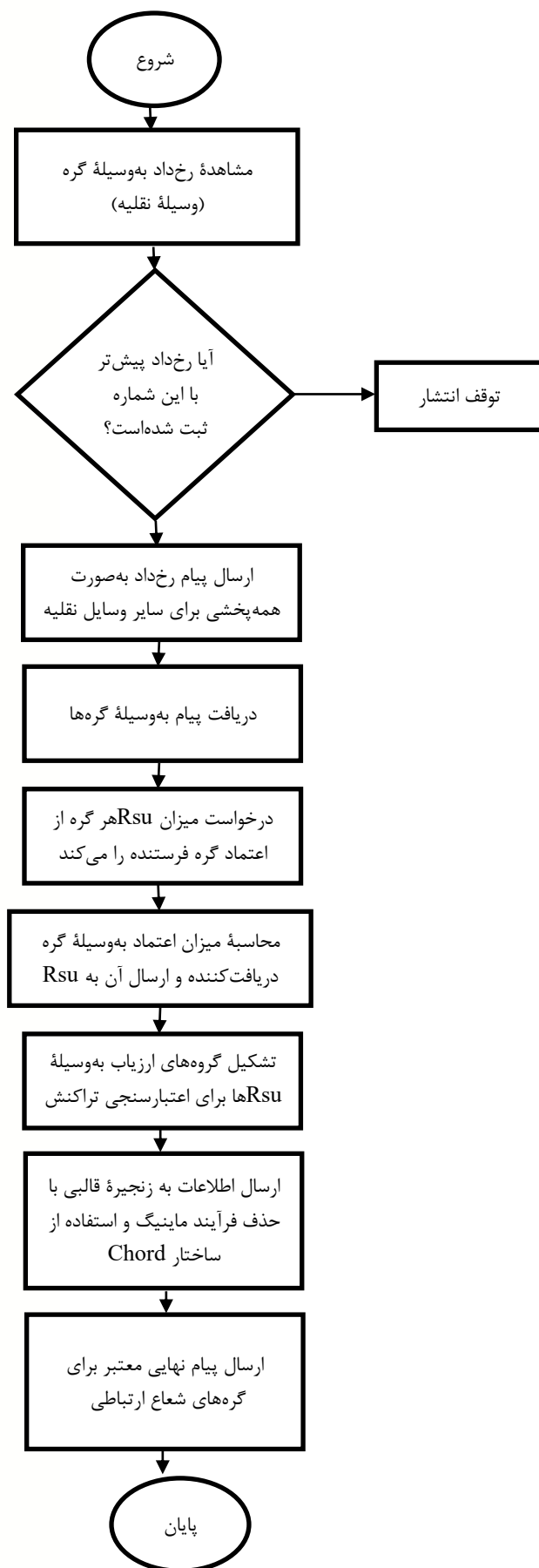
#### ۴- روش پیشنهادی

پس از بررسی چالش‌های اصلی شبکه‌های بین خودرویی شامل اعتماد، امنیت و مقیاس‌پذیری، روش پیشنهادی این پژوهش ارائه می‌شود؛ در این روش، با در نظر گرفتن فرض‌هایی نظیر تجهیز تمامی گره‌های شبکه به فرستنده و گیرنده بی‌سیم، اختصاص شناسه<sup>۲</sup> و شمارنده به رخدادهای شبکه و نیز تجهیز گره‌ها به GPS برای

رقمی داخلی، سازوکاری برای ارزیابی اعتماد پیام‌ها در شبکه فراهم می‌سازد. سامانه پیشنهادی توانایی تشخیص اطلاعات نادرست را دارد و با اعمال سیاست‌های پاداش و تنبیه، رفتار نودها را بهبود می‌بخشد. مقاله [۴۹] یک راه کار مبتنی بر زنجیره قالبی برای انتخاب چندگانه و ایمن<sup>۱</sup> MAP در شبکه‌های خودرویی مبتنی بر G5 ارائه می‌دهد. به جای انتخاب یک مسیر یا نقطه دسترسی، سامانه به صورت multi-path و پویا عمل می‌کند و چند مسیر مطمئن را برای ارتباطات در VANET انتخاب می‌کند. هدف مقاله افزایش امنیت و کاهش تأخیر در دسترسی خودروها به منابع شبکه (برای مثال سرورها یا RSUها)، به ویژه در برابر حملات Sybil و دیگر تهدیدهای رایج در VANET است. مقاله [۵۰] به مدیریت اعتماد در شبکه‌های متحرک خودرو با ارائه یک چهارچوب اعتماد مبتنی بر محل تولید پیام پرداخته است، با توجه به کنترل اعتماد در مبدأ پیام، به علت ارسال نشدن مداوم امتیاز اعتمادها

<sup>۲</sup> ID

<sup>۱</sup> Mobile Access Point



(شکل- ۳) نمودار جعبه‌ای روش پیشنهادی  
(figure-3): Block diagram of the proposed method

موقعیت‌یابی و شناسایی همسایگان، عملکرد سامانه به صورت زیر تعریف می‌شود:

هر گره با دریافت اطلاعات از همسایگان خود، فهرست به‌روزشده‌ای از گره‌های همسایه نگهداری می‌کند؛ در صورتی که گرهی در بازه زمانی مشخص، پیامی از همسایگان خود دریافت نکند، از محدوده ارتباطی آن‌ها حذف می‌شود.

مبنای اصلی تصمیم‌گیری در این شبکه، اطلاعات دریافتی از گره‌های همسایه است. در طرح پیشنهادی، هر وسیله نقلیه در صورت مشاهده یک رخداد در محدوده دید خود، پیامی شامل شناسه رخداد و موقعیت جغرافیایی آن را به صورت همه‌پخشی به سایر وسایل نقلیه ارسال می‌کند؛ از آنجا که چند وسیله نقلیه ممکن است رخداد مشابهی را گزارش دهند، گره دریافت‌کننده برای اعتبارسنجی رخداد، از ایستگاه کنار جاده میزان اعتماد گره فرستنده را درخواست می‌کند؛ سپس، هر گره میزان اعتماد محاسبه‌شده خود را برای RSU ارسال می‌کند تا در پایگاه داده اعتماد ثبت شود.

در ادامه، برای به‌روزرسانی اطلاعات در شبکه، گره‌ها پیام معتبر را برای سایر وسایل نقلیه در شعاع ارتباطی خود ارسال می‌کنند؛ در صورتی که رخدادی با شناسه خاص پیش‌تر به وسیله یک گره گزارش شده باشد، پیام مشابه تحت عنوان «پایش اولیه» مجدد منتشر نمی‌شود. این سازوکار علاوه بر کاهش حجم داده‌های تکراری، موجب کنترل کهنگی پیام‌ها و جلوگیری از انتشار داده‌های قدیمی می‌شود.

به دلیل حجم بالای اطلاعات و محدودیت زمانی در محیط‌های بین خودرویی، استفاده از الگوریتم‌های اجماع سنتی مانند PoW یا PoS کارایی کافی ندارد؛ از این رو در ساختار پیشنهادی، فرآیند ماینینگ حذف و ساختار حلقوی Chord جایگزین آن شده است تا سرعت تأیید تراکنش‌ها افزایش یابد؛ همچنین، به منظور تسریع فرآیند اجماع، گروه‌های ارزیاب در سطح RSU تشکیل می‌شوند که وظیفه آن‌ها بررسی و تأیید تراکنش‌های دریافتی و ارسال نهایی آن‌ها به زنجیره بلوکی است.

در مجموع، سامانه مدیریت اعتماد مبتنی بر زنجیره قالبی پیشنهادی شامل مراحل زیر است:

۱. امتیازدهی به پیام‌ها و ارسال نتایج به RSU
  ۲. محاسبه میزان اعتماد خالص و کل توسط RSU
  ۳. تشکیل گروه‌های ارزیاب در سطح RSUها
  ۴. اعتبارسنجی نهایی و ذخیره‌سازی در زنجیره بلوکی
- شکل (۳) نمودار جعبه‌ای کلی این فرآیند را نشان می‌دهد، که در آن ارتباط میان گره‌های وسایل نقلیه، RSUها و زنجیره قالبی به تفکیک مرحله نمایش داده شده است.

به‌طور طبیعی، پیام‌هایی که از وسایل نقلیه نزدیک‌تر به محل حادثه ارسال می‌شوند، معتبرتر از پیام‌های دریافتی از وسایل نقلیه دورتر هستند. برای ارزیابی این اعتبار، گره گیرنده با استفاده از معادله (۱) مقدار اعتماد  $C_s$  پیام را نسبت به فرستنده  $v_s$  محاسبه می‌کند.

$$C_s = \frac{2}{1+e^{s(g-(d_s)^{-1})}} - 1 \quad (1)$$

در این رابطه:

- $C_s$  میزان اعتماد به پیام ارسال شده از گره  $v_s$
- $d_s$  فاصله بین فرستنده پیام و محل حادثه
- $g$ : نقطه عطف تابع سیگموئید که میزان حساسیت تغییر اعتماد را کنترل می‌کند.
- $s$ : ضریب شیب تابع که شدت کاهش اعتماد با فاصله را تعیین می‌کند.

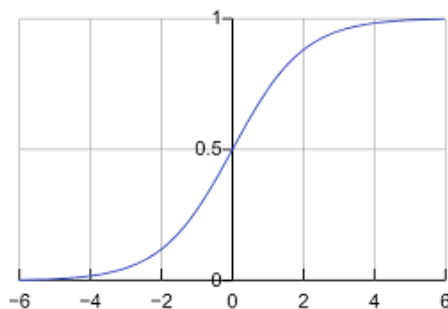
مؤلفه  $d_s$  بر اساس رابطه هندسی زیر محاسبه می‌شود:

$$d_s = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (2)$$

که در آن  $i$  نشان‌دهنده موقعیت گره ارسال‌کننده و  $j$  نشان‌دهنده مختصات محل حادثه است؛ در صورتی‌که گرهی پیامی ارسال نکند، مقدار  $C_s = 0$  در نظر گرفته می‌شود؛ درمقابل، اگر پیام از گرهی با بالاترین میزان اعتبار دریافت شود،  $C_s = 1$  خواهد بود.

تابع به‌کاررفته در معادله (۱) برگرفته از تابع سیگموئید<sup>۴</sup> است که به‌طور گسترده در مدل‌سازی رفتارهای احتمالی و غیرخطی استفاده می‌شود. شکل (۴) نمایی از تابع سیگموئید است، که نقش کاهش اعتماد به پیام‌ها با افزایش فاصله گره‌ها از رخداد را نشان می‌دهد.

- ورودی تابع، فاصله بین گره فرستنده پیام و رخداد واقعی است.
- خروجی تابع، وزن تأثیر پیام بر محاسبه اعتماد نهایی را تعیین می‌کند.
- این مکانیزم، مانع از تأثیرگذاری بیش‌ازحد پیام‌های دوردست و نادرست بر اعتماد شبکه می‌شود.



(شکل-۴): تابع سیگموئید و تغییرات آن با فاصله از محل حادثه

(Figure-4): Sigmoid function

<sup>4</sup> Sigmoid Function

• گره‌های وسایل نقلیه<sup>۱</sup>: این مؤلفه مسئول مشاهده رخدادها در شعاع دید خود، ارسال پیام‌های همه‌پخشی به دیگر وسایل نقلیه و محاسبه اعتماد به فرستنده پیام است؛ همچنین پیام‌های معتبر دریافت‌شده را پردازش کرده و در صورت نیاز به روزرسانی به RSU ارسال می‌کند.

• RSU: نقش پایگاه داده اعتماد و مدیریت تراکنش‌ها را ایفا، گزارش‌های اعتماد از وسایل نقلیه را دریافت، اعتماد خالص و کل را محاسبه و گروه‌های ارزیاب را برای اعتبارسنجی نهایی تراکنش‌ها سازماندهی می‌کنند.

• گروه‌های ارزیاب<sup>۲</sup>: این گروه‌ها مسئول بررسی تراکنش‌های دریافتی، اعتبارسنجی آن‌ها و ارسال نتایج به زنجیره قالبی هستند تا فرآیند اجماع سریع و امن انجام شود.

• زنجیره قالبی<sup>۳</sup>: ذخیره‌سازی تراکنش‌های تأییدشده، تضمین تغییر نکردن اطلاعات و ثبت نهایی اعتبار رخدادها.

• مسیر جریان داده: نشان‌دهنده مسیر انتقال اطلاعات از وسیله نقلیه به RSU؛ سپس به گره ارزیاب و در نهایت ثبت در زنجیره قالبی است، که مراحل مشاهده، ارسال، اعتبارسنجی و ذخیره‌سازی را به‌وضوح مشخص می‌کند. در این شکل مسیر جریان داده، نحوه تبادل پیام‌های اعتماد و ساختار گروه‌های ارزیاب مشخص شده‌است تا درک سازوکار سامانه برای خوانندگان آسان‌تر شود.

## ۴-۱- امتیازدهی به پیام‌های دریافت‌شده و

### ارسال به RSU

فرآیند امتیازدهی پیام‌ها بر مبنای رفتار و موقعیت وسایل نقلیه در محیط شبکه بین‌خودرویی انجام می‌شود. هر وسیله نقلیه، در صورت مشاهده رخدادی خاص در مسیر خود، آن را به‌صورت پیام همگانی برای وسایل نقلیه اطراف ارسال می‌کند.

هر پیام ارسالی به‌صورت چندتایی  $(v_s, LL, e, m)$  تعریف می‌شود که در آن:

- $v_s$  شناسه فرستنده پیام
- $LL$  مختصات جغرافیایی (طول و عرض جغرافیایی) محل رخداد
- $e$  نوع رخداد (مانند تصادف، انسداد مسیر یا تغییر شرایط جوی)
- $m$  شناسه یکتای پیام که ترکیبی از نوع رخداد، موقعیت و زمان وقوع است

<sup>1</sup> Vehicles/Nodes

<sup>2</sup> Committee Groups

<sup>3</sup> Blockchain

اعتماد میان گره‌ها به دو عامل وابسته است:

- وزن داده<sup>۳</sup>: که بیان‌کننده اهمیت نوع پیام ارسالی است.
- زمان تعاملات<sup>۴</sup>: که نقش آن در به‌روزرسانی اعتماد پررنگ‌تر است؛ زیرا تعاملات جدیدتر وزن بیشتری نسبت به تعاملات قدیمی دارند.

در شبکه‌های بین خودرویی، داده‌ها به سه دسته کلی تقسیم می‌شوند:

- داده‌های تفریحی: مانند پیام‌های تبلیغاتی یا اطلاع‌رسانی عمومی.
- داده‌های کاربردی: شامل هشدارهای ترافیکی و وضعیت جاده.
- داده‌های امنیتی: مربوط به هشدار تصادف و شرایط بحرانی.

هر دسته، وزن مخصوصی دارد که نشان‌دهنده اهمیت پیام در محاسبه اعتماد است. داده‌های امنیتی بالاترین وزن را دارند و داده‌های تفریحی کمترین وزن را دارند. این وزن‌دهی در محاسبه اعتماد مستقیم و غیرمستقیم بین گره‌ها استفاده می‌شود. مقادیر پیش‌فرض این وزن‌ها در شکل (۵) نشان داده شده‌است.



(شکل-۵) مقدار پیش‌فرض وزن بسته‌های داده در طرح

پیشنهادی

(Figure -5): Default value of data packet weight in the proposed scheme

از آنجا که تعاملات جدیدتر باید اثر بیشتری در اعتماد کلی داشته باشند، از ضریب تضعیف زمانی  $\rho$  استفاده می‌شود. این ضریب به‌صورت نمایی کاهش می‌یابد تا تأثیر تعاملات قدیمی‌تر کم‌تر شود. مقدار وزن تعامل  $k$ ام از معادل  $Z$  (۴) محاسبه می‌شود:

$$f_k = \rho^{n-k} \quad 0 < \rho < 1, 1 \leq k \leq n \quad (4)$$

در رابطه بالا مقدار  $n$  تعداد تعاملات بین دو گره،  $k$  تعامل جاری و  $\rho$  با مقدار بین صفر و یک ضریب تضعیف را نشان می‌دهد.

#### الف) محاسبه اعتماد مستقیم

اعتماد مستقیم بین دو گره  $a$  و  $b$  با توجه به وزن داده و زمان تعاملات از معادله (۵) محاسبه می‌شود:

$$DT(a, b) = \frac{\sum_{k=1}^n \text{Flag}(k)(f_k + w_d)}{\sum_{k=1}^n (f_k + w_d)} \quad (5)$$

<sup>3</sup> Data Weight

<sup>4</sup> Interaction Time

همان‌گونه که در شکل مشخص است، در نواحی نزدیک به محل حادثه (پیش از نقطه عطف  $g$ ) میزان اعتماد به‌طور تقریبی ثابت و بالا باقی می‌ماند، اما با افزایش فاصله و عبور از نقطه عطف، اعتماد به‌صورت نمایی کاهش می‌یابد. این رفتار در معادله (۳) تابع استاندارد سیگموئید نشان داده شده‌است:

$$C_s = \frac{1}{1+e^{-t}} \quad (3)$$

که در آن  $t$  مؤلفه نرمال‌شده است که بیان‌کننده فاصله نسبی و شدت تغییرات اعتماد نسبت به مرکز حادثه است؛ به‌منظور شفاف‌سازی ساختار داده‌ها در فرآیند امتیازدهی، جدول (۲) جزئیات هر زمینه موجود در پیام را نشان می‌دهد.

(جدول ۲-۲) اطلاعات داده‌ها در طرح پیشنهادی

(table-2): Data information in the proposed plan

| اطلاعات | توضیحات                   |
|---------|---------------------------|
| $v_s$   | شناسه فرستنده پیام        |
| LL      | طول و عرض جغرافیایی حادثه |
| $e$     | نوع رخداد                 |
| $m$     | اطلاعات پیام              |

این مرحله از سامانه، مبنای اصلی فرآیند مدیریت اعتماد در طرح پیشنهادی است؛ زیرا با استفاده از فاصله مکانی و ویژگی‌های پیام، اعتبار اولیه پیام‌ها محاسبه و سپس برای تحلیل‌های بعدی به RSU ارسال می‌شود. در گام بعد، RSU‌ها بر اساس مقادیر  $C_s$  جمع‌آوری‌شده از وسایل نقلیه، میانگین اعتماد هر گره را محاسبه و برای ذخیره‌سازی در زنجیره قلابی آماده می‌سازند.

#### ۴-۲- محاسبه اعتماد کل

همان‌گونه که در بخش پیشین بیان شد، هر گره دریافت‌کننده برای ارزیابی اعتبار پیام، از نزدیک‌ترین RSU میزان اعتماد به فرستنده را درخواست می‌کند؛ بنابراین، یکی از مؤلفه‌های اصلی در مدل پیشنهادی، میزان اعتماد گره‌هاست که با نماد  $T$  نمایش داده می‌شود. محاسبه اعتماد در این پژوهش بر اساس دو نوع تعامل انجام می‌گیرد:

۱. اعتماد مستقیم<sup>۱</sup>: زمانی که دو گره پیش‌تر با یکدیگر تعامل داشته‌اند،

۲. اعتماد غیرمستقیم<sup>۲</sup>: زمانی که بین دو گره تعامل مستقیمی وجود ندارد و اعتماد از طریق گره‌های واسط تخمین زده می‌شود.

<sup>1</sup>Direct Trust

<sup>2</sup>UnDirect Trust

که در آن:

- $w_d$ : وزن نوع داده بر اساس شکل (۵)
- $f_k$ : وزن تعامل  $k$  بر اساس زمان
- $Flag(k)$ : نشان دهنده نوع رفتار گره  $b$  در تعامل  $k$  است؛ به طوری که:
- در رفتار نرمال،  $Flag(k)=1$
- در رفتار مخرب یا غیر قابل اعتماد،  $Flag(k)=0$

به این ترتیب، اعتماد مستقیم در واقع میانگین وزنی از تعاملات موفق گذشته است.

### ب) محاسبه اعتماد غیرمستقیم

در صورتی که دو گره تاکنون تعاملی نداشته باشند، اعتماد میان آن‌ها با استفاده از توصیه‌ها و مشاهدات گره‌های میانی (همسایه‌های مشترک) محاسبه می‌شود. اعتماد غیرمستقیم از معادله (۶) به دست می‌آید:

$$UDT(a, b) = \frac{\sum_{i=1}^n DT(a, N_i)(N_i, b)}{\sum_{i=1}^n DT(a, N_i)} \quad N_i \neq b \quad (6)$$

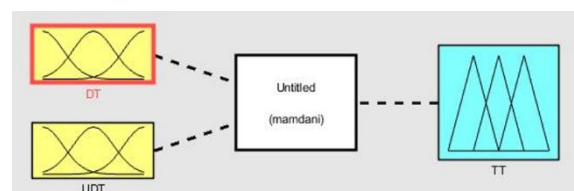
در این رابطه  $N_i$  نشان دهنده آمین همسایه گره  $a$  است که همسایه مشترک بین دو گره  $a$  و  $b$  نیز است؛ در نتیجه، اعتماد غیرمستقیم در واقع میانگین وزنی اعتمادهای منتقل شده از گره‌های واسط معتبر است.

### ج) ترکیب اعتماد مستقیم و غیرمستقیم با سامانه فازی:

باتوجه به اینکه مقدار اعتماد همواره مقداری بین صفر و یک دارد و دارای ابهام است، برای ترکیب و تفسیر بهتر دو مقدار  $UDT$  و  $DT$  از سامانه استنتاج فازی ممدانی<sup>۱</sup> استفاده شده است. این سامانه شامل سه مرحله اصلی است:

### • فازی سازی<sup>۲</sup>

ورودی‌ها شامل اعتماد مستقیم و غیرمستقیم هستند. هر ورودی با سه سطح زبانی کم، متوسط، زیاد تعریف می‌شود. تابع عضویت هر سطح با استفاده از داده‌های شبیه سازی شده در محیط MATLAB تعیین شده است. شکل (۶) فرآیند فازی سازی را نمایش می‌دهد.



(شکل-۶): فرایند فازی سازی رسم شده در برنامه متلب برای طرح پیشنهادی

(Figure-6): Fuzzification process in the proposed design

<sup>1</sup> Mamdani Fuzzy Inference System

<sup>2</sup> Fuzzification

- اعمال قوانین فازی<sup>۳</sup>: قوانین تصمیم گیری سامانه به صورت اگر/آن گاه طراحی شده اند. به طور کلی، دوازده قانون اصلی در جدول (۳) نمایش داده شده اند که بر مبنای میانگین اعتماد مستقیم و غیرمستقیم مقدار نهایی اعتماد تعیین می‌شود.

(جدول ۳-۳) اطلاعات داده ها در طرح پیشنهادی  
(Table-3): Data information in the proposed plan

| قانون | اعتماد مستقیم                                         | اعتماد غیرمستقیم            | اعتماد نهایی |
|-------|-------------------------------------------------------|-----------------------------|--------------|
| ۱     | کمتر از $\frac{Avg DT}{2}$                            | کمتر از $\frac{Avg UDT}{2}$ | خیلی کم      |
| ۲     | کمتر از $\frac{Avg DT}{2}$                            | کمتر از Avg UDT             | کم           |
| ۳     | کمتر از $\frac{Avg DT}{2}$                            | بیشتر از Avg UDT            | کم           |
| ۴     | کمتر از Avg DT                                        | کمتر از $\frac{Avg UDT}{2}$ | کم           |
| ۵     | کمتر از Avg DT                                        | کمتر از Avg UDT             | متوسط        |
| ۶     | کمتر از Avg DT                                        | بیشتر از Avg UDT            | متوسط        |
| ۷     | بیشتر از Avg DT و کمتر از $3 \times \frac{Avg DT}{2}$ | کمتر از $\frac{Avg UDT}{2}$ | متوسط        |
| ۸     | بیشتر از Avg DT و کمتر از $3 \times \frac{Avg DT}{2}$ | کمتر از Avg UDT             | زیاد         |
| ۹     | بیشتر از Avg DT و کمتر از $3 \times \frac{Avg DT}{2}$ | بیشتر از Avg UDT            | زیاد         |
| ۱۰    | بیشتر از $3 \times \frac{Avg DT}{2}$                  | کمتر از $\frac{Avg UDT}{2}$ | زیاد         |
| ۱۱    | بیشتر از $3 \times \frac{Avg DT}{2}$                  | کمتر از Avg UDT             | خیلی زیاد    |
| ۱۲    | بیشتر از $3 \times \frac{Avg DT}{2}$                  | بیشتر از Avg UDT            | خیلی زیاد    |

- دفازی سازی<sup>۴</sup>: پس از اعمال قوانین، برای به دست آوردن یک مقدار عددی از اعتماد نهایی، از روش مرکز ثقل<sup>۵</sup> استفاده شده است. تابع فازی سازی در معادله (۷) تعریف شده است:

$$T = \frac{\sum_{i=1}^n x_i \mu(x_i)}{\sum_{i=1}^n \mu(x_i)} \quad (7)$$

در رابطه بالا  $x_i$  نشان دهنده متغیر فازی و  $\mu(x_i)$  تابع عضویت متناظر با آن است. این روش باعث می‌شود مقدار نهایی اعتماد  $T$  به صورت نرم و پیوسته بین صفر و یک تغییر کند. از آنجا که احتمال نفوذ یا حمله به RSU ها وجود دارد، مقادیر اعتماد محاسبه شده تنها در یک RSU ذخیره نمی‌شوند. در ساختار پیشنهادی، هر مقدار اعتماد در چند RSU هم جوار نیز ثبت می‌شود تا در صورت

<sup>3</sup> Rule Evaluation

<sup>4</sup> Defuzzification

<sup>5</sup> Centroid

خراب‌کاری یا حمله به یکی از RSUها، داده‌های اعتماد معتبر باقی بمانند و فرآیند تصمیم‌گیری دچار اختلال نشود.

### ۴-۳- ایجاد گروه‌های ارزیاب (کمیته‌ها) به‌وسیله RSU

در این مرحله، هر ایستگاه کنار جاده به‌صورت محلی شناسه مخصوص به‌خود را ایجاد می‌کند. این شناسه از ترکیب آدرس IP و یک کلید خارجی به‌دست آمده و در فرآیند احراز هویت مبتنی بر ساختار Chord مورد استفاده قرار می‌گیرد. ساختار Chord به‌عنوان یکی از روش‌های جداسازی و توزیع مسئولیت در شبکه‌های همتا به‌همتا<sup>۱</sup>، امکان تقسیم وظایف و ایجاد امنیت بالا در سطح غیرمتمرکز را فراهم می‌سازد.

در فرآیند تشکیل گروه‌ها، از یک الگوریتم تکه‌بندی یا تقسیم‌بندی تصادفی استفاده می‌شود. در ابتدای هر مرحله، تابع درهم‌سازی<sup>۲</sup> مقدار تصادفی اولیه را برابر با ۳۲ بایت صفر در نظر می‌گیرد. استفاده از این مقدار تصادفی باعث می‌شود معادله غیرقابل پیش‌بینی باشد و بدین ترتیب از بروز حملات Sybil در شبکه جلوگیری می‌شود. تابع درهم‌سازی فرآیندی یک‌طرفه است که داده‌های ورودی با هر اندازه را به یک رشته خروجی با اندازه ثابت تبدیل می‌کند. مقدار خروجی حاصل از تابع درهم‌سازی را مقدار هش می‌نامند که امکان بازگرداندن آن به داده اولیه وجود ندارد. هدف از استفاده از الگوریتم‌های درهم‌سازی، افزایش امنیت داده‌ها، اطمینان از صحت انتقال اطلاعات و تسریع فرآیند جست‌وجو در پایگاه‌های داده توزیع شده‌است. الگوریتم‌های MD5 و SHA از جمله متداول‌ترین توابع درهم‌سازی در این زمینه‌اند. این فرآیند در رابطه (۸) نمایش داده شده‌است:

$$f(x) = y \quad (8)$$

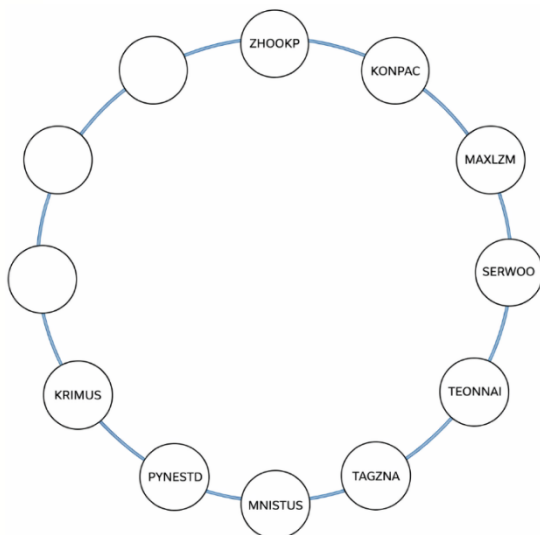
که در آن  $x$  داده ورودی و  $y$  مقدار هش حاصل از آن است. در طرح پیشنهادی، خروجی حاصل از درهم‌سازی بر روی ساختار Chord نگاشت می‌شود؛ در این ساختار، هر RSU به یک انبار<sup>۳</sup> در شبکه تخصیص می‌یابد. این انبارها به‌عنوان محل اجرای عملیات رمزگذاری، رمزگشایی و ذخیره کلیدهای رمز مورد استفاده قرار می‌گیرند؛ درواقع، کمیته‌ها به‌منزله همین انبارها هستند

<sup>۱</sup> P2P

<sup>۲</sup> Hash Function

<sup>۳</sup> Repository

و اعضای آن‌ها همان RSUهای موجود در شبکه هستند. فرآیند تشکیل کمیته‌ها نیز با تکیه بر تابع درهم‌سازی یک‌نواخت<sup>۴</sup> انجام می‌گیرد. این ساختار به‌صورت عمومی و توزیع شده در اختیار تمام نهادهای شبکه قرار دارد تا از تمرکزگرایی جلوگیری شده و نقطه آسیب‌پذیر واحدی در شبکه وجود نداشته باشد. شکل (۷) ساختار Chord و نحوه ذخیره کلیدهای رمز در انبارها را نشان می‌دهد که هر RSU یک شناسه محلی منحصر به فرد از طریق IP و کلید خارجی اختصاصی دریافت می‌کند. این شناسه‌ها و کلیدها در ساختار Chord نگهداری می‌شوند تا فرآیند احراز هویت و اجماع توزیع شده تسهیل شود. Chord امکان نگاشت شناسه‌ها به RSUهای مسئول ذخیره‌سازی را فراهم و نقاط آسیب‌پذیر متمرکز را حذف می‌کند. نقش این ساختار، تضمین امنیت اطلاعات و جلوگیری از حملات Sybil و دست‌کاری داده‌ها است.



(شکل-۷) انبارهای روی ساختار Chord برای نگهداری کلیدهای رمز

(Figure-7): Storage on the Chord structure for storing encryption keys

با استفاده از ساختار Chord، RSUها قادر خواهند بود صحت و اصالت اطلاعات ثبت شده در بستر زنجیره قالبی را تأیید کنند. این کار از طریق سازوکار رمزگذاری و رمزگشایی مبتنی بر احراز هویت توزیع شده انجام می‌شود. به کمک این ساختار، هر RSU می‌تواند از معتبر بودن فرستنده یا گیرنده پیام اطمینان حاصل کرده و در صورت نیاز با مراجعه به سوابق تراکنش‌های گذشته، تصمیم‌گیری دقیق‌تری درخصوص صحت داده انجام دهد.

طرح پیشنهادی از الگوی Chord توزیع شده بهره می‌برد؛ به این معنا که برای هر RSU یک زیرساخت Chord اختصاصی در نظر گرفته می‌شود. هدف از این

<sup>۴</sup> Consistent Hashing

طراحی، کاهش احتمال سازش<sup>1</sup> در فرآیند اجماع و کاستن از پیچیدگی محاسباتی است. این ساختار می‌تواند به صورت لایه‌ای بالاتر از سامانه متمرکز عمل کرده و در بازه‌های زمانی منظم (روزانه، هفتگی یا ماهانه) برای افزایش امنیت شبکه به‌روزرسانی شود.



(شکل-۸): فرآیند احراز هویت در ساختار Chord  
(Figure-8): Authentication process in chord structure

پس از تولید شناسهٔ رخ داده‌ها در زنجیرهٔ قالبی، انبارها تعریف و جداول انگشتی<sup>۲</sup> مقداردهی اولیه می‌شوند؛ سپس شناسهٔ رخداد در ساختار Chord نگاشت یافته و فرآیند احراز هویت انجام می‌شود. در این ساختار، شناسه‌ها به صورت مدور و بر مبنای پیمانهٔ  $2^m$  مرتب‌سازی شده و

<sup>1</sup> Collusion  
<sup>2</sup> Finger Tables

هر گره محدودهٔ خاصی از فضای شناسه‌ها را اشغال می‌کند. شکل (۸) نحوهٔ احراز هویت در ساختار Chord را نمایش می‌دهد، که در آن رخ داده‌ها به شناسه تبدیل شده و در ساختار Chord نگاشت می‌شوند. RSUهای مسئول با استفاده از شناسه‌های نگه‌داری شده و کلیدهای رمز، صحت تراکنش‌ها را تأیید می‌کنند. گروه‌های ارزیاب، تراکنش‌ها را بررسی و در صورت صحت، آن‌ها را به زنجیرهٔ قالبی ارسال می‌کنند. این فرآیند، پاسخ RSUها را در جریان اجماع مخفی نگه می‌دارد و از سازش در شبکه جلوگیری می‌کند.

در ادامه، پالایه‌های ذخیره‌سازی بر اساس داده‌های درهم‌سازی شده در ساختار قرار می‌گیرند. سامانه Chord قادر است عملیات درج، حذف، جست‌وجو و به‌روزرسانی زوج‌های کلید-مقدار<sup>۳</sup> را به صورت توزیع شده و کارآمد انجام دهد. این ساختار از درهم‌سازی یک‌نواخت برای تخصیص کلیدها به گره‌های RSU استفاده می‌کند. در صورت بروز خرابی در یکی از گره‌ها، داده‌های آن به صورت خودکار به گره پیشین منتقل می‌شود.

به منظور افزایش قابلیت اطمینان، در طرح پیشنهادی برای ساختار Chord یک نسخهٔ پشتیبان<sup>۴</sup> نیز در نظر گرفته شده است. نسخهٔ پشتیبان به صورت پیش‌فرض پس از گذشت تعداد معینی از چرخه‌های شبکهٔ دور به‌روزرسانی می‌شود و در صورت بروز اشکال در ساختار اصلی، کنترل شبکه به نسخهٔ پشتیبان منتقل خواهد شد؛ در نهایت، پس از احراز هویت RSUها و تعیین شناسه‌ها، این گره‌ها بر اساس مجاورت جغرافیایی و فاصلهٔ فیزیکی اقدام به تشکیل گروه یا کمیته‌های ارزیاب<sup>۵</sup> می‌کنند. شاخص تعیین‌کننده در این فرآیند، فاصلهٔ میان RSUها است؛ به طوری که اگر فاصلهٔ بین دو RSU از مقدار آستانهٔ مشخصی کمتر باشد، در یک خوشه<sup>۶</sup> قرار گرفته و به عنوان اعضای یک کمیته شناخته می‌شوند. این کمیته‌ها وظیفهٔ بررسی و تأیید صحت رخ داده‌ها را برعهده دارند. تنها RSUهایی که فاصلهٔ آن‌ها از مقدار آستانه کمتر است، مجاز به شرکت در تشکیل کمیته و تأیید نهایی رویدادها خواهند بود.

#### ۴-۴-۴ اعتبارسنجی

پس از ارسال تراکنش‌ها به کمیتهٔ ارزیابی، فرآیند اعتبارسنجی تراکنش‌ها آغاز می‌شود. در این مرحله، گره دریافت‌کنندهٔ تراکنش، آن را برای بررسی و ارزیابی به اعضای

<sup>3</sup> key-value pairs

<sup>4</sup> Backup Chord

<sup>5</sup> Evaluator Committees

<sup>6</sup> Cluster

MATLAB R2023b پیاده‌سازی و شبیه‌سازی شده‌است. این محیط به‌دلیل دارا بودن کتابخانه‌های قدرتمند برای تحلیل داده، مدل‌سازی سامانه‌های هوشمند و پیاده‌سازی الگوریتم‌های فازی و ریاضی، گزینه‌ای مناسب برای انجام این پژوهش محسوب می‌شود.

در این بخش، به‌منظور بررسی کارایی روش پیشنهادی، یک شبکه بین‌خودرویی در ابعاد مشخص طراحی شده‌است. در این شبکه، تعداد RSUها ثابت و به‌صورت تصادفی در نواحی مختلف محیط توزیع شده‌اند. وسایل نقلیه (گره‌ها) نیز به‌صورت تصادفی در محدوده شبکه قرار گرفته و با سرعت‌های متغیر شروع به حرکت می‌کنند. رخ داده‌هایی همچون خرابی جاده، ازدحام ترافیکی و وقوع تصادف نیز به‌طور تصادفی در محیط رخ می‌دهند تا سناریوهای مختلف شبکه مورد آزمون قرار گیرد.

هر گره با مشاهده رخ دادی در محدوده خود، یک پیام همه‌پخش<sup>۵</sup> برای سایر وسایل نقلیه مجاور ارسال می‌کند. پیام‌های دریافتی بر اساس الگوریتم امتیازدهی و سامانه فازی اعتمادسنجی (مطابق بخش‌های ۴-۱ و ۴-۲)، تحلیل شده و نتیجه نهایی برای تصمیم‌گیری در سطح RSUها ذخیره می‌شود.

رویکرد پیشنهادی در فاز پیاده‌سازی شامل مجموعه‌ای از مؤلفه‌های کلیدی است که مقاردهی صحیح آن‌ها برای تکرارپذیری نتایج ضروری است. جدول (۴) مؤلفه‌های اصلی شبیه‌سازی را نشان می‌دهد.

(جدول ۴) مؤلفه‌های شبیه‌سازی

(Table-4): Simulation parameters

| مؤلفه             | مقدار     | توضیحات                            |
|-------------------|-----------|------------------------------------|
| زمان شبیه‌سازی    | ۳۰۰ دور   | تعداد چرخه‌های زمانی اجرای مدل     |
| تعداد RSU         | ۲۰        | واحدهای کنار جاده‌ای ثابت در محیط  |
| تعداد گره‌ها      | ۱۰۰۰      | گره‌های متحرک در شبکه بین‌خودرویی  |
| ابعاد محیط        | ۱۰۰۰×۱۰۰۰ | ناحیه فیزیکی شبیه‌سازی             |
| توان ارسال سیگنال | ۲۰۰ متر   | محدوده ارتباطی هر وسیله نقلیه      |
| تعداد رخ داده‌ها  | ۱۰۰       | شامل خرابی، تصادف و ازدحام ترافیکی |

<sup>۵</sup> Broadcast Message

گروه ارزیاب ارسال می‌کند. هر RSU که پیام تراکنش را دریافت کند، یک پیام تأیید به سایر اعضای گروه ارسال کرده و در انتظار دریافت تأیید از سوی آن‌ها باقی می‌ماند. پس از آن که تعداد کافی از اعضای کمیته پیام‌های تأیید را ارسال کردند، تراکنش مورد نظر به‌عنوان تراکنش معتبر<sup>۱</sup> شناخته می‌شود. در ادامه، کمیته ارزیابی تراکنش را برای گروه نهایی<sup>۲</sup> ارسال می‌کند. وظیفه گروه نهایی، بررسی صحت امضاهای رقمی اعضای کمیته ارزیاب و اطمینان از اصالت فرایند اجماع است. پس از تأیید نهایی، تراکنش در قالب یک بلوک جدید به زنجیره قالی شبکه بین‌خودرویی افزوده می‌شود.

فرآیند بالا اطمینان می‌دهد که هر تراکنش پیش از ثبت در زنجیره قالی، چندین مرحله بررسی و اعتبارسنجی را پشت سر گذاشته و در برابر حملات جعل، دست‌کاری داده یا ارسال اطلاعات مخرب مقاوم باشد.

اعتبارسنجی تراکنش‌ها، نقش تعیین‌کننده‌ای در مشخص کردن وضعیت رخ داده‌های ثبت‌شده در شبکه دارد. این وضعیت می‌تواند یکی از دو حالت زیر را نشان دهد:

۱. وضعیت پایشی<sup>۳</sup>: در این حالت، تراکنش‌های ثبت‌شده نشان‌دهنده رخ داده‌های واقعی و معتبر در شبکه هستند، مانند گزارش وقوع تصادف، اعلام خرابی مسیر یا ثبت تراکم ترافیک.

۲. وضعیت معیوب یا مخرب<sup>۴</sup>: در این حالت، تراکنش شامل داده‌های اشتباه، غیرواقعی یا حاصل رفتارهای بدخواهانه از سوی گره‌های مخرب است. چنین داده‌هایی با توجه به سامانه امتیازدهی و اعتماد پیشین (بخش ۴-۱ و ۴-۲)، شناسایی شده و از ورود به زنجیره قالی جلوگیری می‌شود؛ در نتیجه، فرآیند اعتبارسنجی در طرح پیشنهادی علاوه بر تضمین صحت و اصالت تراکنش‌ها، باعث افزایش اعتماد میان RSUها و بهبود کیفیت تصمیم‌گیری در سطح شبکه بین‌خودرویی می‌شود؛ بدین ترتیب، تنها داده‌های معتبر و دارای پشتوانه محاسباتی و فازی، اجازه ثبت در دفترکل توزیع‌شده (زنجیره قالی) را خواهند داشت.

## ۴-۵- پیاده‌سازی مدل

ره‌یافت پیشنهادی این پژوهش به‌منظور ارزیابی عملکرد و تحلیل رفتار سامانه مدیریت اعتماد مبتنی بر زنجیره قالی در شبکه‌های بین‌خودرویی، در محیط برنامه‌نویسی

<sup>۱</sup> Valid Transaction

<sup>۲</sup> Final Committee

<sup>۳</sup> Monitoring State

<sup>۴</sup> Faulty State

- در رخ داده‌های مختلف، سطح اعتماد به RSUها در طرح پیشنهادی و طرح پایه چه تفاوتی دارد؟
- میزان قابلیت اطمینان کمیته‌های ارزیاب مبتنی بر زنجیره‌ی قالبی در هر دو مدل چگونه است؟
- افزایش تعداد رخ داده‌ها چه تأثیری بر میزان اعتماد و عملکرد سامانه دارد؟
- پیچیدگی محاسباتی طرح پیشنهادی نسبت به طرح پایه در چه سطحی قرار دارد؟

## ۵-۱- معرفی طرح پایه<sup>۲</sup>

طرح پایه مورد استفاده برای مقایسه، مدل SBTMS ارائه شده توسط قاجار و همکاران (۲۰۲۱) است [۱۹]. در این مدل، با استفاده از فناوری زنجیره‌ی قالبی، یک معماری غیرمتمرکز برای مدیریت اعتماد در شبکه‌های بین خودرویی ارائه شده است.

در این رویکرد، هر وسیله نقلیه با تکیه بر رابطه‌ی بیز<sup>۳</sup>، اعتبار پیام‌های دریافتی را محاسبه و نتایج را به نزدیک‌ترین RSU ارسال می‌کند. RSUها پس از جمع‌آوری داده‌های اعتماد از وسایل نقلیه، با استفاده از سازوکار اجماع، مقدار اعتماد خالص<sup>۴</sup> را محاسبه و در زنجیره‌ی قالبی ذخیره می‌کنند.

این مدل توانسته است چالش متمرکز بودن شبکه‌ها و فقدان اعتماد متقابل بین واحدهای VANET را تا حدی برطرف کند؛ با این حال، از آنجا که در SBTMS سازوکار اجماع نیازمند هماهنگی گسترده بین تمام RSUهاست، پیچیدگی محاسباتی بالا و افزایش تأخیر در اعتبارسنجی تراکنش‌ها از جمله نقاط ضعف آن محسوب می‌شود.

## ۵-۲- تحلیل عملکرد طرح پیشنهادی در

### مقایسه با مدل پایه

در طرح پیشنهادی، برخلاف مدل SBTMS، فرآیند محاسبه و مدیریت اعتماد از طریق ترکیب محاسبات فازی، سامانه ارزیابی چندسطحی و ساختار Chord در RSUها انجام می‌شود. این ترکیب باعث شده است تا:

۱. محاسبه اعتماد برای پیام‌ها دقیق‌تر و پویاتر انجام گیرد.
۲. بار محاسباتی شبکه به صورت توزیع شده میان RSUها تقسیم شود.
۳. فرآیند اجماع و اعتبارسنجی تراکنش‌ها با سرعت بیشتری انجام پذیرد.
۴. امکان تشکیل کمیته‌های محلی برای ارزیابی تراکنش‌ها فراهم شود که این امر از ایجاد گلوگاه<sup>۵</sup> در شبکه جلوگیری می‌کند.

<sup>2</sup> SBTMS

<sup>3</sup> Bayesian Trust Model

<sup>4</sup> Net Trust

<sup>5</sup> Bottleneck

برای اجرای شبیه‌سازی، الگوریتم پیشنهادی در قالب شبه‌کد<sup>۱</sup> زیر پیاده‌سازی شده است. این شبه‌کد شامل مراحل تولید گره‌ها، تولید رخ داده‌ها، ارسال پیام‌ها، محاسبه اعتماد، تشکیل گروه‌های ارزیاب و ثبت نتایج در زنجیره قالبی است.

(جدول ۵): شبه‌کد روش پیشنهادی

(table-5): Pseudo code of the proposed method

### Algorithm 1: Proposed SBTFC method

```

1: Define network parameters (Number of RSUs,
   Vehicles, Communication range)
2: Initialize Chord structure for key management
3: FOR each vehicle v in Vehicles:
4:   Sense events in local vicinity
5:   Set event priority (delay-sensitive or not)
6:   IF event is delay-sensitive:
7:     Process event at edge
8:   ELSE:
9:     Process event in cloud
10:  Broadcast event message with EventID and
   Timestamp
11:  IF message already broadcasted:
12:    Skip message distribution
13:  ELSE:
14:    Broadcast message to neighboring
   vehicles
15:  FOR each receiving vehicle r:
16:    Allocate points to message
17:    Request trust rate of sender from RSU
18:    Verify message content
19:    Send computed trust rate to RSU
20:  RSUs calculate vehicle trust
21:  RSUs form assessment groups
22:  Evaluator groups perform consensus on
   messages
23:  Final confirmation of message in network
24:  Register vehicle trust and confirmed
   transactions in blockchain using Chord
25:  Send confirmed message to vehicles within
   communication radius
26: END FOR

```

## ۵- تجزیه و تحلیل

در این بخش، عملکرد روش پیشنهادی در مقایسه با طرح پایه مورد بررسی و تحلیل قرار گرفته است؛ هدف از این تحلیل، ارزیابی میزان بهبود اعتماد، قابلیت اطمینان و کارایی محاسباتی در طرح پیشنهادی نسبت به روش‌های موجود است.

به منظور انجام این تحلیل، تلاش شده است به پرسش‌های کلیدی زیر پاسخ داده شود:

<sup>1</sup> Pseudocode

و پایداری بیشتری نسبت به مدل پایه SBTMS برخوردار است؛ در حالی‌که مدل پایه در مقیاس‌های بزرگ دچار افزایش تأخیر و سربار محاسباتی می‌شود، مدل پیشنهادی با تقسیم وظایف بین RSU ها، نه تنها بار شبکه را کاهش می‌دهد، بلکه باعث افزایش دقت و سرعت در اعتبارسنجی داده‌ها می‌شود.

به اختصار می‌توان بیان کرد که سامانه مدیریت اعتماد پیشنهادی در مقایسه با طرح پایه:

- اعتمادپذیری شبکه را افزایش داده،
- تأخیر و پیچیدگی محاسباتی را کاهش داده،
- و در برابر گره‌های مخرب و حملات داده‌های جعلی مقاوم‌تر عمل کرده‌است.

تحلیل‌های انجام‌شده نشان‌دهنده برتری طرح پیشنهادی در شاخص‌های اصلی اعتماد، کارایی و امنیت نسبت به مدل پایه است. در بخش بعدی (نتایج و نمودارها)، به صورت کمی و تصویری، میزان این بهبود برای مؤلفه‌های مختلف ارائه می‌شود.

## ۶- شبیه‌سازی و تحلیل نمودارها

### ۶-۱- نرخ اعتماد

همان‌طور که در بخش‌های پیشین توضیح داده شد، RSU ها نقش اصلی در محاسبه و مدیریت میزان اعتماد در شبکه را برعهده دارند؛ پس از دریافت تراکنش‌ها از گره‌ها، هر RSU با استفاده از روابط تعریف‌شده در مدل پیشنهادی، اعتماد مستقیم را نسبت به گره‌های فرستنده محاسبه کرده و نتیجه را در بلاک ثبت می‌کند.

در مدل پیشنهادی، فرآیند ثبت این محاسبات در بلاک‌ها به گونه‌ای انجام می‌شود که هر RSU تنها پس از تأیید کمیته ارزیاب قادر به افزودن بلاک جدید به زنجیره خواهد بود. این سازوکار باعث جلوگیری از ورود مقادیر جعلی به شبکه می‌شود. یانگ و همکاران [۲۶] در پژوهش خود، مدلی به نام POW<sup>۹</sup> را پیشنهاد کردند که در آن، هر RSU پس از محاسبه میزان اعتماد، بلاکی جدید برای ذخیره محاسبات خود ایجاد می‌کند. این طرح به عنوان مدل پایه دوم در این مقاله مورد استفاده قرار گرفته‌است؛ باوجود نوآوری در مدل POW، ضعف اصلی آن، اتکای زیاد به صداقت RSU ها است. در این طرح، هر RSU می‌تواند برای افزایش تعداد بلاک‌های ثبت‌شده در زنجیره، مقادیر جعلی اعتماد را وارد کند؛ زیرا سایر گره‌ها به محتوای تراکنش‌ها دسترسی مستقیم ندارند.

مقاله پایه [۱۷] با استفاده از الگوریتم تکه‌بندی و انتشار همگانی پیام‌ها، تا حد زیادی این مشکل را برطرف کرده‌است؛ زیرا در این روش، تشکیل هر بلاک منوط به تأیید یک کمیته

<sup>۹</sup> Proof of Work

در این رویکرد، هر گره پس از دریافت پیام، با استفاده از معادله‌های (۱) و (۲) میزان اعتماد به پیام دریافتی را محاسبه و سپس باتوجه به معادله (۴) و (۵) مبتنی بر منطق فازی، اعتماد به فرستنده پیام را تعیین و درنهایت، گره میزان اعتماد خود را برای RSU ارسال می‌کند تا فرآیند اجماع محلی در سطح RSU و گروه‌های ارزیاب انجام گیرد.

بدین ترتیب، طرح پیشنهادی در مقایسه با مدل پایه، ضمن حفظ دقت در محاسبات اعتماد، توانسته است:

- تأخیر محاسباتی<sup>۱</sup> را کاهش دهد،
- قابلیت اطمینان به داده‌ها<sup>۲</sup> را افزایش دهد،
- و قابلیت مقیاس‌پذیری<sup>۳</sup> شبکه را بهبود بخشد.

## ۵-۳- مؤلفه‌های ارزیابی و شاخص‌های مقایسه

برای تحلیل عملکرد دو مدل، شاخص‌های زیر مورد ارزیابی قرار گرفته‌اند:

(جدول ۶- مؤلفه‌های ارزیابی و شاخص‌های مقایسه)

(Table-6): Evaluation parameters and comparison indicators

| شاخص ارزیابی                    | توضیحات                                                        | انتظار در مدل پیشنهادی  |
|---------------------------------|----------------------------------------------------------------|-------------------------|
| میانگین سطح اعتماد <sup>۴</sup> | میانگین مقدار اعتماد محاسبه‌شده به وسیله گره‌ها نسبت به RSU ها | افزایش نسبت به مدل پایه |
| نرخ صحت پیام‌ها <sup>۵</sup>    | نسبت پیام‌های معتبر به کل پیام‌های ارسال‌شده در شبکه           | افزایش قابل توجه        |
| تأخیر محاسباتی <sup>۶</sup>     | مدت زمان بین دریافت پیام تا ثبت در زنجیره قابل‌بای‌پهره‌گیری   | کاهش محسوس              |
| پیچیدگی محاسباتی <sup>۷</sup>   | تعداد عملیات محاسباتی برای هر بلوک تراکنش                      | کمتر از مدل پایه        |
| پایداری شبکه <sup>۸</sup>       | مقاومت سامانه در برابر گره‌های مخرب و داده‌های پرت             | افزایش چشم‌گیر          |

## ۴-۵- جمع‌بندی تحلیلی

نتایج تحلیل‌ها نشان می‌دهد که مدل پیشنهادی به واسطه استفاده از سامانه فازی برای تصمیم‌گیری تطبیقی و ساختار Chord برای توزیع فرآیند اجماع، از انعطاف‌پذیری

<sup>۱</sup> Computation Delay

<sup>۲</sup> Data Reliability

<sup>۳</sup> Scalability

<sup>۴</sup> Average Trust Level

<sup>۵</sup> Message Validity Rate

<sup>۶</sup> Processing Delay

<sup>۷</sup> Computational Complexity

<sup>۸</sup> Network Stability

از RSU ها است؛ با این حال، این روش نیز به دلیل افزایش پیچیدگی محاسباتی و نبود هماهنگی کامل بی RSU ها، در شرایط پرتراфик یا مقیاس بزرگ با چالش روبه‌رو می‌شود؛ در نتیجه، در این پژوهش، عملکرد سه مدل زیر در شاخص نرخ اعتماد مورد مقایسه قرار گرفته است:

• مدل POW [۷]

• مدل SBTMS [۱۹]

• مدل پیشنهادی SBTFC (سامانه فازی مبتنی بر زنجیره قالبی)

رابطه محاسبه نرخ اعتماد کلی در شبکه به صورت زیر تعریف می‌شود:

$$R = \sum_{i=1}^n UT_i \quad (10)$$

که در آن:

•  $UT$  مقدار اعتماد کل به گره نام است،

•  $N$  تعداد کل گره‌های موجود در شبکه است.

این شاخص، نشان‌دهنده میزان کلی اعتماد RSU ها به گره‌ها در هر مرحله از شبیه‌سازی است.

#### الف) رخ داده‌های تصادفات<sup>۱</sup>

در این آزمایش، عملکرد مدل‌ها در تشخیص رخ داده‌های مربوط به تصادفات جاده‌ای بررسی شده است. هر RSU، پس از مشاهده رخداد، قابلیت اطمینان داده‌های گزارش شده را ارزیابی کرده و نتیجه را در شبکه منتشر می‌کند.

نتایج شبیه‌سازی نشان می‌دهد که روش پیشنهادی، در مقایسه با مدل‌های پایه، نرخ خطای پایین‌تری در تشخیص رخ داده‌های تصادف دارد و میزان اعتماد به RSU ها در طول زمان به طور پیوسته افزایش می‌یابد. در فازهای ابتدایی شبیه‌سازی، میزان اعتماد در مدل پیشنهادی و مدل پایه به طور تقریبی مشابه است؛ اما از دور هشتم به بعد، به دلیل استفاده از سامانه استنتاج فازی، عملکرد مدل پیشنهادی به صورت قابل ملاحظه‌ای بهبود می‌یابد.

در این ساختار، هر وسیله نقلیه پس از دریافت پیام رخداد، میزان اعتماد به فرستنده را از RSU مربوطه درخواست کرده و با استفاده از آن، مقدار نهایی اعتماد خود را محاسبه و دوباره به RSU ارسال، سپس، RSU نتایج اعتماد را در شبکه به صورت همه‌پخشی میان سایر RSU ها منتشر می‌کند تا اطلاعات اعتماد در کل شبکه به روزرسانی شود. در نتیجه این همکاری میان اجزای شبکه، نرخ اعتماد با افزایش زمان و افزایش تعداد تعاملات میان گره‌ها، روندی صعودی پیدا می‌کند.

بر اساس نمودار (۱)، با گذشت زمان، مقدار نرخ اعتماد در مدل پیشنهادی پیوسته افزایش یافته و از حدود راند ۳۹ به بعد رشد محسوسی را نشان می‌دهد. در انتهای شبیه‌سازی (راند ۲۰۲)، نرخ اعتماد در مدل SBTFC به بیشینه مقدار خود یعنی ۱.۰ رسیده است.

در مقایسه با دو مدل پایه:

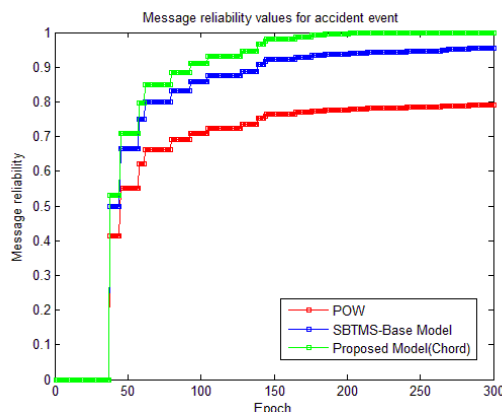
• نرخ اعتماد در مدل پیشنهادی نسبت به SBTMS حدود

چهار درصد بیشتر بوده است.

• و نسبت به مدل POW، ۲۱ درصد افزایش را نشان می‌دهد.

این نتایج نشان‌دهنده آن است که استفاده از کمیته‌های ارزیاب مبتنی بر Chord و استنتاج فازی پویا باعث افزایش پایداری و صحت در فرآیند تشخیص رخ داده‌ها و جلوگیری از ورود داده‌های جعلی شده است.

به اختصار، نرخ اعتماد بالاتر در مدل پیشنهادی نشان‌دهنده بهبود چشم‌گیر دقت در ارزیابی پیام‌های شبکه، کاهش داده‌های غیرقابل اعتماد و افزایش هماهنگی میان RSU ها در محیط‌های پویا و واقعی است. نمودار (۱) نتایج این بررسی را نشان می‌دهد.



(نمودار-۱): ارزیابی نرخ اعتماد به پایش رخ داده‌های تصادف  
(Chart-1): Assessing the confidence rate in accident event monitoring

#### ب) رخ داده‌های ترافیک<sup>۲</sup>

در این آزمایش، عملکرد مدل پیشنهادی در تشخیص و ارزیابی رخ داده‌های مربوط به ترافیک جاده‌ای مورد بررسی قرار گرفته است؛ هدف از این ارزیابی، مقایسه میزان اعتماد شبکه به گره‌های گزارش‌دهنده رخداد ترافیکی در مدل پیشنهادی و دو مدل پایه SBTMS و POW است.

در فرآیند شبیه‌سازی، هر RSU پس از دریافت داده‌های مربوط به تراکم ترافیک از وسایل نقلیه، آن‌ها را با داده‌های سایر RSU ها مقایسه کرده و با استفاده از سامانه استنتاج فازی، میزان اعتماد نهایی<sup>۳</sup> را برای هر رخداد محاسبه می‌کند؛ سپس، این اطلاعات از طریق

<sup>۲</sup> Traffic Events

<sup>۳</sup> Final Trust Rate

<sup>۱</sup> Accident Events

## ج) رخ داده‌های خرابی جاده<sup>۲</sup>

در این آزمایش، عملکرد مدل پیشنهادی در تشخیص و ارزیابی رخ داده‌های مرتبط با خرابی جاده‌ها مورد بررسی قرار گرفته‌است. هدف، سنجش توانایی مدل در تفکیک رخ داده‌های واقعی از داده‌های پرت یا خطاهای ناشی از حس‌گرها و وسایل نقلیه است. فرآیند شبیه‌سازی مشابه دو سناریوی پیشین (تصادف و ترافیک) انجام شده‌است؛ با این تفاوت که در این بخش نوع رخ داده‌ها شامل شکستگی سطح جاده، وجود چاله‌ها و ناهنجاری‌های مسیر بوده‌است که به‌وسیلهٔ وسایل نقلیه در حین عبور شناسایی و به RSUهای مجاور گزارش می‌شود.

هر RSU پس از دریافت پیام رخ داده، با استفاده از تابع اعتماد محلی (بر اساس روابط یک تا هفت) و سازوکار استنتاج فازی، میزان اعتماد به فرستنده و درستی داده را محاسبه می‌کند؛ سپس مقادیر نهایی به کمیتهٔ ارزیابی ارسال می‌شود تا در زنجیرهٔ قالبی ثبت شوند.

نتایج شبیه‌سازی نشان می‌دهد که مدل پیشنهادی در مقایسه با دو مدل پایهٔ SBTMS و POW توانایی بالاتری در شناسایی و تأیید رخ داده‌های خرابی جاده دارد. در سه راند ابتدایی شبیه‌سازی، تفاوت محسوسی میان مدل‌ها مشاهده نمی‌شود؛ اما از راندهای میانی به بعد، با افزایش تعاملات بین RSUها و وسایل نقلیه، دقت مدل پیشنهادی به‌شکل قابل توجهی افزایش می‌یابد.

در راند ۹۲ از اجرای شبیه‌سازی، مقدار قابلیت اطمینان مدل پیشنهادی به بیشینهٔ مقدار خود یعنی صد درصد می‌رسد؛ در حالی که در همین نقطه:

- قابلیت اطمینان مدل SBTMS برابر با ۹۵ درصد؛
- و مدل POW برابر با ۷۳ درصد است.

این تفاوت بیان‌کنندهٔ توانایی بالاتر مدل پیشنهادی در مدیریت داده‌های نوفه‌دار، حذف خطاهای ناشی از فاصلهٔ زیاد گره‌ها و مقابله با داده‌های جعلی است.

همانند دو سناریوی پیشین، روند تغییرات نرخ اعتماد در این آزمایش نیز صعودی است و با گذشت زمان، شبکه به یک وضعیت پایدار و هم‌گرا می‌رسد. پس از گذشت حدود راند سه، افزایش چشم‌گیری در نرخ اعتماد مشاهده می‌شود و از راند ۲۸۸ به بعد، هر سه مدل به حالت کمابیش پایدار دست می‌یابند. این رفتار نشان‌دهندهٔ خودتنظیمی و پایداری مدل پیشنهادی در برابر نوسانات ترافیکی و تغییرات محیطی است. درکل، استفاده از سامانه فازی، ساختار Chord و گروه‌های ارزیاب RSU موجب می‌شود که روش پیشنهادی در تشخیص رخ داده‌های خرابی جاده از

زنجیرهٔ قالبی میان سایر RSUها منتشر می‌شود تا در سطح شبکه، هماهنگی و سازگاری اطلاعات ایجاد شود.

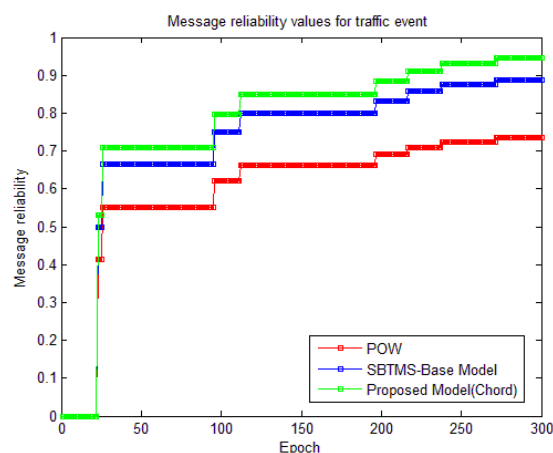
نتایج به‌دست‌آمده از اجرای شبیه‌سازی نشان می‌دهد که در رخ داده‌های ترافیکی نیز، نرخ اعتماد شبکه روندی صعودی و باثبات دارد. در مراحل ابتدایی شبیه‌سازی (تا حدود راند ۱۹)، اختلاف قابل توجهی میان روش‌ها مشاهده نمی‌شود و تمامی مدل‌ها در بازه‌ی مشابه از نظر اعتماد عمل می‌کنند؛ با این حال، از راندهای میانی به بعد، به‌ویژه با افزایش تراکم داده‌ها و تعاملات میان RSUها، مدل پیشنهادی به‌دلیل بهره‌گیری از سازوکار ارزیابی گروهی<sup>۱</sup> و منطق فازی پویا، توانایی بهتری در تشخیص رخ داده‌های واقعی از داده‌های پرت یا جعلی نشان می‌دهد.

در پایان فرآیند شبیه‌سازی، مقادیر کمی نرخ اعتماد به‌صورت زیر اندازه‌گیری شده‌است:

- مدل پیشنهادی (SBTFC) ۹۵ درصد
- مدل پایهٔ (SBTMS) ۸۹ درصد
- مدل پایهٔ (POW) ۷۴ درصد

افزایش شش درصدی نسبت به مدل SBTMS و ۲۱ درصدی نسبت به مدل POW، نشان‌دهندهٔ بهبود معنادار در پایداری اعتماد و دقت تشخیص رخ داده‌های ترافیکی در طرح پیشنهادی است.

این نتایج تأیید می‌کنند که در شرایطی که ترافیک جاده‌ای سنگین و پویا است، به‌کارگیری ترکیب سازوکار زنجیرهٔ قالبی غیرمتمرکز، سامانه فازی ممدانی و ساختار Chord در مدل پیشنهادی باعث می‌شود داده‌های مخرب یا نادرست با دقت بیشتری شناسایی و حذف شوند؛ در نتیجه، شبکه از نظر اعتمادپذیری، مقاومت در برابر داده‌های جعلی و هماهنگی بین RSUها، عملکردی پایدار و برتر دارد.

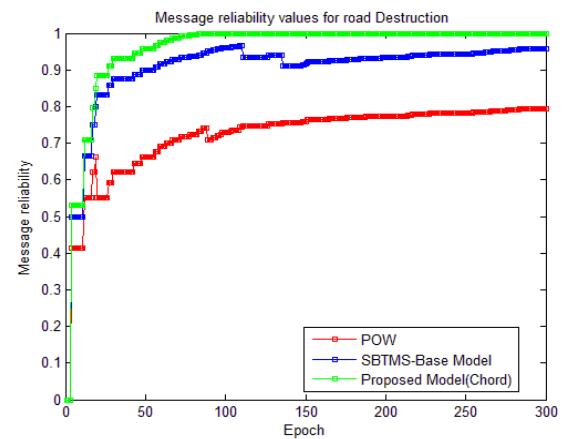


(نمودار - ۲): ارزیابی نرخ اعتماد به پایش رخ داده‌های ترافیک  
(Chart-2): Assessing the trust rate of traffic event monitoring

<sup>۱</sup> Committee-based Validation

<sup>۲</sup> Road Damage Events

دقت و اعتمادپذیری بالاتری نسبت به روش‌های پایه برخوردار باشد.



(نمودار-۳): ارزیابی نرخ اعتماد به پایش

رخ داده‌های خرابی جاده

(Chart-3): Assessing the confidence rate in monitoring road damage events

#### (د) تعداد رخ داده‌های متفاوت<sup>۱</sup>

در این آزمایش، هدف بررسی تأثیر تعداد رخ داده‌های هم‌زمان و متنوع بر عملکرد مدل پیشنهادی و مدل‌های پایه است. در این سناریو، رخ داده‌ها به وسیلهٔ RSU‌ها شناسایی شده و برای صحت‌سنجی و تأیید امضا به کمیتهٔ ارزیابی ارسال می‌شوند؛ پس از تأیید نهایی، تراکنش مربوط به رخداد در زنجیرهٔ قالبی ثبت می‌شود.

برای ارزیابی دقیق‌تر، شبیه‌سازی در پنج سطح مختلف از نظر تعداد رخداد انجام شده است: ۲۰، ۴۰، ۶۰، ۸۰ و ۱۰۰ رخداد. هر مجموعه از رخ داده‌ها ترکیبی از سه نوع اصلی یعنی خرابی جاده، ترافیک و تصادف بوده است تا شرایط نزدیک به واقعیت در شبکهٔ بین‌خودرویی شبیه‌سازی شود.

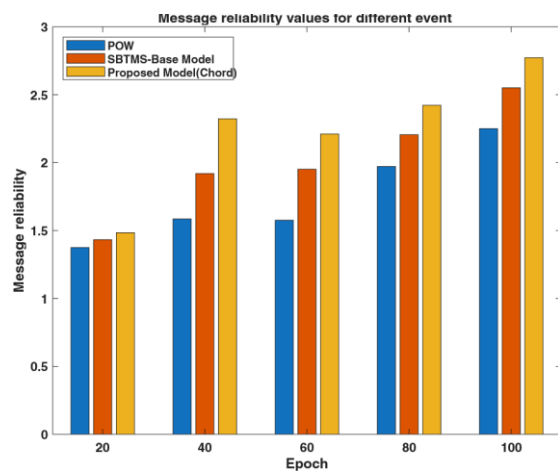
نتایج آزمایش نشان می‌دهد که با افزایش تعداد رخ داده‌ها، مدل پیشنهادی (SBTFC) همچنان قادر است با پایداری و دقت بالا، رخ داده‌های صحیح را شناسایی و تأیید کند؛ این در حالی است که در مدل‌های پایه SBTMS و POW با افزایش حجم رخ داده‌ها، نرخ اعتماد کاهش محسوسی پیدا می‌کند. دلیل این امر، افزایش بار محاسباتی در فرآیند اجماع و محدودیت در هماهنگی بین RSU‌ها در مدل‌های پایه است؛ در حالی که مدل پیشنهادی با استفاده از الگوریتم تقسیم‌بندی مبتنی بر ساختار Chord و کمیته‌های محلی، توانسته است بار پردازشی را بین RSU‌ها توزیع و از ازدحام محاسباتی جلوگیری کند.

بر اساس نتایج، در بیشترین مقدار آزمایش (صد رخداد)، میزان قابلیت اطمینان میانگین RSU‌ها در مدل

<sup>1</sup> Number of Different Events

پیشنهادی حدود ۹۳ درصد بوده است؛ در حالی که در مدل SBTMS این مقدار ۸۵ درصد و در مدل POW حدود ۶۸ درصد گزارش شده است. این اختلاف نشان‌دهندهٔ افزایش هشت تا ۲۵ درصدی دقت و اعتماد شبکه در مدل پیشنهادی نسبت به مدل‌های پایه است.

به طور خلاصه، نتایج این سناریو نشان می‌دهد که حتی در صورت افزایش حجم رخ داده‌ها و بار تراکنش‌های شبکه، پایداری، هماهنگی و دقت مدل پیشنهادی در سطح بالایی حفظ می‌شود و سامانه توانایی مدیریت رخ داده‌های متنوع را بدون افت محسوس در اعتماد دارد.



(نمودار-۴): ارزیابی نرخ اعتماد به پایش رخ داده‌های متفاوت

(Chart-4): Assessing the confidence rate in monitoring different events

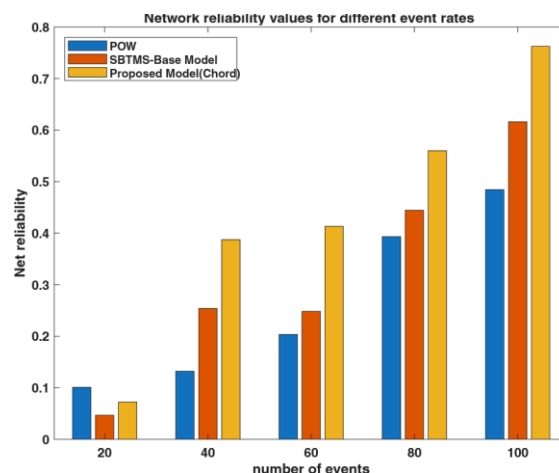
همان‌گونه که در نمودار (۴) مشاهده می‌شود، میانگین قابلیت اطمینان ره‌یافت پیشنهادی (SBTFC) در مقایسه با دو طرح پایه، به شکل محسوسی بهبود یافته است؛ این افزایش به‌ویژه در بازه‌هایی که تعداد رخ داده‌ها زیاد، (بیش از شصت رخداد)، چشم‌گیرتر است.

نتایج کمی شبیه‌سازی نشان می‌دهد که میانگین قابلیت اطمینان به پیام‌ها در مدل پیشنهادی برابر با ۲.۳، در مدل SBTMS برابر با ۲.۱۶ و در مدل POW برابر با ۲.۰۴ بوده، به عبارت دیگر، ره‌یافت پیشنهادی در مقایسه با مدل SBTMS حدود شش درصد و در مقایسه با مدل POW حدود یازده درصد بهبود در شاخص اعتماد ایجاد کرده است. این یافته‌ها نشان‌دهندهٔ توانایی مدل پیشنهادی در افزایش پایداری شبکه، بهبود هماهنگی بین RSU‌ها، و کاهش نرخ خطا در تشخیص رخ داده‌ها است.

در مجموع، این نتایج اثبات می‌کند که ترکیب ساختار مبتنی بر کمیته‌های ارزیابی و منطق فازی در مدل SBTFC نقش کلیدی در ارتقای اعتماد سامانه بین‌خودرویی ایفا می‌کند و مدل را در مقایسه با ره‌یافت‌های پایه، از نظر قابلیت اطمینان، دقت و پایداری عملکرد در سطح بالاتری قرار می‌دهد.



در سناریوی رخ دادهای ترافیکی نمایش می‌دهد. در مراحل ابتدایی شبیه‌سازی، هر سه مدل عملکردی تا حدودی مشابه دارند، اما با افزایش تعداد تعاملات و پیچیدگی داده‌ها، مدل پیشنهادی به‌واسطه بهره‌گیری از سامانه فازی و سازوکار ارزیابی گروهی، به‌طور پیوسته نرخ اعتماد بالاتری را حفظ می‌کند. از حدود راند بیست به‌بعد، اختلاف عملکرد مدل‌ها نمایان‌تر می‌شود و مدل پیشنهادی با شیب صعودی ملایم، به نرخ اعتماد نزدیک به ۱۰۰ می‌رسد؛ درمقابل، مدل POW دچار نوسانات بیشتری شده و در نرخ‌های بالای رخداد، کاهش اعتماد را تجربه می‌کند. این نمودار نشان می‌دهد که مدل پیشنهادی در محیط‌های پرتراffیک، از پایداری و دقت بالاتری در ارزیابی پیام‌ها برخوردار است و نسبت به مدل‌های پایه، اعتمادپذیری شبکه را به‌طور معناداری افزایش می‌دهد.

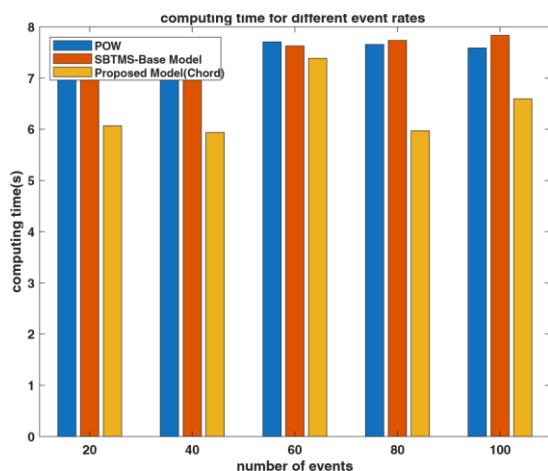


(نمودار-۸): اعتماد به کمیته‌ها در رخ دادهای مختلف  
(Chart-8): Trust in committees in various events

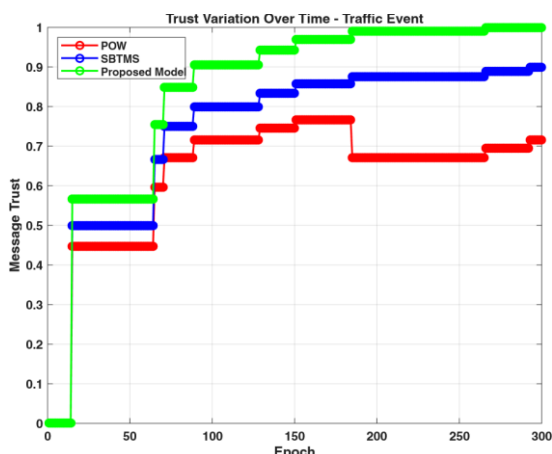
### ۳-۶- پیچیدگی محاسباتی

در این سناریو، ره‌یافت پیشنهادی (SBTFC) و دو مدل پایه SBTMS و POW در شرایط به‌طورکامل یکسان و مشابه پیاده‌سازی شده‌اند و پیچیدگی محاسباتی آن‌ها باتوجه به تعداد رخ دادهای شبکه بین‌خودرویی و وسایل نقلیه مورد ارزیابی قرار گرفته‌است. نتایج این بررسی در نمودار (۹) نمایش داده شده‌است.

همان‌گونه که مشاهده می‌شود، میانگین پیچیدگی محاسباتی در مدل پیشنهادی، در مقایسه با مدل‌های پایه، کمتر است. به‌طور دقیق، ره‌یافت پیشنهادی در مقایسه با SBTMS حدود شش درصد کاهش و در مقایسه با POW حدود پنج درصد کاهش در پیچیدگی محاسباتی نشان می‌دهد.



(نمودار-۹): پیچیدگی محاسباتی مدل  
(Chart-9): Computational complexity of the model



(نمودار-۱۰): تغییرات اعتماد پیام در طول زمان - ترافیک  
(Chart-10): Trust Variation Over Time - Traffic Event

نمودارهای (۱۱) و (۱۲) به‌ترتیب تغییرات نرخ اعتماد پیام در طول زمان را برای رخ دادهای تصادف و خرابی جاده نمایش می‌دهند. در هر دو سناریو، مدل پیشنهادی با گذشت

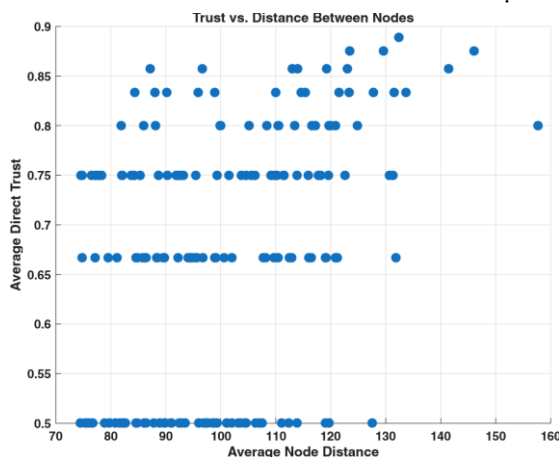
این کاهش پیچیدگی ناشی از استفاده از الگوریتم تقسیم‌بندی مبتنی بر ساختار Chord و کمیته‌های محلی برای اعتبارسنجی تراکنش‌ها است که اجازه می‌دهد بار پردازشی بین RSU ها توزیع شده و از محاسبات زائد جلوگیری شود؛ درنتیجه، حتی با افزایش تعداد رخ دادهای، زمان پردازش و منابع محاسباتی مورد نیاز بهینه باقی می‌ماند و شبکه توانایی مدیریت تراکنش‌ها و رخ دادهای متعدد را بدون افت عملکرد دارد.

به‌اختصار، نتایج این تحلیل نشان می‌دهد که مدل پیشنهادی نه‌تنها قابلیت اعتماد و دقت بالاتری نسبت به مدل‌های پایه دارد، بلکه بهینه‌تر و کارآمدتر از نظر محاسباتی نیز عمل می‌کند.

### ۴-۶- بررسی اعتماد در طول زمان

در ادامه به بررسی اعتماد در طول زمان برای سه نوع رخداد ترافیک، تصادف و خرابی جاده پرداخته شده‌است. نمودار (۱۰)، روند تغییرات نرخ اعتماد پیام در طول زمان را برای سه مدل POW، SBTMS و مدل پیشنهادی

مدل قادر است اعتماد را به‌صورت تطبیقی و واقع‌گرایانه محاسبه کند.

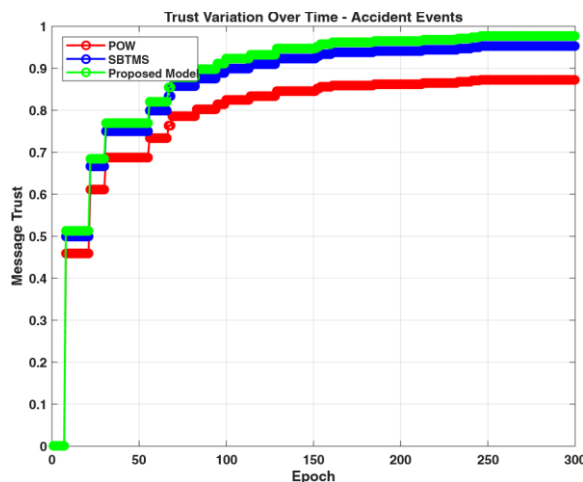


(نمودار-۱۳): نمای کلی از فاصله فیزیکی  
گره‌ها و اعتماد مستقیم  
(Chart-13): Trust vs. Distance Between Nodes

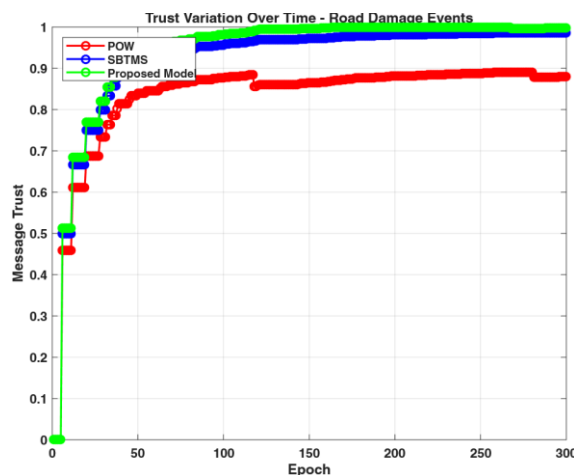
در بخش پایانی، عملکرد کلی سه مدل بررسی شده‌است. نمودار (۴) میانگین نرخ اعتماد پیام را در سناریوهای مختلف برای سه مدل POW، SBTMS و مدل پیشنهادی نشان می‌دهد، که محور افقی تعداد رویدادهای شبیه‌سازی‌شده و محور عمودی میانگین اعتماد پیام در هر مدل را نشان می‌دهد؛ همان‌طور که مشاهده می‌شود، مدل پیشنهادی در تمامی سناریوها عملکرد برتری دارد و میانگین اعتماد بالاتری را حفظ می‌کند. این برتری به‌ویژه در سناریوهایی با تعداد رویداد بیشتر و شرایط پرتراфик و پیچیده، برجسته است. عملکرد بهتر مدل پیشنهادی ناشی از بهره‌گیری از سامانه فازی تطبیقی و ساختار توزیع‌شده Chord در فرآیند اجماع است که دقت ارزیابی پیام‌ها را افزایش داده و تأثیر داده‌های جعلی را کاهش می‌دهد؛ در کل، نمودار (۱۴) نشان‌دهنده پایداری و مقیاس‌پذیری بالای مدل پیشنهادی در محیط‌های متغیر و چالش‌برانگیز شبکه است.

نمودار (۱۵) قابلیت اطمینان شبکه را در سناریوهای مختلف برای مدل‌های POW، SBTMS و مدل پیشنهادی نمایش می‌دهد، که محور افقی تعداد رویدادهای شبیه‌سازی‌شده و محور عمودی مقدار قابلیت اطمینان محاسبه‌شده در هر مدل را مشخص می‌کند؛ همان‌طور که مشاهده می‌شود، مدل پیشنهادی در تمامی سناریوها از قابلیت اطمینان بالاتری برخوردار است و این برتری در سناریوهای پرتراфик و پیچیده، برجسته‌تر می‌شود. عملکرد برتر مدل پیشنهادی به‌دلیل استفاده از سازوکار اجماع مبتنی بر کمیته‌های ارزیاب، منطق فازی تطبیقی و ساختار توزیع‌شده Chord است که موجب کاهش خطاهای محاسباتی، حذف داده‌های نادرست و افزایش هماهنگی میان RSU‌ها می‌شود. درمجموع، نمودار (۱۵)

زمان و افزایش تعاملات میان گره‌ها، نرخ اعتماد بالاتری نسبت به مدل‌های پایه حفظ می‌کند. این روند صعودی نشان‌دهنده پایداری و دقت بالاتر مدل پیشنهادی در ارزیابی پیام‌ها در شرایط متنوع و چالش‌برانگیز شبکه است.



(نمودار-۱۱): تغییرات اعتماد پیام در طول زمان - تصادف  
(Chart-11): Trust Variation Over Time - Accident Event



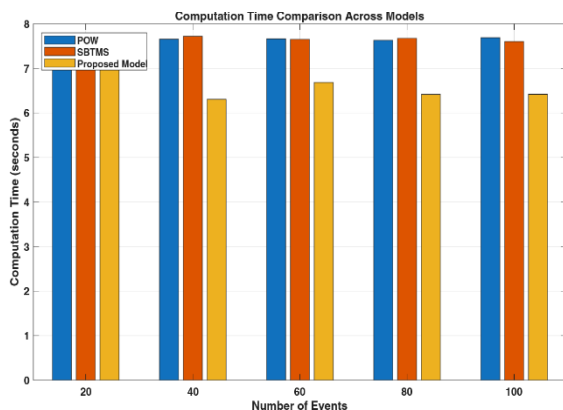
(نمودار-۱۲): تغییرات اعتماد پیام در طول زمان - خرابی جاده  
(Chart-12): Trust Variation Over Time - Road Damage Event

در ادامه، مدل پیشنهادی با توجه به موقعیت مکانی گره‌ها بررسی شد. نمودار (۱۳) رابطه بین فاصله فیزیکی گره‌ها و میزان اعتماد مستقیم آن‌ها را نشان می‌دهد؛ همان‌طور که مشاهده می‌شود، با افزایش فاصله، اعتماد مستقیم به‌طور نسبی کاهش می‌یابد. این نتیجه نشان می‌دهد که گره‌های نزدیک به یکدیگر، به‌دلیل تعاملات بیشتر و مشاهده مستقیم رخدادها، اعتماد بالاتری دارند؛ درحالی‌که گره‌های دورتر به‌دلیل کاهش ارتباط مستقیم و احتمال خطا یا تأخیر در دریافت داده‌ها، اعتماد کمتری دارند.

این رابطه منفی میان فاصله و اعتماد، صحت و اعتبار مدل پیشنهادی را در ارزیابی دقیق و پویا بر اساس موقعیت مکانی گره‌ها تأیید می‌کند و نشان می‌دهد که

## ۵-۶- تحلیل رسمی مدل پیشنهادی SBTFC

در این بخش، امنیت مدل پیشنهادی مبتنی بر زنجیره قالبی و سامانه فازی (SBTFC) از منظر مقاومت در برابر حملات متداول شبکه‌های بین‌خودرویی مورد بررسی قرار گرفته‌است. هدف، ارزیابی پایداری و قابلیت اطمینان ساختار کمیته‌ای RSUها در مواجهه با حملات رایج از قبیل Sybil، DoS، و Replay است.



(نمودار-۱۶): زمان اجرای الگوریتم‌ها  
(Chart-16): Algorithm execution time

مدل پیشنهادی با ترکیب چهار مؤلفه اصلی شامل زنجیره قالبی غیرمتمرکز، سامانه استنتاج فازی، ساختار کمیته‌ای RSU و الگوریتم درهم‌سازی Chord طراحی شده‌است تا ضمن کاهش پیچیدگی محاسباتی، مقاومت امنیتی شبکه را افزایش دهد.

### ۶-۶ مقاومت در برابر حمله Sybil

در حملات Sybil، مهاجم با ایجاد چندین هویت جعلی تلاش می‌کند فرآیند تصمیم‌گیری شبکه را مختل کند. در مدل SBTFC، شناسه هر RSU بر اساس درهم‌سازی ترکیبی از آدرس IP، کلید عمومی و عدد تصادفی ۳۲ بیتی در ساختار Chord تولید می‌شود. این شناسه در زمان عضویت گره به‌وسیله کمیته‌های RSU اعتبارسنجی می‌شود.

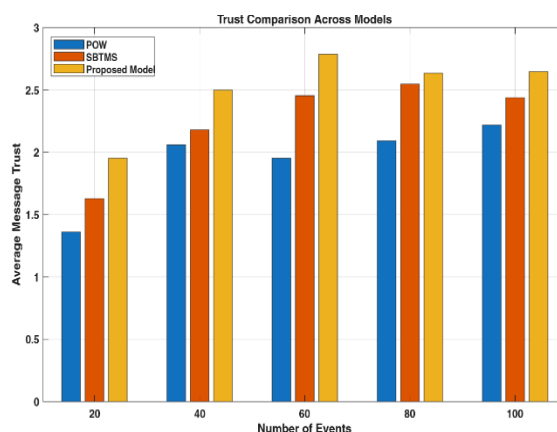
از آنجا که مقدار درهم‌سازی یک‌طرفه و غیرقابل پیش‌بینی است، تولید هویت‌های جعلی یا تکراری در عمل غیرممکن است؛ علاوه بر این، نتایج احراز هویت در دفترکل زنجیره قالبی ذخیره می‌شود و هیچ گرهی قادر به تغییر یا جعل اطلاعات ثبت‌شده نیست؛ در نتیجه، مدل پیشنهادی در برابر حملات Sybil از مقاومت بسیار بالایی برخوردار است و امکان نفوذ با هویت‌های متعدد وجود ندارد.

### ۶-۷ مقاومت در برابر حمله DoS (انکار سرویس)

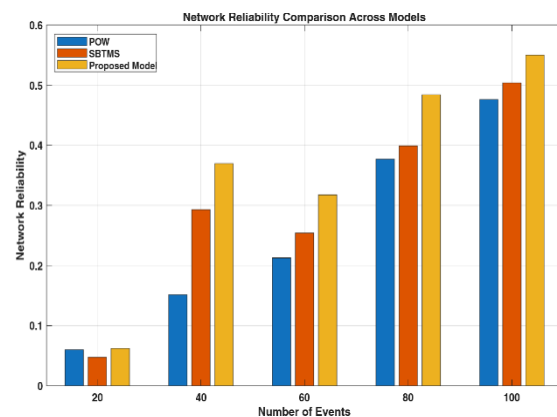
در حملات DoS، مهاجم با ارسال حجم زیادی از درخواست‌های غیرواقعی، منابع شبکه را اشباع و مانع از ارائه خدمات به گره‌های سالم می‌شود.

نشان‌دهنده پایداری و دقت بالای مدل پیشنهادی در حفظ قابلیت اطمینان شبکه تحت شرایط متغیر و چالش‌برانگیز است.

نمودار (۱۶) زمان اجرای محاسباتی مدل‌های POW، SBTMS و مدل پیشنهادی را در سناریوهایی با تعداد رویداد متفاوت نشان می‌دهد، که محور افقی تعداد رویدادهای شبیه‌سازی شده و محور عمودی زمان اجرای الگوریتم‌ها (بر حسب ثانیه) را نمایش می‌دهد؛ همان‌طور که دیده می‌شود، مدل POW به دلیل ساختار ساده‌تر زمان اجرای کمتری دارد، اما دقت و قابلیت اطمینان پایین‌تری ارائه می‌دهد. مدل SBTMS با افزایش تعداد رویدادها، رشد قابل توجهی در زمان اجرا نشان می‌دهد که ضعف مقیاس‌پذیری آن را آشکار می‌کند؛ درمقابل، مدل پیشنهادی با وجود پیچیدگی بیشتر، به‌واسطه تقسیم وظایف بین RSUها و استفاده از ساختار Chord، زمان اجرای متعادلی را حفظ کرده‌است و حتی در سناریوهای پرترافیک نیز عملکرد مناسبی ارائه می‌دهد. این نمودار نشان می‌دهد که مدل پیشنهادی علاوه بر دقت و قابلیت اطمینان بالا، از نظر زمان اجرا نیز در شرایط واقعی شبکه پایدار و بهینه عمل می‌کند.



(نمودار-۱۴): میانگین اعتماد پیام در مدل‌ها  
(Chart-14): Average message confidence in models



(نمودار-۱۵): قابلیت اطمینان شبکه در مدل‌ها  
(Chart-15): Network reliability in models

## ۷- بحث و نتیجه گیری

در این پژوهش، یک چهارچوب هوشمند و ایمن برای شبکه‌های بین خودروبی مبتنی بر ترکیب فناوری زنجیره قالی، منطق فازی و ساختار توزیع شده Chord ارائه شد. هدف از این مدل، افزایش قابلیت اعتماد، کاهش پیچیدگی محاسباتی و حذف نقاط متمرکز آسیب‌پذیر در زیرساخت ارتباطی سامانه‌های حمل‌ونقل هوشمند<sup>۴</sup> بود.

باتوجه به پویایی بالای گره‌ها و فقدان اعتماد ذاتی در محیط شبکه‌های بین خودروبی، طراحی یک سازوکار اعتماد توزیع شده و غیرمتمرکز ضرورتی اجتناب‌ناپذیر است. مدل پیشنهادی (SBTFC) با استفاده از سامانه فازی برای محاسبه اعتماد مستقیم و غیرمستقیم و زنجیره قالی جهت ثبت تغییرناپذیر تراکنش‌ها، توانست پایداری و قابلیت اطمینان شبکه را به‌طور چشم‌گیری بهبود دهد؛ افزون‌براین، با بهره‌گیری از الگوریتم Chord در تشکیل کمیته‌های RSU و تخصیص کلیدهای رمز، خطر حملات جعل هویت و سازش در فرآیند اجماع کاهش یافت و امکان شناسایی رخ داده‌ها (نظیر تصادف، خرابی جاده و ازدحام ترافیکی) با دقت بالاتری فراهم شد.

نتایج شبیه‌سازی‌ها نشان داد که روش پیشنهادی، در مقایسه با طرح‌های پایه SBTMS و POW، میانگین نرخ اعتماد و قابلیت اطمینان را به‌ترتیب شش و یازده درصد افزایش داده و درعین حال پیچیدگی محاسباتی را پنج تا شش درصد کاهش داده‌است. این نتایج مؤید آن است که حذف فرآیند ماینینگ و جایگزینی آن با ساختار Chord، ضمن حفظ امنیت، موجب تسریع در اجماع و کاهش مصرف منابع محاسباتی در شبکه شده‌است.

از نگاه کاربردی، ره‌یافت پیشنهادی می‌تواند به‌عنوان هسته‌ای قابل اتکا برای مدیریت داده و اعتماد در سامانه‌های حمل‌ونقل هوشمند به‌کار گرفته شود. در خودروهای خودران و ناوگان‌های مشارکتی<sup>۵</sup>، این چهارچوب قادر است در زمان واقعی، اعتماد میان وسایل نقلیه را ارزیابی کرده و با اطمینان از صحت پیام‌های مبادله شده، تصمیم‌گیری‌های خودکار را ایمن‌تر کند؛ همچنین با به‌کارگیری این مدل در زیرساخت‌های شهری هوشمند، می‌توان تبادل اطلاعات بین ایستگاه‌های RSU، مراکز کنترل ترافیک و سرویس‌های ابری را با امنیت بالا و بدون وابستگی به نهاد متمرکز انجام داد.

در راستای توسعه‌های آینده، ترکیب ره‌یافت پیشنهادی با فناوری‌های پردازش لبه<sup>۶</sup> و رایانش مه<sup>۷</sup>

در طرح SBTFC، سه سازوکار مکمل برای مقابله با این نوع حمله در نظر گرفته شده‌است:

۱. توزیع بار پردازشی میان کمیته‌های RSU باعث حذف نقاط متمرکز و کاهش احتمال اشباع منابع می‌شود.
  ۲. مدل اعتماد تطبیقی فازی<sup>۱</sup> سبب می‌شود پیام‌های مشکوک یا غیرمعتبر توسط RSU‌ها شناسایی و حذف شوند.
  ۳. در صورت تشخیص رفتار غیرعادی، هشدار امنیتی از طریق زنجیره قالی به سایر RSU‌ها منتقل و گره مهاجم در سطح شبکه مسدود می‌شود.
- این ساختار، انعطاف‌پذیری بالایی در برابر حملات انکار سرویس ایجاد می‌کند و عملکرد سامانه را پایدار نگه می‌دارد.

## ۸-۶- مقاومت در برابر حمله بازپخش پیام<sup>۲</sup>

در حمله Replay، مهاجم با ضبط پیام معتبر و بازپخش آن در زمانی دیگر، قصد ایجاد اختلال یا انتشار داده‌های نادرست دارد.

در مدل پیشنهادی، هر پیام دارای شناسه یکتای پیام  $m_i$  است که از ترکیب نوع حادثه، مختصات مکانی و مهر زمان<sup>۳</sup> تولید می‌شود. این شناسه در زنجیره قالی ثبت و در فرآیند اعتبارسنجی بررسی می‌شود.

در صورت مشاهده شناسه تکراری، کمیته مربوطه پیام را مردود اعلام کرده و از درج آن در بلاک جلوگیری می‌کند؛ همچنین سامانه فازی اطمینان باعث می‌شود پیام‌های مشابه با وزن اعتماد کمتر ارزیابی و حذف شوند؛ بنابراین احتمال موفقیت حملات بازپخش پیام در این مدل نزدیک به صفر است.

## ۹-۶- تحلیل جامع امنیتی

نتایج تحلیل‌ها نشان می‌دهد که مدل پیشنهادی SBTFC در مقایسه با ره‌یافت‌های پایه SBTMS و POW از نظر احراز هویت، تمامیت داده‌ها، مقاومت در برابر جعل و جلوگیری از حملات توزیع شده برتری محسوسی دارد. ترکیب چهار لایه امنیتی شامل:

۱. درهم‌سازی غیرقابل معکوس Chord
  ۲. کمیته‌های تأییدکننده RSU با ساختار اجماع مبتنی بر زنجیره قالی،
  ۳. سامانه استنتاج فازی برای تصمیم‌گیری هوشمند در خصوص اعتبار داده‌ها،
  ۴. سازوکار انتشار امن و غیرمتمرکز پیام‌ها
- باعث شده‌است که مدل پیشنهادی ضمن حفظ کارایی محاسباتی، امنیت و قابلیت اعتماد بالاتری را در شبکه‌های بین خودروبی فراهم آورد.

<sup>۴</sup> ITS

<sup>۵</sup> Collaborative Driving

<sup>۶</sup> Edge Computing

<sup>۷</sup> Fog Computing

<sup>۱</sup> Fuzzy Trust

<sup>۲</sup> Replay

<sup>۳</sup> Timestamp

- [1] S. Jiang, Z. Huang, and Y. Ji, "Adaptive UAV-assisted geographic routing with q-learning in VANET," *IEEE Communications Letters*, vol. 25, no. 4, pp. 1358-1362, 2020.
  - [2] Y. Liang, E. Luo, and Y. Liu, "Physically secure and conditional-privacy authenticated key agreement for VANETs," *IEEE Transactions on Vehicular Technology*, 2023.
  - [3] N. Hu, X. Qin, N. Ma, Y. Liu, Y. Yao, and P. Zhang, "Energy-efficient Caching and Task offloading for Timely Status Updates in UAV-assisted VANETs," *arXiv preprint arXiv:2205.00692*, 2022.
  - [4] M. M. Hamdi, Y. A. Yussen, and A. S. Mustafa, "Integrity and Authentications for service security in vehicular ad hoc networks (VANETs): A Review," in *2021 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2021, pp. 1-7: IEEE.
  - [5] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503-531, 2022.
  - [6] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, 2023.
  - [7] Y. He, D. Zhai, F. Huang, D. Wang, X. Tang, and R. Zhang, "Joint task offloading, resource allocation, and security assurance for mobile edge computing-enabled UAV-assisted VANETs," *Remote Sensing*, vol. 13, no. 8, p. 1547, 2021.
  - [8] M. Fotros, J. Rezazadeh, and O. Ameri Sianaki, "A survey on vanets routing protocols for iot intelligent transportation systems," in *Workshops of the International Conference on Advanced Information Networking and Applications*, 2020, pp. 1097-1115: Springer.
  - [9] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, and A. S. Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs)," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1-7: IEEE.
  - [10] R. Rajeswari and S. Rajesh, "Enhance Security and Privacy in VANET Based Sensor Monitoring and Emergency Services," *Cybernetics and Systems*, pp. 1-22, 2023.
  - [11] B. Hou, Y. Xin, H. Zhu, Y. Yang, and J. Yang, "VANET Secure Reputation Evaluation & Management Model Based on Double Layer Blockchain," *Applied Sciences*, vol. 13, no. 9, p. 5733, 2023.
  - [12] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.
  - [13] S. Yogarayan, S. F. A. Razak, A. Azman, M. F. A. Abdullah, S. Z. Ibrahim, and K. J. Raman, "A review of routing protocols for vehicular ad-hoc networks (VANETs)," in *2020 8th International Conference on Information and Communication Technology (ICoICT)*, 2020, pp. 1-7: IEEE.
- پیشنهاد می‌شود تا با انتقال بخشی از پردازش به نزدیک‌ترین RSU یا گره خودرویی، تأخیر شبکه کاهش و واکنش به رخدادها در زمان واقعی امکان‌پذیر شود؛ همچنین می‌توان از ساختارهای هم‌ارز با Chord مانند Pastry یا Kademlia برای بهبود توازن بار و مقیاس‌پذیری استفاده کرد؛ در کل، مدل ارائه‌شده می‌تواند به‌عنوان یک چهارچوب پایه برای طراحی سامانه‌های اعتمادپذیر در خودروهای خودران، ناوگان‌های هوشمند و شبکه‌های حمل‌ونقل آینده مورد استفاده قرار گیرد و گامی مؤثر در مسیر تحقق شهرهای هوشمند ایمن و پایدار باشد.
- باوجود نتایج مطلوب مدل پیشنهادی SBTFC، همچنان محدودیت‌هایی وجود دارد که در توسعه‌های آینده باید مورد توجه قرار گیرد. نخست آنکه عملکرد مدل تا حدی به تراکم و در دسترس بودن ایستگاه‌های کنار جاده وابسته است. در نواحی با پوشش اندک RSU، فرآیند تشکیل کمیته‌های ارزیاب و احراز هویت گره‌ها ممکن است با تأخیر یا افت دقت مواجه شود؛ بنابراین برای افزایش پایداری، ترکیب این مدل با نودهای سیار جانشین<sup>۱</sup> یا زیرساخت‌های ابری سبک‌وزن پیشنهاد می‌شود.
- دوم، استفاده از زنجیرهٔ قالبی خصوصی هرچند امنیت و کنترل را افزایش می‌دهد، اما موجب افزایش سربار ذخیره‌سازی و پردازش تراکنش‌ها در RSU می‌شود. این مسئله به‌ویژه در سناریوهای پرتراکنش یا در محیط‌هایی با محدودیت توان محاسباتی، می‌تواند کارایی سامانه را کاهش دهد.
- سوم، مدل پیشنهادی به‌دلیل بهره‌گیری از ساختار Chord برای مدیریت شناسه‌ها و توزیع کلیدها، در شبکه‌های بسیار بزرگ ممکن است با چالش نگهداری جداول انگشتی و به‌روزرسانی مستمر مواجه شود که بر زمان هم‌گرایی و پایداری شبکه اثر می‌گذارد.
- درنهایت، از آنجا که منطق فازی به قوانین ازپیش تعریف‌شده وابسته است، در شرایط غیرقابل پیش‌بینی (مانند رفتارهای تصادفی رانندگان یا حملات ترکیبی) ممکن است دقت تصمیم‌گیری کاهش یابد. توسعهٔ یک سامانه یادگیری تطبیقی<sup>۲</sup> یا ادغام با یادگیری تقویتی<sup>۳</sup> می‌تواند این محدودیت را برطرف کند.
- با در نظر گرفتن این چالش‌ها، پژوهش‌های آتی می‌تواند با طراحی ساختارهای هیبریدی مبتنی بر-Edge Fog Computing و زنجیرهٔ قالبی سبک‌وزن، کارایی و پایداری طرح را در محیط‌های واقعی خودروهای خودران و سامانه‌های حمل‌ونقل هوشمند ارتقا دهند.

<sup>1</sup> Mobile Agents<sup>2</sup> Adaptive Learning-based Fuzzy System<sup>3</sup> Reinforcement Learning

- verification scheme for vehicular ad hoc networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 5, p. e3857, 2022.
- [27] X. Li and X. Yin, "Blockchain-based group key agreement protocol for vehicular ad hoc networks," *Computer Communications*, vol. 183, pp. 107-120, 2022.
- [28] C. Lin, D. He, X. Huang, N. Kumar, and K.-K. R. Choo, "BCPPA: A blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 12, pp. 7408-7420, 2020.
- [29] S. P. Singh and G. H. Sastry, "Blockchain-Enabled Security in Vehicular Ad Hoc Network Check for updates," *Advances in Data Science and Computing Technologies: Select Proceedings of ASDC 2022*, vol. 1056, p. 181, 2023.
- [30] M. Azath and V. Singh, "An approach to preventing vehicular ad-hoc networks from malicious nodes based on blockchain," *Review of Computer Engineering Research*, vol. 10, no. 1, pp. 16-27, 2023.
- [31] A. Ansari, "The basics of fuzzy logic: A tutorial review," *COMPUTER EDUCATION-STAFFORD-COMPUTER EDUCATION GROUP*, vol. 88, pp. 5-8, 1998.
- [32] D.-G. Zhang, C.-H. Ni, J. Zhang, T. Zhang, and Z.-H. Zhang, "New method of vehicle cooperative communication based on fuzzy logic and signaling game strategy," *Future Generation Computer Systems*, 2022.
- [33] X. Zhang, J. Lai, and A. J. Moshayedi, "Traffic data security sharing scheme based on blockchain and traceable ring signature for VANETs," *Peer-to-Peer Networking and Applications*, pp. 1-18, 2023.
- [34] H. Panchal and S. Gajjar, "Fuzzy Logic-Based Cluster Head Selection an Underwater Wireless Sensor Network: A Survey," in *Communication and Intelligent Systems: Proceedings of ICCIS 2021*: Springer, 2022, pp. 661-673.
- [35] S. Kniesburges, A. Koutsopoulos, and C. Scheideler, "Re-chord: a self-stabilizing chord overlay network," *Theory of Computing Systems*, vol. 55, no. 3, pp. 591-612, 2014.
- [36] H. Thakkar and S. Ujjwal, "The Successful Key Division Using Chord, Pastry, and Kadmelia," in *2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC)*, 2023, pp. 1-8: IEEE.
- [37] H. Li, Y. Li, Q. Zhang, and Z. Yang, "Contact-aware Multiple-Layer CHORD for routing in Large-scale Satellite Networks," in *2023 IEEE/CIC International Conference on Communications in China (ICCC)*, 2023, pp. 1-6: IEEE.
- [38] C.-P. Balatsouras, A. Karras, C. Karras, D. Tsolis, and S. Sioutas, "Wichord: A chord protocol application on p2p lora wireless sensor networks," in *2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA)*, 2022, pp. 1-8: IEEE.
- [39] S. Wang, Y. Hu, and G. Qi, "Blockchain and deep learning based trust management for
- [14] A. P. Mdee, M. T. R. Khan, J. Seo, and D. Kim, "Security compliant and cooperative pseudonyms swapping for location privacy preservation in VANETs," *IEEE Transactions on Vehicular Technology*, 2023.
- [15] M. A. Al-Shareeda and S. Manickam, "A Systematic Literature Review on Security of Vehicular Ad-hoc Network (VANET) based on VEINS Framework," *IEEE Access*, 2023.
- [16] مجاهد، محمد مهدی، حسنی کرباسی، امیر، دری نوگورانی، صادق، کیاکجوری، علیرضا، «پروتکلی برای ارتباطات گمنام احراز اصالت شده با رمزنگاری پساکوانتومی و قراردادهای هوشمند»، *مجله مهندسی برق دانشگاه تبریز*، ۵۳ (۱)، ۴۹-۵۹، فروردین ۱۴۰۲.
- [16] M. M. Mojahid, A. Hassani Karbasi, S. Dari Nogurani, A. Kiakjori, "A protocol for authenticated anonymous communications with post-quantum cryptography and smart contracts", *Journal of Electricity of Tabriz University*, Vol. 53, No. 1, pp. 49-59, 2023.
- [17] A. Alharthi, *Blockchain Based Security and Trust Mechanisms for Vehicular Ad hoc Networks*. Lancaster University (United Kingdom), 2023.
- [18] مهدی خان، روزبه، خالقی بیزکی، حسین، طباطبایی، سیدغلام حسین، «تخصیص منابع برش‌های شبکه با استفاده از زنجیره بلوکی در شبکه‌های چندین دامنه‌ای»، *مجله مهندسی برق دانشگاه تبریز*، ۵۴ (۱)، ۷۳-۸۵، اردیبهشت ۱۴۰۳.
- [18] R. Mehdi Khan, H. Khaleghi Bizeki, S. G. H. Tabatabaei, "Resource Allocation of Network Slices Using Blockchain in Multi-Domain Networks", *Journal of Electrical Engineering, University of Tabriz*,
- [19] F. Ghovanlooy Ghajar, J. Salimi Sratkhti, and A. Sikora, "Sbtms: Scalable blockchain trust management system for vanet," *Applied Sciences*, vol. 11, no. 24, p. 11947, 2021.
- [20] B. Sekhar et al., "Artificial neural network-based secured communication strategy for vehicular ad hoc network," *Soft Computing*, vol. 27, no. 1, pp. 297-309, 2023.
- [21] H. Amari, Z. Abou Elhouda, L. Khoukhi, and L. H. Belguith, "Trust Management in Vehicular Ad-hoc Networks: Extensive Survey," *IEEE Access*, 2023.
- [22] J. Zhang, H. Fang, H. Zhong, J. Cui, and D. He, "Blockchain-Assisted Privacy-Preserving Traffic Route Management Scheme for Fog-Based Vehicular Ad-Hoc Networks," *IEEE Transactions on Network and Service Management*, 2023.
- [23] J. Grover, "Security of Vehicular Ad Hoc Networks using blockchain: A comprehensive review," *Vehicular Communications*, vol. 34, p. 100458, 2022.
- [24] X. Feng, K. Cui, H. Jiang, and Z. Li, "EBAS: An Efficient Blockchain-Based Authentication Scheme for Secure Communication in Vehicular Ad Hoc Network," *Symmetry*, vol. 14, no. 6, p. 1230, 2022.
- [25] A. S. Akhter, M. Ahmed, A. Anwar, A. S. Shah, A.-S. K. Pathan, and A. Zengin, "Blockchain in vehicular ad hoc networks: Applications, challenges and solutions," *International Journal of Sensor Networks*, vol. 40, no. 2, pp. 94-130, 2022.
- [26] Y. Yang, D. He, H. Wang, and L. Zhou, "An efficient blockchain-based batch

- processing, 2018; 15 (۱): 101-112. URL: <http://jsdp.rcisp.ac.ir/article-1-394-en.html>
- [52] کبریائی، حامد، کمالی نژاد، حوراء، نجار اعرابی، بابک، «پیش‌بینی بار کوتاه‌مدت با انتخاب ورودی به روش LLE و موتور پیش‌بینی ترکیبی RBF-Fuzzy»، فصلنامه پردازش علائم و داده ها، ۱۶ (۱)، ۴۱-۵۶، بهار ۱۳۹۸.
- [52] Kebriaei H, Kamalinejad H, Nadjar Araabi B. "Short term load forecast by using Locally Linear Embedding manifold learning and a hybrid RBF-Fuzzy network", *Journal of signal and data processing*, 2019; 16 (1): 41-56. URL: <http://jsdp.rcisp.ac.ir/article-1-776-en.html>



**نیلوفر خسروی راد** مدرک  
کارشناسی ارشد خود را در سال ۱۳۹۶  
از دانشگاه شهاب دانش قم دریافت  
کرد. ایشان در حال حاضر دانشجوی  
مقطع دکترای دانشکده مهندسی  
کامپیوتر دانشگاه آزاد اسلامی واحد قم است.  
نشانی رایانامه ایشان عبارت است از:

Niloufarkhosravirad73@gmail.com



**رضا احسن** مدرک دکترای خود را از  
دانشگاه قم در گرایش مهندسی  
فناوری اطلاعات دریافت و مدرک  
کارشناسی ارشد خود را در گرایش  
مهندسی کامپیوتر هوش مصنوعی از  
دانشگاه آزاد اسلامی واحد علوم و تحقیقات و مدرک  
کارشناسی خود را در گرایش نرم‌افزار دانشگاه صنعتی  
سجاد دریافت کرده‌است. ایشان در حال حاضر استادیار و  
عضو هیئت علمی دانشگاه آزاد اسلامی واحد قم و رئیس  
دانشکده مهارت و کارآفرینی است.  
نشانی رایانامه ایشان عبارت است از:

ahsan.ac.ir@gmail.com



**احمد شریف** مدرک دکترای خود را  
از دانشگاه آزاد اسلامی واحد قم در  
گرایش مهندسی کامپیوتر دریافت و  
مدرک کارشناسی ارشد خود را در  
گرایش مهندسی کامپیوتر دانشگاه  
آزاد اسلامی واحد علوم و تحقیقات و مدرک کارشناسی  
خود را در گرایش نرم‌افزار دانشگاه آزاد اسلامی واحد اراک  
دریافت کرده‌است. ایشان در حال حاضر استادیار و عضو  
هیئت علمی گروه مهندسی کامپیوتر، مدیر گروه مهندسی  
کامپیوتر دانشکده فنی و مهندسی دانشگاه آزاد اسلامی  
واحد قم است.

نشانی رایانامه ایشان عبارت است از:

asharif@iau.ac.ir

- Internet of Vehicles," *Simulation Modelling Practice and Theory*, vol. 120, p. 102627, 2022.
- [40] X. Zhang, J. Lai, and A. J. Moshayedi, "Traffic data security sharing scheme based on blockchain and traceable ring signature for VANETs," *Peer-to-Peer Networking and Applications*, pp. 1-18, 2023.
- [41] C. P. Fernandes, C. Montez, D. D. Adriano, A. Boukerche, and M. S. Wangham, "A blockchain-based reputation system for trusted vanet nodes," *Ad Hoc Networks*, vol. 140, p. 103071, 2023.
- [42] B. Li, R. Liang, D. Zhu, W. Chen, and Q. Lin, "Blockchain-based trust management model for location privacy preserving in VANET," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3765-3775, 2020.
- [43] K. A. Awan, I. U. Din, and A. Almogren, "A blockchain-assisted trusted clustering mechanism for IoT-enabled smart transportation system," *Sustainability*, vol. 14, no. 22, p. 14889, 2022.
- [44] W. Ahmed, W. Di, and D. Mukathe, "Privacy-preserving blockchain-based authentication and trust management in VANETs," *IET Networks*, vol. 11, no. 3-4, pp. 89-111, 2022.
- [45] T. Gazdar, O. Alboqomi, and A. Munshi, "A Decentralized Blockchain-Based Trust Management Framework for Vehicular Ad Hoc Networks," *Smart Cities*, vol. 5, no. 1, pp. 348-363, 2022.
- [46] W. Ahmed, D. Wu, and D. Mukathie, "Blockchain-Assisted Trust Management Scheme for Securing VANETs," *KSII Transactions on Internet & Information Systems*, vol. 16, no. 2, 2022.
- [47] G. Anand, Lawal, Blockchain-Assisted Machine Learning Framework for Trust Management in VANETs (March 20, 2025). Available at SSRN: <https://ssrn.com/abstract=5321428> or <http://dx.doi.org/10.2139/ssrn.5321428>
- [48] Ehsan Memary, Chien-Chung Shen, Hao Guo, and Mark Nejad, "TrCoin: A Blockchain-Based Robust Trust Management System for VANET". *ACM J. Auton. Transport. Syst.* 2, 3, Article 13 (September 2025), 20 pages. <https://doi.org/10.1145/3729430>
- [49] Journal Article, "Blockchain-Based Multi-Path Mobile Access Point Selection for Secure 5G VANETs", Zhang, Zhiou, Guo, Weian, Li, Li, Li, Dongyang, arXiv preprint arXiv:2411.03371, 2024
- [50] Journal Article, "A trust management framework for vehicular ad hoc networks", Shahariar, Rezvi, Phillips, Chris, arXiv preprint arXiv:2405.04885, 2024
- [51] خداقلی، منا، دولتی، اردشیر، حسین زاده، علی، شمس‌الکتابی، خشایار، «روشی جدید برای عضویت‌دهی به داده‌ها و شناسایی نوفه و داده‌های پرت با استفاده از ماشین بردار پشتیبان فازی»، فصلنامه پردازش علائم و داده ها، ۱۵ (۱)، ۱۰۱-۱۱۲، پاییز ۱۳۹۷.
- [51] Khodaghohi M, Dolati A, Hosseinzadeh A, Shamsolketabi K. "A New Method to Determine Data Membership and Find Noise and Outlier Data Using Fuzzy Support Vector Machine", *Journal of signal and data*



**علی کریمی** مدرک کارشناسی ارشد خود را از دانشگاه آزاد اسلامی قم در رشته مهندسی کامپیوتر در سال ۱۴۰۳ دریافت کرده‌است. ایشان در حال حاضر دانشجوی دکترای مهندسی کامپیوتر گرایش نرم‌افزار واحد قم و کارمند سازمان فناوری و اطلاعات شهرداری قم در سمت رئیس اداره زیرساخت است.

نشانی رایانامه ایشان عبارت است از:

a.alikarimi91@gmail.com

