

Research article

Blockchain-enabled heterogeneous 6G supported secure vehicular management system over cloud edge computing

Abdul Razaque^{a,*}, Meenhoon Khan^b, Joon Yoo^c, Aziz Alotaibi^d, Majid Alshammari^d, Muder Almiani^e

^a Department of Cyber Security, Information Processing and Storage, Satbayev University, Almaty, Kazakhstan

^b Department of Computer Science, Bahria University, Islamabad, Pakistan

^c School of Computing, Gachon University, South Korea

^d Computers and Information Technology College, Taif University, Saudi Arabia

^e Management Information System (MIS) Gulf University for Science and Technology, Kuwait

ARTICLE INFO

Keywords:

IoT
Blockchain technology
6G network
Privacy-preservation
Vehicular management system
Heterogeneous network
Cloud edge computing

ABSTRACT

The emergence of 6G networks increases both the suitability and the speed of Internet-of-Things (IoT) devices within vehicular communication systems (VCSs). Wireless capabilities can be improved using a 6G network to successfully manage IoT devices in VCSs. 6G networks can be employed to reduce cyberattacks due to their unclaimed and unused operating frequencies. However, 6G networks could be vulnerable to cyberattacks due to their flexibility. The issues of 6G networks can adequately be addressed using blockchain technology. If a smart vehicular system uses IoT, then faster response times, substantial power reductions, and security for possible accident avoidance and safety provision can be achieved. Therefore, an energy-efficient consortium-based blockchain-enabled heterogeneous (EBH) 6G network for IoT devices can provide the best platform for secure management vehicular systems. In this article, we introduce a perspective architecture for the IoT-enabled secure vehicular system using a blockchain-enabled heterogeneous 6G network over cloud edge computing. The heterogeneous support of a 6G network is discussed, which is highly effective for smart vehicular management systems. The primary goal of the article is to motivate the community and researchers to use multidisciplinary and cross-cutting technologies integratively.

1. Introduction

Over decades of development, automobile use has increased exponentially across the world [1,2], making traffic complex and stressful to drivers. With the emergence of modern technologies, vehicle users prefer to gain access to social media and entertain applications using cellular wireless networks [3]. Vehicles are connected through several devices, such as mobile phones, laptops, and tablets, and the basic use and need for these devices to explore maps for road directions and sending messages must balance the safety of autonomous vehicles, weather conditions, etc. In addition, there are several power-hungry applications (e.g., Facebook, Netflix, WeChat, WhatsApp, Tiktok, etc.) that require higher power and faster wireless networks to maintain reliable data downloads and operate applications [4]. Existing cellular frequencies have become expensive and too congested to support IoT-enabled devices inside vehicles [5–8]. For the consumer, 6G wireless speeds are strongly desired and provide the ability to work efficiently in

* Corresponding author.

E-mail addresses: r.abdul@satbayev.university (A. Razaque), 01-134212-085@student.bahria.edu.pk (M. Khan), joon.yoo@gachon.ac.kr (J. Yoo), azotaibi@tu.edu.sa (A. Alotaibi), m.alshammari@tu.edu.sa (M. Alshammari), Almiani.M@gust.edu.kw (M. Almiani).

<https://doi.org/10.1016/j.iot.2024.101115>

Received 27 November 2023; Received in revised form 20 January 2024; Accepted 6 February 2024

Available online 15 February 2024

2542-6605/© 2024 Elsevier B.V. All rights reserved.

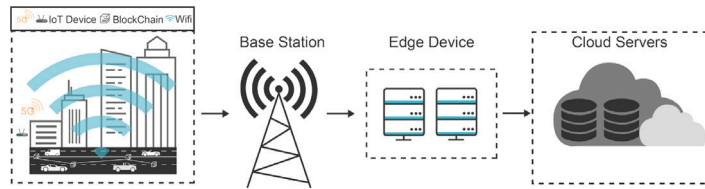


Fig. 1. Blockchain-enabled heterogeneous 6G supported secure vehicular management system over cloud edge computing.

vehicular systems [9–11]. Consumer 6G products have already started to emerge, and companies will begun to provide 6G wireless solutions for residential usage [12–14]. Thus, 6G can offer support for the full implementation of a vehicular system through a Wi-Fi access point. The problem of faster response times, power reduction, and downloading and uploading without interruption can successfully be addressed with 6G. Thus, an accident can be avoided, and reliable communication can be preserved. The efficiency and safety of a vehicular system can be increased by improving the operations of IoT devices in traffic management systems [8,15,16]. A standard vehicular management system uses static signaling times at junctures and does not give priority to emergency vehicles (e.g., ambulances, police cars, firefighters), possibly leading to property damage, life loss, pollution, increased fuel costs, and congestion [17,18]. The deployment of IoT devices with 6G can manage vehicular systems effectively during emergencies and dangers, and can facilitate cutting-edge technologies and communication processes for the design and development of applications to smart vehicular management systems. IoT-enabled devices can monitor vehicles in a given area, and using different devices (e.g., sensors) can quantify numerous physical traffic factors, such as density, flow, headway, volume, throughput, waiting time, and pollution. [19]. Using 6G with IoT devices reduces energy consumption because IoT devices do not consume a lot of energy relative to other non-IoT devices (e.g., base stations). As soon as vehicle drivers turn on a light, the IoT-enabled device begins to transmit signals, and the power consumption of 6G will be less than that of Wi-Fi [20]. Most significantly, when multiple devices are connected to the Internet concurrently, wireless transmission speeds are not affected, allowing IoT devices to transfer large amounts of data successfully [21–24]. Vehicular management systems are prone to security loopholes due to wireless network susceptibilities; the privacy and security issues of IoT-enabled devices; transmission failure; transmission interruption; and transmission snooping problems that markedly affect network performance. All of these outstanding problems must be solved before smart vehicular management systems become feasible. Addressing these issues, blockchain technology with 6G could be a potential solution.

The use of consortium blockchain in vehicular management systems provides transparency and addresses the issues of IoT devices by providing certifiable and unchangeable messages of any action that occurs. The consortium blockchain can mitigate transmission snooping and transmission interruption using cryptographic features. Conversely, blockchain technology has an additional overhead that can be addressed using 6G and edge cloud computing [25]. An algorithm for detecting vehicles and pedestrians is used, which uses semi-precision acceleration and lightweight YOLOv3-promote characteristics to provide real-time detection [26]. A decentralized integrity of data audit approach based on blockchain is intended to improve security and efficiency [27]. A novel Blockchain-enabled Large-scale Parked Vehicular Computing architecture has been presented to better utilize energy efficiency and vehicular computational resources [28].

Some existing vehicular management systems use wireless networks with the support of IoT devices to achieve smooth communication. However, coverage, communication cost, and faster traffic incident notification issues are not fully be addressed [29, 30]. Existing vehicle management systems rely on IoT devices for efficient communication. However, connectivity, coverage, communication costs, and speedier traffic incident response challenges remain unresolved [31,32]. Conversely, 6G can resolve the problem of connectivity and coverage to guarantee effective resource management for IoT devices. The communication cost and faster traffic incident notification can also be achieved with 6G. A reputation-based blockchain-enabled vehicular system has been studied with regard to security and privacy preservation [33]. However, that system experienced a lack of management of the vehicles and additional communication overhead [34].

An energy-efficient blockchain-enabled heterogeneous 6G-supported network for vehicular management systems over edge cloud computing has been proposed shown in Fig. 1. The proposed EBH includes modeling of edge computing, consortium blockchain, and 6G heterogeneity. Together, these cutting-edge technologies tackle the problems of energy efficiency, latency, and secure data sharing. For successful data sharing, a consortium blockchain-enabled privacy-preserving model is used, which increases scalability and offers quick delivery, security, and automation. The vehicle energy efficiency and latency are managed by the 6G heterogeneity. New features like logical radio frequencies (LRF), load balancing, and dynamic load balancing are added to the heterogeneity. Edge computing modeling determines the edge computer's power gain, instantaneous transmission rate, and local delay, which improves energy efficiency and reduces latency. Furthermore, the consortium's blockchain-enabled privacy-preserving model is critical for addressing transmission interruption and snooping issues. The use of the consortium blockchain is motivated by the desire to give control to a single party, but it is immune to monopoly. If all members agree, this control allows each member to define their own rules, review or cancel fictitious transactions, modify balances, and take other measures to foster beneficial cooperation for vehicles with a common goal. The consortium enjoys greater privacy. As a result, the vehicles can gain more trust and confidence.

1.1. Research contribution

The primary contributions of the article are summarized as follows:

- The 6G heterogeneity formulation is introduced for vehicular management. This heterogeneity formulation includes logical radio frequencies (RF), load balancing, and dynamic load balancing as new features. To support IoT devices in most urban areas, the logical RF network is used to prevent interference with 6G signals. Logical RF can cover a large number of 6G access points. As a result, IoT and consortium blockchain provisions have been established. If an IoT device's connection is unstable due to a loss of a 6G connection, a Wi-Fi access point is added to continue a steady connection. The threshold value is set in the 6G network through a threshold detector, and access points that are higher than the set threshold value are used for coverage. As a result, data loss is reduced. Due to the random deployment of many IoT devices, the integration of the dynamic load-balancing feature is employed to handle the backhaul in a 6G network for dealing with all vehicles. If vehicles receive poor signals from the micro base station. Vehicles, on the other hand, may benefit from improved services from nearby small cells via the consistent wireless backhaul. This 6G heterogeneity improves energy efficiency and lower latency.
- Edge computing is modeled to determine the power gain, instantaneous transmission rate, and local delay of the edge computer, which supports energy efficiency and reduces latency.
- The privacy preservation model is used in conjunction with consortium blockchain to deal with the vehicle compromise process. As a result, security is ensured by addressing issues such as transmission interruption, transmission failure, and transmission snooping. Furthermore, vehicle users are validated when communication is established, which leads to successful data sharing.

1.2. Paper organization

The remainder of this paper is organized as follows. Section 2 reviews the relevant literature. Section 3 presents the modeling of edge computing for vehicular management. The 6G heterogeneity formulation for the vehicle is discussed in Section 4. The proposed consortium blockchain-enabled privacy-preservation model is discussed in Section 5. Experimental results are provided in Section 6, and finally, the paper is concluded in Section 7.

2. Relevant literature

This section discusses the characteristics of previously proposed approaches that are closely related to the proposed method. Table 1 shows a summary of the contributions of the previously proposed solutions. A novel blockchain conditional privacy-preserving authentication protocol was introduced by Lin et al. [35] to address security and privacy issues in vehicular ad hoc networks. The proposed approach uses public key infrastructure (PKI) and blockchain to acquire secure communication in vehicular ad hoc networks (VANETs). Thus, storing a considerable amount of private keys by participating vehicles could be reduced. Additionally, the proposed method uses a modified version of the elliptic curve digital signature algorithm (ECDSA) to minimize the required time to verify participants. The authors implemented their approach in an Ethereum test network known as Rinkeby and simulated their vehicular network architecture using NS-2 and VanetMobiSim. However, the resulting computational latency was high.

An edge computing-based protocol was proposed by Rasheed et al. [32] to preserve privacy in vehicular networks. The authors introduced an improved type of certificate-less aggregation sign-cryption scheme to ensure the security of edge computing. Additionally, the proposed solution used an information transmission protocol to subedit the road monitoring network traffic. This protocol provides various security requirements to participants in vehicular networks, such as privacy, anonymity, integrity, confidentiality, and joint authentication. The proposed method was tested and compared with other related work and demonstrated its validity for 5G-vehicular-to-everything (V2X) networks in terms of communication overhead, computational cost, and security analysis.

A secure peer-to-peer (P2P) data sharing technique based on consortium blockchain technology was developed by Kang et al. [33] to be deployed in vehicular networks. The authors used consortium blockchain because it could create distributed and shared databases of several preselected network entities with minimum cost. The preselected network entities were roadside units (RSUs) that were used to store public auditing shared data. Smart contracts (i.e., executable scripts existing on blockchain used to permit the automation of distributed multistep operations) were used to implement efficient vehicular data management blueprints. These smart contract blueprints can also be used to prevent unauthorized secondhand data sharing. Last, the authors improved the data credibility using a three-weight subjective logic (TWSL) model that is capable of selecting a more reliable data source and eventually constructing a reputation-based data sharing technique.

To reduce energy consumption and latency in 5G wireless networks, Lai et al. [30] proposed computational task offloading using edge computing. The authors used a UAV to eavesdrop on a secure communication channel that resided between the user and the computational access point (CAP). The goal of this approach was to improve the physical layer security and reduce the energy consumption and latency in both computation and communication. To measure the cost of the system, the authors developed a multi-objective optimization problem from mobile edge networks (MECs) and then used a linear energy consumption and latency combination. Additionally, an adaptive offloading approach based on deep reinforcement learning (DRL), a deep Q-network (DQN) in particular, was used to automatically address the optimization issue by establishing the system state, action, and reward function.

Table 1
Summary of existing techniques contributions.

Method	Description	Blockchain	MEC	Cellular/6G	Features/Characteristics	Limitations
[32]	Introduced a privacy-preserving method targeting VANET and utilizing 6G-based edge computing		✓	✓	Provides several security requirements to clients including anonymity, integrity, privacy, confidentiality, and joint authentication	Claimed to accomplish many security requirements such as privacy, anonymity, integrity, confidentiality, and joint authentication but failed to fulfill all of the requirements. The approach just achieved partial privacy of users but not data.
[30]	Proposed a deep reinforcement learning to address the optimization issue in 6G networks		✓	✓	Energy-efficient and secure approach capable of reducing energy consumption and improving physical layer security	Consumed an additional bandwidth and there is the possibility of data loss.
[33]	Presented a secure peer-to-peer data sharing method based on Blockchain	✓	✓		Implement an efficient vehicular data management blueprints, prevent unauthorized second-hand data sharing, construct a reputation-based data sharing	Restricted only to secondhand data sharing and increased latency.
[35]	Proposed a blockchain conditional privacy-preserving authentication protocol	✓			Storing huge amount of private keys can be reduced and the required time to verify clients can be minimized	Increased latency and used an elliptic curve digital signature algorithm, which adds complexity to secure implementation primarily with standard curves.
[36]	Presented a privacy-preserving pseudonym management technique	✓	✓		Preserves communication system location privacy, decreases pseudonym generation, and reduces management cost	Attempted to secure the data privacy but increased latency and time complexity
Ours	Introduced a perspective architecture for the IoT-enabled secure vehicular system utilizing consortium blockchain-enabled heterogeneous 6G network over the cloud edge computing	✓	✓	✓	Improve the energy efficiency and lower latency, obtain 6G network connectivity for secure vehicular management system and ensures data transmission process of the vehicles could not be compromised by attackers	The power of consensus is limited to the vehicles.

The adaptive offloading technique integrated both the transmit power allocation among users and wireless bandwidth allocation. The proposed approach was evaluated in MEC networks and compared with other related approaches, which demonstrated its effectiveness in terms of efficient power consumption and latency.

A privacy-preserving pseudonym management framework was introduced by Bao et al. [36]. This framework used blockchain as a first contributor and then a pseudonym certificate shuffling scheme to preserve vehicular communication system (VCS) location privacy and decrease pseudonym generation and management costs. To reduce the computational complexity that RSUs face and improve network robustness, the authors proposed a decentralized privacy manager (PM) that could be deployed as a multiaccess edge computing (MEC) network entity. The pseudonym shuffle path was protected by blockchain transactions encrypted with public key cryptography. Each transaction was marked with the PM's private key and then encrypted with the recipient PM's public key. As a result, other PMs or attackers could not read transactions in transit.

3. Modeling of edge computing for vehicular management

Edge computing is a distributed information technology paradigm in which client data is processed as close to the source as is practical at the network's edge. All current autonomous vehicles use edge computing, frequently trained using machine learning models from data centers. The incredible computing power of contemporary data centers with hundreds of petaflops of processing power makes autonomous vehicle feasible. To support the increasingly complex software being installed in automobiles, edge computing and 6G are being investigated and adopted within the automotive industry [37]. Together, 6G and edge computing can deliver high bandwidth with low latency safely and dependably. Edge computing reduces computing latency by utilizing the computing power in edge devices like base stations and access points. One of the main problems with edge computing is figuring out the mechanisms for computing task offloading. To further cut down on computation time for secure vehicular management, edge computing may be necessary. Fig. 2 illustrates how edge computing aids in vehicle management. If cloud computing is unable to

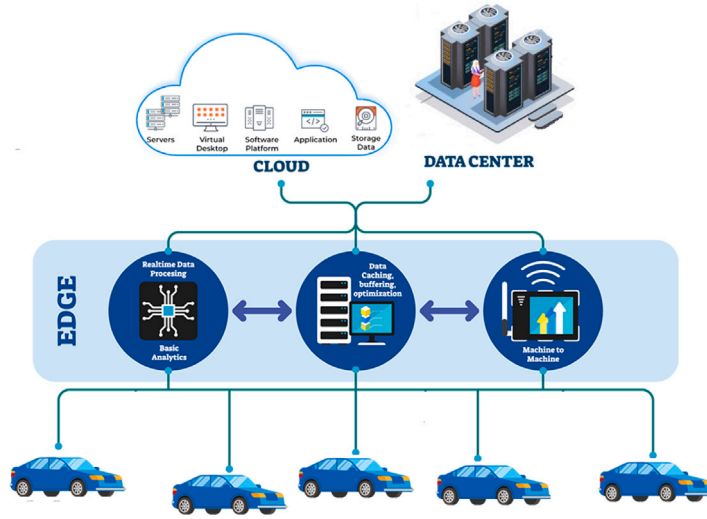


Fig. 2. The role of edge computing in vehicle management.

establish a connection with the vehicle after a service session, vehicle-to-vehicle communication is used to transmit the computing result. Edge computing is a new paradigm that offers quick and energy-efficient computing services for vehicle users to get around cloud computing's limitations. Resource-constrained vehicle users are permitted to offload their computationally intensive tasks to highly capable edge servers co-located with roadside units via vehicle-to-infrastructure. There are numerous roadside units situated along the highway to provide services for the vehicles on the road. Additionally, it is assumed that vehicle users will use orthogonal channels to transmit information, preventing any interfering activity. As a result, the distance between the vehicle users and the base station has a major impact on the transmission performance between them. As a result, we apply the same channel model here as in [38]. The optimal solution found in this article can be used as a performance benchmark despite the channel model's simplicity.

Let us assume that P_g be power gain between channels and P_c is the power channel at the distance $r_0 = 1$ and σ is a path-loss component.

$$P_g = P_c r_o(t)^{(-\sigma)} = \frac{P_c}{\{BS_h^2 + R^2 + (l + vt)^2\}Z^\sigma} \quad (1)$$

Where R represents distance between the highway and the base station. BS_h is the height of the base station. Additionally, the vehicle user travels unidirectionally at speed v along the highway starting at position $(l, 0, 0)$.

Let t_p and φ^2 represent the transmission power and noise power for the vehicle user respectively. Therefore, instantaneous transmission rate I_r between base station and vehicle user can be obtained as

$$I_r = C_b \log_2 \left(1 + \frac{t_p P_g}{\varphi^2} \right) \quad (2)$$

Where C_b is the bandwidth of channel. The messaging task is alienated into two portions: $(1 - O_R)\Delta I_d$ bits for the local computing and $O_R L$ bits for edge computing. Thus, local delay of the edge computer E_{ld} can be computed as

$$E_{ld} = \frac{(1 - O_R)\Delta I_d}{L_f} \quad (3)$$

Where ΔI_d is the input data size, I_C is the computational intensity, O_R is an offloading ratio, and L_f is the local frequency of the CPU. The energy consumption for the edge computing E_{ec} can be calculated as

$$E_{ec} = \epsilon L_f^3 \Delta I_d = (\epsilon \Delta I_d \cdot I_C \cdot L_f^2 (1 - O_R) \Delta I_d) \quad (4)$$

Where ϵ is an active switched capacitance.

Hence, offloading computation and edge computing occur simultaneously, and the latency of the vehicle V_i to complete the entire task can be determined by

$$V_i = \max(E_{ld}, L_{co}) = \max \left(\frac{(1 - O_R)\Delta I_d}{L_f}, T_r + \frac{O_R \Delta I_d}{C_{c+e}} \right) \quad (5)$$

where L_{co} is the computing latency, M_u is the uploading messaging data, and $C_{(c+e)}$ is the computational capability of the edge. The energy consumed E_c by edge computing to send the message to vehicle users can be calculated as

$$E_c = E_{ec} + M_u = (\epsilon \Delta I_d \cdot I_C \cdot L_f^2 (1 - O_R) \Delta I_d) + P_g \cdot T_r \quad (6)$$

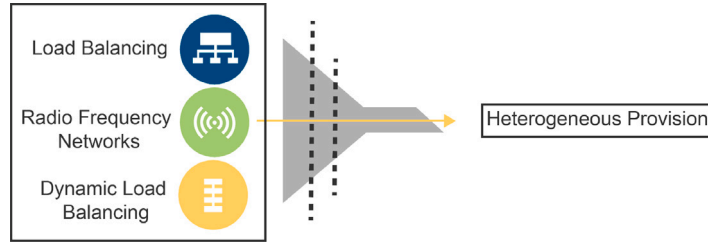


Fig. 3. Characteristics of 6G heterogeneity provision.

The role of edge computing is to minimize the computational overhead caused by computation and communication. Thus, the computational overhead is demarcated as the weight of the energy consumption WE_c and weighted sum of the latency WV_t . Therefore, effective vehicular management is achieved through the deployment of edge computing that is given by

$$\min p_g = (O_R \cdot T_r) + L_f(W E_c + W V_t) \quad (7)$$

4. 6G heterogeneity formulation for vehicles

Wireless fidelity (Wi-Fi) has become popular worldwide but experiences problems due to volatility of wireless signals, overhead, and slow internet access [39]. Wireless network communication primarily uses electromagnetic waves that have limitations, demonstrating that it cannot fulfill the growing demand for data communication. There are hundreds of thousands of base stations (BSs) that consume energy for communication services. Currently, emerging 6G technology solves the problems of energy efficiency, latency, slower communication, connectivity, and coverage. However, 6G lacks penetration ability that results in a lower data communication rate in cases of blurred or dim light near the 6G access point. Light from sources (bulbs) to vehicles can be reachable; however, vehicle mobility may result in connection loss or lower data rates. This problem can be managed with emerging technologies and 6G to create a heterogeneous network shown in Fig. 3.

4.1. Radio Frequency (RF) networks

The logical RF network should be integrated with 6G, which has the potential not to interfere with 6G signals. The best type of RF integrates Wi-Fi with 6G because Wi-Fi is widely used and implemented in most urban areas to provide support for IoT devices. This integration can cover a large area. Thus, a single Wi-Fi access point can cover several 6G access points. This heterogeneous provision is ideal for vehicles and can efficiently support IoT and consortium blockchain technology. A smaller number of RF chains can adequately reduce the energy consumption and hardware cost. Thus, heterogeneous beamforming is critical to the success of 5G that could be addressed with introduction of 6G. Thus, maintaining an efficient end-to-end delay, the heterogeneous beam-forming problem should be formulated and given by:

$$\begin{aligned} (A_\gamma, D_\gamma) &= \|F_{db} - A_\gamma D_\gamma\|_F \\ \text{Subject to } &\begin{cases} \|(A_\gamma(i, j))\| \leq 2, \\ \|(A_\gamma, D_\gamma)\|_{S_c}^2 \leq U D_{st} S_c. \end{cases} \end{aligned} \quad (8)$$

where (A_γ, D_γ) : Analogue and digital components for heterogeneity; D_{st} : Data streams for sending and receiving among the vehicles; S_c : subcarrier for sending additional information; and F_{db} : Combined fully digital heterogeneous beamforming.

The optimized heterogeneity H_{op} beamforming for the RF is determined as:

$$H_{op} = Z_{ne} \sum_{i \in \omega} \|\Delta h d - (x_i, y_i)\|^2 \quad (9)$$

where Z_{ne} : Non-zero element; (x_i, y_j) : objective function in optimized heterogeneity; and fully digital heterogeneous component. Where Z_{ne} : Non-zero element; (x_i, y_j) : objective function in optimized heterogeneity; and $\Delta h d$: fully digital heterogeneous component.

The efficiency of the spectrum's links E_{sl} for the number of vehicles V_n can be determined as:

$$\begin{aligned} E_{sl}(V_n) &= \log_2 \left(1 + \frac{q' RF_{ms} H_{ms} (H_{ms}) \tilde{RF}_{ms} \tilde{q}'}{\sum_{i=1, i \neq V_n}^{V_n} q' RF_{ms} H_{ms} (H_{ms}) \tilde{RF}_{ms} \tilde{q}' + \lambda_{pa}^2} \right) \end{aligned} \quad (10)$$

where q' : Downlink channel between the Base station (BS) and the number of the vehicles; RF_{ms} : RF beamforming generation support for the multi-stream; H_{ms} : optimization of the beamforming generation support for the heterogeneous multi-stream; $(H_{ms}) \tilde{}$: optimized downlink channel for the support of heterogeneous multi-stream; $(RF_{ms}) \tilde{}$: downlink channel for the multi-stream; and λ_{pa} : Power amplifier efficiency.

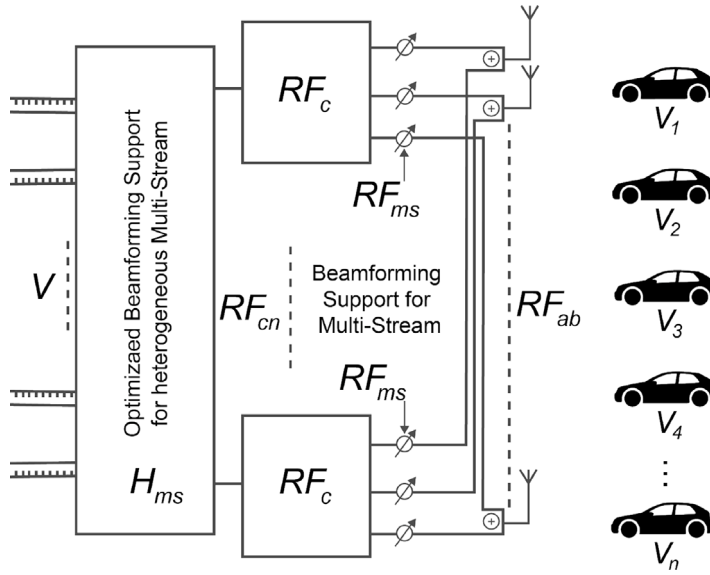


Fig. 4. Multiple-vehicle scenario without a loss of generality.

The energy efficiency of the BS can be maximized with the optimization of H_{ms} , RF_{ms} , and RF_c . Thus, the optimization problem is formulated as:

$$Opt(H_{ms}, RF_{pc}, RF_c) = \frac{B_t \times S_e}{BS_{ae}} \quad (11)$$

such that $[\{RF_{pc}\}_{i,j}]^2 = RF_{ap}$.

Without a loss of generality, the multiple-vehicle scenario is generated, as shown in Fig. 4.

The efficiency of the spectrum can be described by:

$$S_e = \sum_{V=1}^{V_n} E_{sl} \quad (12)$$

The aggregate power of the BS is given by:

$$BS_{ae} = \frac{1}{\lambda_{pa}} \sum_{v=1}^{V_n} \|RF_{ms} H_{ms}\|^2 + RF_c \cdot RF_c \cdot RF_{pc} + \forall \Psi \quad (13)$$

where B_t : transmission bandwidth; S_e : spectrum efficiency; BS_{ae} : aggregate energy of the BS; RF_{pc} : power consumption at each RF chain; and $\forall \Psi$: power consumption for synchronization, baseband processing and site cooling for BS to support 6G.

The RF precoding amplitude RF_{ap} is held constant and is included in Eq. (14). Also, each vehicle requires a minimum data rate for communication, which can be determined by multiplying the bandwidth and the minimum spectrum efficiency, where the bandwidth is also held constant. Therefore, the corresponding minimum spectrum efficiency limitation is used to fulfill the requirement for the minimum data rate, which is given by:

$$(E_{sl}) \geq S_{me}, V = 1, 2, \dots, V_n \\ \& \sum_{v=1}^{V_n} \|RF_{ms} H_{ms}\|^2 \leq TP_{max} \quad (14)$$

where (E_{sl}) : Efficiency of the spectrum's link to manage the number of vehicles; S_{me} : Minimum efficiency of a spectrum; V : Vehicle; and TP_{max} : Maximum transmit power of 6G.

4.2. Load-balancing

We consider that the scenario where several 6G access points are not connected with an area that they cover. Because they are not linked, traveling between congested areas or larger obstacles results in connection loss. A Wi-Fi access point must be added to connect the networks, and Wi-Fi must choose the connection when 6G loses connection. The threshold should be set in the 6G area and permit access points that are higher than the set threshold value for coverage when moving. As soon as the vehicles reach a lower threshold than the set threshold, Wi-Fi should connect the vehicle with 6G areas that have an appropriate threshold value, thus mitigating data loss. The probability of identifying a stable process of 6G area selection via Wi-Fi can be expressed as:

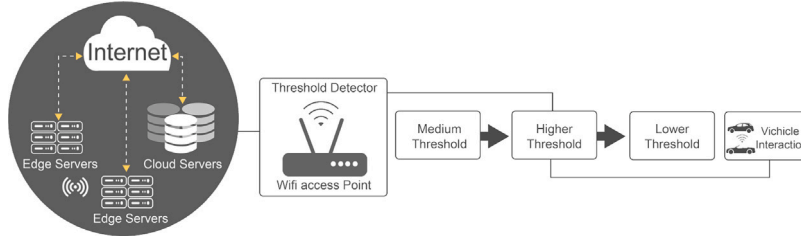


Fig. 5. Load-balancing process of 6G area networks.

Assuming that the output value of the threshold is evenly distributed over its entire range of 6G, and that the predicted value has m bits, then the threshold value has $n = m^2$ possible outputs. For any 6G access point k , which should be less than the total number of 6G and wireless access points as ($k \leq n$), the probability p of identifying a lower threshold of 6G can be calculated by:

$$\begin{aligned}
 p(n, k) &= 1 - \frac{n!}{(n-k)! \times n^k} \\
 p(n, k) &= 1 - \left[\left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) \right] \\
 p(n, k) &= 1 - \prod_{i=1}^{k-1} \left(1 - \frac{i}{n}\right) \approx 1 - \Pi \\
 p(n, k) &= 1 - e^{-\left(\frac{k(k-1)}{2n}\right)}
 \end{aligned} \tag{15}$$

Based on Eq. (8), and provided that the threshold value has an output of m bits, only $k = 2^{m/2}$ attempts will lead to a lower threshold with a probability of at least 50% given in Eq. (16):

$$\begin{aligned}
 P_0 &= 1, \lim_{Z \rightarrow \infty} P_Z = 0 \\
 C_Z &= P_Z + 1, r = \frac{q}{p}
 \end{aligned} \tag{16}$$

A vehicle can obtain strong 6G signals with the probability q , and p_l is the lower 6G signal, which leads to data loss. Initially, a vehicle is at point $x = z$; then, there will be no 6G signals, and the vehicle will stop. If it reaches $x = 0$. Therefore, the probability of 6G detection is successful at saving γ :

$$\gamma = \frac{nq}{p_l} \tag{17}$$

Fig. 5 shows that a higher threshold value provides maximum signals of 6G; a medium threshold value produces the average signals, which are sufficient for communication; and a lower threshold value could lead to data loss. Thus, the Wi-Fi access point is used to detect the threshold value of obtaining lower signals.

4.3. Dynamic load-balancing

Data rates primarily remain variable for many reasons. The differences in spreading 6G signals between vehicles are markedly different due to mobility. To prevent this issue, the vehicle's connection must be monitored, and if it drops below the set threshold, the connection will switch from a 6G access point to a wireless network access point. Fig. 6 shows the visual representation of how this process would function in reality.

The dynamic load-balancing backhaul in a 6G heterogeneous network faces a new problem due to self-backhauled small cells (SSCs). Therefore, the micro base station (MBS) does not work well with all vehicles due to the random deployment of many IoT devices and mobile phones. Thus, vehicles may obtain poor signals from further MBSs. Conversely, vehicles may obtain better services from adjacent small cells through a consistent wireless backhaul (WB) that consists of a robust single beam from the multiple received antennas of 6G or macro base station (MBS), as shown in Fig. 7. The MBS consists of uniformly deployed full duplex small cells (SCs), which serve a number of vehicles V_n with the connectivity of the single vehicle device (SVD) and macrovehicle device (MVD). Let us assume that open access policy at full duplex SCs is equipped with a number of antennas $A_{(n+1)}$, where a single antenna supports the wireless backhaul, and the transmitting antenna serves the SVD and MVD with the same frequency bandwidth. The challenge of vehicle scheduling V_s and vehicle association V_a should be addressed for dynamic load balancing. Thus, the MBS should provide data transmission concurrently to wireless backhaul and MVD to support full-duplex SCs. Thus, full-duplex SCs should have the capability to serve both SVD and MVD. If we take T_p^a and T_p^b as transmission pointers from the MBS to serve the SVD and MVD, the dynamic load-balancing constraints β_{ω} are given by:

$$\beta_{\omega} = \sum_{Sc=0}^{SCt} T_p^a \leq 1, \sum_{mc}^{Mct} T_p^a + T_p^b \leq V_{n(a)}, \forall Sc, mc \in V_n \tag{18}$$

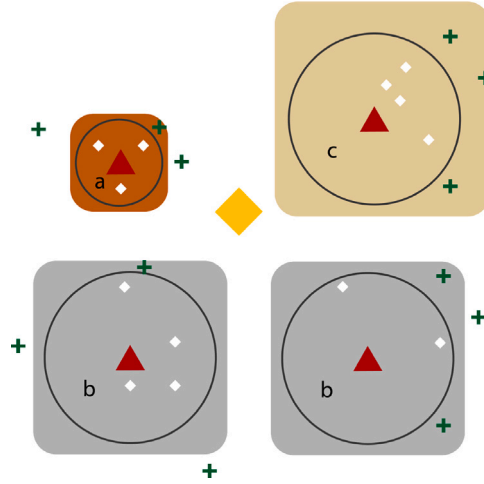


Fig. 6. 6G + Wi-Fi hybrid network. The yellow diamond represents the Wi-Fi access point. The rings inside of the 6G coverage represent the threshold for switching between the two networks. The green four-point stars represent vehicles connected to the network via Wi-Fi, and the white diamonds represent vehicles connected via 6G.

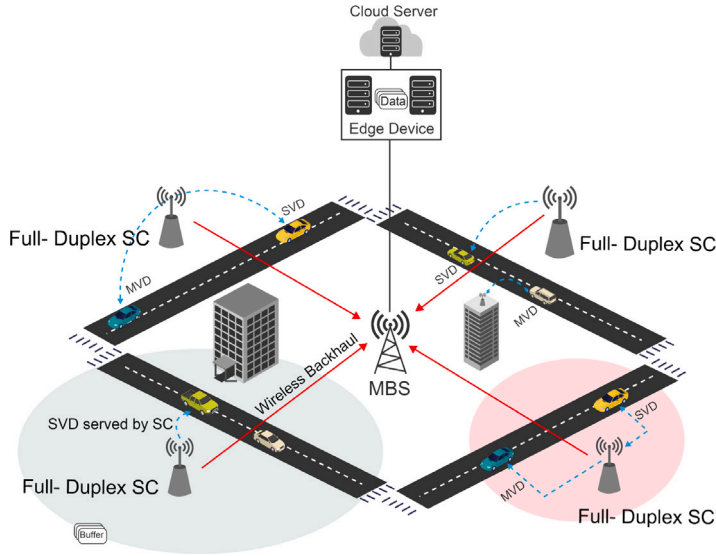


Fig. 7. Unified access and wireless backhaul architecture for 6G heterogeneous networks.

where $V_{n(a)}$: The number of active vehicles; mc : macro cells; Mct : Total number of macro cells; Sc : Small cells; SCt : Total number of small cells.

Let $SCt_{(Tx)} = T_p^a + T_p^b$ be the total number of small transmitting cells at the SCs, and thus Eq. (18) becomes $SCt_{(Tx)} \leq V_{n(a)}, \forall Sc \in V_n$.

Assuming that each full-duplex small cell Fd_c^S functions as a relay to transmit data to its corresponding vehicles, the data transmission process of Fd_c^S will be deactivated if the 6G-enabled MBS forwards data to Fd_c^S . Thus, the Fd_c^S cannot serve its SVD. Therefore, data buffering at the SCs and wireless backhaul at Fd_c^S during each time slot t_{sl} can be written as:

$$Db_{sc}(t_{sl} + 1) = \text{Max} \left\{ Db_{sc}(t_{sl}) + \right. \\ \left. Mct(t_{sl}) - D_{s_{t_{sl}}}^{Bs}, 0 \right\}, \forall Sc \in SCt \quad (19)$$

where Db_{sc} : Data buffering at the small cell; D_s^r : Data transmission rate at small cell; $D_{s_{t_{sl}}}^{Bs}$: Total data rate of the base station to serve all of the small cells during the time slot.

Small cells can offload some MVD from the MBS if the WB capability between the MBS and SCs is assured. Thus, each SC can set WB condition for all $t_{sl} \geq 0$. If the access link between the MBS and MVD is stable and considered better than the connection between the SCs and MVD, then the MVD is connected with the MBS instead of another SCs:

$$\begin{aligned} & \text{if } (D'_s) + Mct(t_{sl}) \geq D'_{mc_{sl}}^{BS}, \\ & \text{then } t_{sl}^{BS} = 0, \forall Sc \in SCt, mc \in V \end{aligned} \quad (20)$$

where t_{sl}^{BS} : Time slot from the MBS to macrocells; and $D'_{mc_{sl}}^{BS}$: Data transfer from the MBS to macrocells during the time slot.

Definition 1 (Buffer Constancy). For buffer B over time slots $t_{sl} \in \{0, 1, \dots, \infty\}$ and $B \in \mathbb{Z}_+$. Thus, B is consistent. If $\bar{B} \triangleq \infty \frac{1}{t_{sl}} \sum_{\sigma=0}^{t_{sl}} Q[|B\{\sigma\}|] < \infty$. Thus, a buffer network is consistent if each buffer is consistent.

5. Consortium blockchain-enabled privacy preservation model

Authorized vehicles use a consortium blockchain to maintain distributed shared databases depicted in Fig. 8. A blockchain consortium aims to develop a unified and secure peer-to-peer (P2P) privacy preservation model. In this article, the consortium blockchain aims to reduce latency while providing data privacy preservation (PP). Because it allows for rapid data delivery between vehicles. A consortium blockchain with use of 6G can greatly support IoT devices (e.g., transmission interruption, transmission failure, and transmission snooping). Communication between legitimate vehicles is confirmed using blockchain-enabled servers, and vehicle users must be validated when establishing communication because an attacker could use resources maliciously to capture the legitimate messaging process. As a result, vehicle users' identities and data are authorized. Key operations of the consortium blockchain-enabled PP model are given below:

- Initialization Process
- Privacy preservation trading roles
- Privacy preservation validation server
- proof-of-luck of PP
- Block authenticity
- Consensus process

1. **Initialization Process** In consortium blockchain-enabled PP, we employ a secure Boneh-Boyen short signature for the initialization process of the PP model. After completion of the registration process, each vehicle becomes an authentic entity. An authentic vehicle V_a with true identity IDV_a joins the consortium blockchain-enabled PP system for getting public PuK_{V_a} and private keys PrK_{V_a} and certificate C_{er} . The certificates are used to identify the authentic vehicles through requisite registration process of authentic vehicle. The authentic vehicle V_a gets set of wa wallet addresses $W \times IDV_a, kWk = 1$ from the relevant authority. The authority is responsible to map the list $IDV_a, PuK_{(V_a)}, PrK_{(V_a)}, C_{er}, W \times IDV_a, kWk = 1$ and stores the given list in vehicle pools. When a vehicle performs the initialization process, the vehicle uploads its address to the pool of nearest privacy preservation aggregator (PPA). The vehicle examines the integrity of the wallet and downloads current data about the wallet from the storage pool in PPA. The storage pool stores all communication messages in the PP consortium blockchain. The PPA server monitors the registered vehicles. The monitoring stability process should be accomplished. Let P_t be the storage pool and V_r is the number of the registered vehicles at time t . Given specific time $t = \{1, 2, 3, \dots, n\}$ the goal is to ensure the monitoring stability process M_γ , which can be determined as follows:

$$M_\gamma = \sum_{i=1}^n \left(d_p P_t \right)^2 + \left(\Psi_w d V_r \right)^2 \quad (21)$$

where d_p denotes the decentralized process, Ψ_w represents the proportionate weight assigned to the trade-off between authentic vehicles and registration process.

2. **Privacy preservation trading roles:** PP vehicles pick their roles according to current PP status. The PP vehicles with the legitimate role may become authenticator vehicle to meet the requirements of nearest vehicles that can be expressed as $V_1, V_2, \dots, V_n \in V_a$.

The PP trading roles employ a balancing token to keep the vehicles from being unpredictable. Every token functions consistently. Furthermore, real-time authentication is enabled by a common pattern that keeps the condition predictable.

The numbers of the tokens T_n increase as tokens are issued to vehicle for authentication process A_p , while it decreases when legitimate vehicles are not identified. Thus, increase in the token trading process $T_{ir} + 1$ is given by:

$$T_{ir} + 1 = \left(T_{ir} + A_p \right) - \left(\frac{A_t^p}{T_t^p + A_s^v} \right) \quad (22)$$

where A_t^p denotes the token issuing authority that is responsible to issue token for authentication, A_t^p is total time for requesting the token, and A_s^v is the authentication server that takes time to issue the token.

3. **Privacy preservation validation server:** The authentic vehicle requests that the PPA's authentic server broadcast its authenticity to other vehicles. The PPA serves as the controller for all authenticated vehicles' records. When the broadcasted messages reach the authenticated vehicles, they respond with their authenticity. The PPA verifies the legitimacy of the vehicles that responded. When the vehicles' authenticity is confirmed, the PPA broadcasts a list of all authenticated vehicles. As a result, the vehicles can communicate with authenticated vehicles. Since the vehicles need to be authenticated before joining the consortium blockchain. The block S_t^b is analogous to the security parameters kept within it; it expands in proportion to the number of newly added cars and contracts in proportion to the drop in vehicles.

$$S_t^b + 1 = \left(S_t^b - A_p \right) + \left(\frac{A_t^p}{T_t^p + A_s^v} \right) \quad (23)$$

Blocks in transit must therefore be identified in order to avoid any potential threats.

Where D_t^i denoted the release of blocks at the given time.

The number of vehicles in the consortium blockchain technology C_b and the value of the block V_b are provided. Assuming that the block's release is proportional to the number of vehicles in the existing network at a given time. Assuming that release of the block is proportionate to the number of vehicles which are the part of the existing network at a specified time.

$$V_b = \left(\frac{B_t^r}{T_{tr}} \right) \quad (24)$$

Where B_t^r denotes the release of blocks at the given time.

4. **Proof-of-luck for privacy-preservation:** The proof-of-luck (PoL) method enables the vehicles to select the witnesses depending on their communication, which helps to conserve their energy. The majority of vehicles that take part in the communication and obtain the most votes can take control of the whole vehicular network. As a result, the chosen vehicles are awarded for participating in the validation process and building new blocks one at a time. The activity of block generation is moved to the next vehicle if a vehicle is unable to generate the block for which it has been assigned. And the other vehicles vote for a new vehicle (witness) to take its place. This method also solves the problem of latency. To select a leader vehicle, this method generates a trustworthy random number using the trusted execution environment (TEE) platform. It is safe because the TEE prohibits the attacker from controlling the CPUs and manipulating the blockchain. The vehicle is protected against the double-spending attack due to using the strong immunity of the PoL method.

Assume that the blockchain vehicle is attack-free and does not depreciate performance within a certain period. The attack-free environment provides a meaningful and relevant standard. Thus, take into account a certain period $0 \leq t < T$ and a brief window of time $(t, t + \Delta)$ from t to $t + \Delta$, $\Delta > 0$. We suppose that during this time, the communication among the vehicles V_{c_i} remains constant.

Let T_t^v be the certain amount of transactions for vehicle protection are initiated and transformed into secure blocks over the edge computer for the vehicles. As a result, the secured blocks for privacy preservation P_{pb} can be determined as follows:

$$P_{pb} = 1 + \left(\frac{T_t^v}{B_n} \right) \quad (25)$$

where B_n denotes the number of total secured blocks.

5. **Block authenticity:** PPA accumulates the information of all authentic vehicles which are registered and confirmed with registering servers in different locations during certain periods, then digitally sign the records of the vehicles to ensure the accuracy and authenticity. The vehicle records are arranged into blocks. Each block in the PP consortium blockchain comprises a cryptographic hash to the previous blocks for verification and traceability. The PPA looks for a legitimate proof-of-work for the record, much like Bitcoin does (i.e., a hash value providing a certain difficulty $D_{c\tau}$). The PPA determines the hash value of each block based on a random nonce value N_{rv} , the hash value of the previous block H_{pb} , the timestamp T_s , and the record's origin R_o .

Hash $(N_{rv} + H_{pb} + T_s) < D_{c\tau}$. Therefore, $D_{c\tau}$ can be accustomed by the PP model to rheostat the speed of determining the particular N_{rv} . After confirming a valid proof-of-work (i.e., N_{rv}), the faster authenticator in the (PPA) takes responsibility for broadcasting the block and the particular N_{rv} to another PPA. In response, another PPA checks and confirms the authentic records in the block and N_{rv} . If another PPA approves getting the block, data in an approved block is added in sequential order in the PP consortium blockchain, and the fastest authenticator is awarded the PP certification.

The vehicle's authenticity is an important, which is attained by utilizing PP consortium blockchain for threat avoidance because it serves as a protection for the vehicle communication network. To do this, smart contracts are dynamically distributed across blockchain-enabled vehicles. This is performed through the use of a time-varying parameter $\beta(t)$ ranging between 0 and 1:

As a result, the authentication procedure at the given time $A_u(t)$ can be computed as follows:

$$A_u(t) = U_r(t) \cdot \left(k_i(t) + R_c \cdot R - e(t) \cdot \beta(t) \right) \quad (26)$$

$$N_{br}(t) = R_c \cdot R - e(t) \cdot \left(1 - \beta(t) \right) - k_i(t) \quad (27)$$

where $k_i(t)$ denotes the key issuing time, R_c is an average collateral ratio, $R - e(t)$ represents reward-earning vehicle to get faster authentication, F is a function that grows indefinitely.

The modification of time-varying parameter $\beta(t)$ becomes compatible to the key issuing process $k_i(t)$ that is of paramount significance to the stable system. The consortium blockchain technology for balanced PP for accurate authentication process $PP_a(t)$ can be determined as follows:

$$PP_a(t) = \Omega \left(\frac{k_i(t)}{A_u(t)} \right) \beta(t) \quad (28)$$

where Ω is a monotonically increasing concave function

6. **Consensus process:** Authorized PPA and a leader that is the quickest PPA with a valid proof-of-work carry out the consensus process. To enable auditing and confirmation, the leader broadcasts block data, timestamps, and its proof-of-luck to other authorized PPAs. These PPAs audit the block and broadcast their audit evidence with their signatures to one another for mutual supervision and confirmation. Each PPA reviews its results in comparison to those of the others after receiving the audit results, then responds to the leader. The audit evidence, signatures, comparison result, and records of received audit results provided by the PPA make up this response. The leader assesses the PPAs' responses after receiving them. The leader will send records containing up-to-date audited block data and a conforming signature to all authorized PPAs for storage if all PPAs concur on the block data. The block is then saved in the consortium blockchain, and the leader is recognized with a PPA award. If some PPAs disagree with the block data, its leader will review the audit findings and, if necessary, resend the block data to all these PPAs for audit. The PP blockchain has high stability and can handle a large number of IoT-enabled vehicles while maintaining network scale. Contrary to public blockchains, only a few authorized PPA are used in the PP blockchain's consensus process. The pre-defined vehicles are capable of scaling their computing and storage resources in accordance with the growth in the number of records as the vehicle network expands. When the formation of the authorized PPAs is complete and constant, the overall time required to reach a consensus on a new block is secure regardless of the vehicle network size. it is important to count the number of issued blocks for vehicles.

Let $M_c^t \Delta$ at $t + \Delta$ be the total number of blocks at given time with risk neutrality and rationality for the number of the vehicles V_t for authenticated of the vehicles V_a can be determined as follows:

$$V_a = \left(\frac{m_t^v + \Delta}{L_n \Delta} \times P_s \right) + \left(1 - P_s \right) P_t \Delta \quad (29)$$

The number of delegates in the blockchain technology, $m_t^v = M_c^t V_a$, can be used to determine the key-generating rate at $t + \Delta$ if the block counts at t do not match. The number of initial blocks in the network at the beginning of the time period $(t, t + \Delta)$ is m_t^v . The rapid increase in the number of blocks in the network is not something that the verified vehicles are willing to accept. There will be $M_c^t \Delta$ blocks in the process, and it will end at $t + \Delta$ with a success chance of P_s . With a success probability of $1 - P_s$, the run proceeds, and the total blocks at the beginning of the next time interval are $m_t^v + \Delta$.

Thus, the capacity of consortium blockchain technology to complete consensus process N_c^t can be calculated as follows:

$$N_c^t = \left(\gamma_t * m_t^v \Delta \right) + \left(1 - P_s \right) \quad (30)$$

An illustration of the privacy preservation model of malicious activities using consortium blockchain technology is shown in Fig. 9 and explained in algorithm 1.

Algorithm 1 shows the process of detecting a malicious message to identify malicious and non-malicious messages shared by vehicles using consortium blockchain technology. Step 1 initializes the variables, and the input and output are given at the beginning of the algorithm. In Step 2, vehicle-1 sends the message to vehicle-2. Once the message is broadcast, then the sniffing server primarily checks the authenticity of the vehicle's message. If a message-sending vehicle is legitimate, it provides an interface to send the message for the further process described in Step 3. The sniffer is not responsible for rejecting the messages at this stage. Step 4 decodes and analyzes the messages captured by the decoder, and the analyzed outcomes are stored on a consortium blockchain-enabled server. In Step 5, the function of message preprocessing is defined that converting the consortium blockchain technology messages into message formats required for mining, filtering, noise elimination, and known attacks detected by third-party detection tools. Step 6 describes the use of an anomaly analyzer on the messages. The anomaly detector determines new attacks using association analysis and sequence analysis and sends these abnormal behaviors to the rule base method. In Steps 7 and 8, the message is analyzed to detect the possibility of legitimacy/illegitimacy of the message. Thus, the message is compared with the log record. Two types of log records are kept: packet information produced by the known network (normal behavior traffic), and packet information produced by unknown intrusion behavior. There is a rule-based database that provides a message comparison process. The rule database involves intrusion detection rules, which provide a basis for misuse detection, which is used to match a known intrusion behavior with the library of intrusion rules. If an intrusion behavior is found directly, an alarm is sounded in Steps 9 and 10. If a non-malicious data block is detected, then miners (vehicular network) declare the message to be legitimate and add it to the network described in Step 11. In Steps 12 through 14, if a malicious message is detected, then it is added to the network. When the alarm deviates from the analyzer to report an abnormal behavior, the alarm sends a notice to the administrator through the human-machine interface.

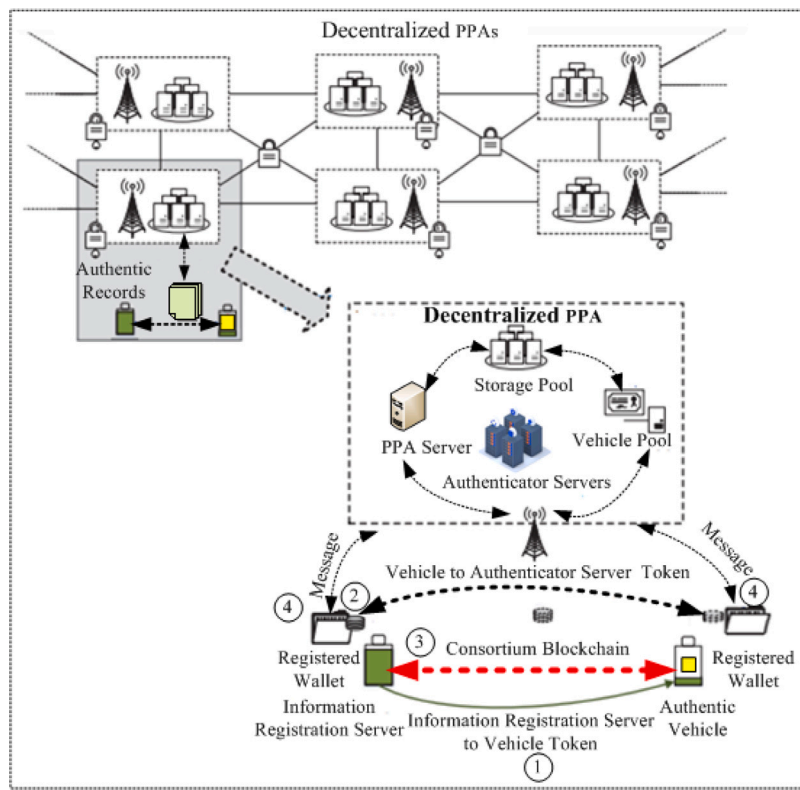


Fig. 8. Consortium blockchain-enabled privacy preservation model.

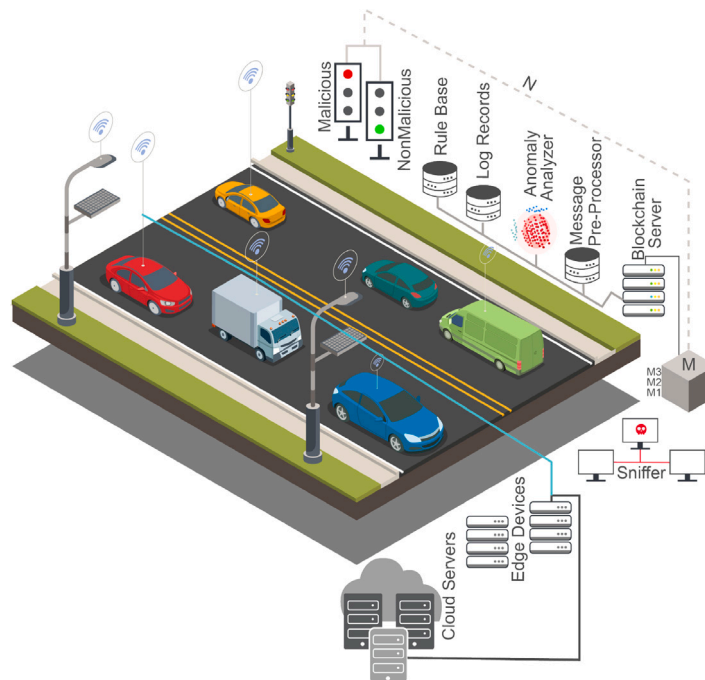


Fig. 9. Malicious detection rules using blockchain technology.

Algorithm 1 Malicious message detection process of vehicles**Input:** M in**Output:** MI ; NM out

```

1: Initialization:  $V_1$ : Vehicle-1;  $V_2$ : Vehicle-2;  $M$ : Message;  $S$ : Sniffer;  $D_e$ : Decoder;  $B_{cs}$ : Blockchain-enabled server;  $M_{pre}$ : Message Pre-processor;  $A_{ana}$ : Anomaly Analyzer;  $L_{rec}$ : Log Record;  $R_{ba}$ : Rule Base;  $A(M)$ : Accepting message;  $MI$ : Malicious;  $NM$ : Non-Malicious;  $M_i$ : Mines;  $AI$ : Alarm
2: Send  $V_1(M) \rightarrow V_2$ 
3:  $S$  collects  $M$  & provides  $I_{ia}$ 
4:  $D_e$  analyzes  $M$  & stores  $M \rightarrow B_{cs}$ 
5: Calculate  $M_{pre} \Leftrightarrow M \in B_{cs}$ 
6: Initiate  $A_{ana}$  on  $M$ 
7: Compare  $M$  with  $L_{res}$  &  $R_{ba}$ 
8: Detect  $M$  &  $NM$ 
9: if  $M \notin R_{ba}$  then
10:   Set  $M \equiv NM \& AI$ 
11:    $M_i$  accepts  $M$  and declares  $M \in A(M)$ 
12:   if  $M \in R_{ab}$  then
13:     Set  $M = M_i$ 
14:      $M_i$  rejects  $M$ 
15:   end if
16: end if

```

Thus, the malicious-message detection algorithm is used to automatically identify potentially malicious blocks for transparent message transfer between vehicles. The anomaly analyzer also consists of the detection function, which is a critical factor that identifies a message as malicious or non-malicious. The detection function is assigned a value of 0 or 1. If a message is identified as a malicious vehicle, the anomaly analyzer assigns the detection function as 1, and subsequently, the specific message is not forwarded for the comparison process to a rule-based database. The resultant detection function is represented as out, and the capability of the data function is symbolized as C_i^{df} .

```

if (out = 1)
if (Detection function = 1)
if (out = 0)
if (Detection function = 0)

```

Definition 2 (Unpredictability). The use of various nondeterministic data encryption systems significantly increases the security of access to messages from third parties.

Theorem 1. With unauthorized access to messages, the time (T) of their decryption increases significantly.

Proof of Theorem 1. Taking the average time to decrypt messages without a private key, the approximate time to decrypt the message can be calculated using blockchain:

$$E_t = \sum_{i=1}^n t^i \quad (31)$$

where t^i : mean time of the specific encryption algorithm; and E_t : encryption time.

Thus, total time of decryption is calculated by:

$$T_t = n \times E_t \quad (32)$$

where T_t : total time of decryption.

Assuming that the number of messages is $(M) = \{M_1, M_2, \dots, M_n\}$, and that the behavior of the messages $\gamma = \{\gamma_1, \gamma_2, \dots, \gamma_n\}$ is used as the input to analyze the detection of malicious messages, the message M and behavior γ are characterized by $C(\gamma, M)$. Another characteristic of the privacy-preserving model is to integrate the features of the neural network. Thus, malicious message M_m is calculated by:

$$M_m = Ac_f \left(B_{wi} + \sum_{i=1}^{n_i} H_{nij} C(\gamma, M) \right) \quad (33)$$

where Ac_f : Activation function; B_{wi} : Weight of bias for i th number of messages in the decentralized network; n_i : Input neuron count; i th: Input neurons weight; and H_{nij} : Hidden neuron in privacy-preserving model. Thus, the output of the privacy-preserving model for anomaly detection AD_o can be computed as:

$$AD_o = Ac_f \left(B_{wo} + \sum_{i=1}^{N_{hc}} H_{nij} (H_{wio}) M_m \right) \quad (34)$$

where B_{wo} : Output neurons bias weight; N_{hc} : Hidden neuron count; and H_{wio} : Weight of hidden input and output neuron.

If the message is considered malicious (M_m), then a detection function is added with a particular message, and the detection function is zero. The inaccuracy I among real and predicted values is determined by:

$$I = O_w + \sum_{\{B_{wi}, W_{bij}, B_{wo}, H_{wio}\}=1}^{n_{oc}} [A_{oup} - P_{oup}] \quad (35)$$

where n_{oc} : Neuron output count; A_{oup} : real output; P_{oup} : Predicted output; and O_w : Optimized weight.

The rule base involves the authentication process that is incorporated from blockchain technology, and the messages are encrypted and hashed during transmission. Thus, the previous H_p and current hash H_c are computed as:

$$H_p = f \{ IM_{u1} (G_k (PU_k (C_k) M_1)) \} \quad (36)$$

$$H_c = f \{ IM_{u2} (H_p) (G_k (PR_k (C_k) M_2)) \} \quad (37)$$

where IM_{u1} : Unique identity of message-1; PR_k : Public key node; G_k : Key generator; C_k : Key contents; C_i : Cipher text; IM_{u2} : Unique identity of message-1; M_1 : message-1; and M_2 : message-2.

Hypothesis 1. If the switching time is the same between all traffic lights, then the occupancy of street A by transport depends on the outgoing $Flow_{O(A)}$ and incoming $Flow_{I(A)}$ traffic flow to the intersection of the streets within a green light.

Proof. Suppose that the waiting time for the green light is t_w , and the time to wait for a green traffic light is t_g . Assuming that a M number of cars manage to cross the intersection in time t_g , and the waiting time for the green light is t_w , the N number of vehicles arrives at this section of the street. Therefore, if $M < N$ for time $t_w + t_g$, then the street is occupied by a high density of cars; elsewhere, the traffic flow is referred to as free.

Corollary 1.1. At the intersection of two streets where traffic is controlled by traffic lights, streets with more traffic flow should receive more green-traffic-light time than streets with fewer cars. This expression is one of the conditions for avoiding traffic jams at street intersections.

5.1. Provable security for block generation and allocation

Here, we evaluate the security of the proposed EBH-G6 approach.

Proof Correctness: Each vehicle uses a secret key and pseudonym P_s to sign a communication. To ensure geographic privacy, a distinct pseudonym and secret key are utilized to generate block. To ascertain the message's integrity and authenticity, an authenticating vehicle utilizes the sender's public key. The vehicle generates each block for the Message M_e , then the vehicle transmits $(M_e, P_s, M_c, R_n, t_c)$ to other vehicles on the network. where M_c denoted the message contents, R_n denoted the random number that the vehicle picks, and t_c is current timestamp to prevent replay attacks. On receiving the tuple $(M_e, P_s, M_c, R_n, t_c)$, a authenticating vehicle executes the steps. Initially, the authenticating vehicle examines the withdrawal list of the vehicles, which consists of rejected vehicles' pseudonym P_s with valid keys, if the pseudonym P_s of the block-generating vehicle is available in the rejected vehicles' list, then generated block is revoked.

The authenticating vehicle determines whether or not the block is current. In other words, it determines whether $(t_1 - t_2 \leq \delta t)$, condition is satisfied, then block is considered fresh, otherwise the block is deleted that demonstrates the freshness check is unsuccessful. where t_1 is a block generation time, t_2 is a block reception time, and δt is the permitted transmission delay.

The authenticating vehicle verifies the generated block's time validity using the 0-encoding approach described in [40]. If the generated block is not time-valid, the procedure ends; otherwise, it continues. We apply the small exponent test method [41] to provide non-repudiation of generated block utilizing batch verification. This technique uses a vector of randomly generated small integers to identify any modification of a batch of generated blocks. A road side unit (RSU) carries out the batch verification process for several generated blocks in order to increase efficiency. The RSU verifies that all of the received blocks have current timestamps. The process proceeds if a block has a valid timestamp; otherwise, it is rejected. Additionally, the RSU uses 0-encoding to verify the blocks' time correctness. A block is discarded if the time validity check fails. The RSU uses the random vector $(R_v = R_{v1}, R_{v2}, \dots, R_{vb})$, where $R_{vi} \in [1, 2^\tau]$ and τ is a tiny integer with a low processing overhead, while b_i is the number of blocks. Furthermore, multi-copy cloud data auditing approach can be employed [42] with consortium blockchain technology to protect the security.

Thus the validity of the block generation and allocation Y can be determined as follows:

$$Y = \left(\sum_{i=1}^{b_i} R_{vi} \cdot R_{ni} \right) + \left(\sum_{i=1}^{b_i} R_{vi} \cdot h_i \cdot V_{li} \right) \cdot T_{mc} \quad (38)$$

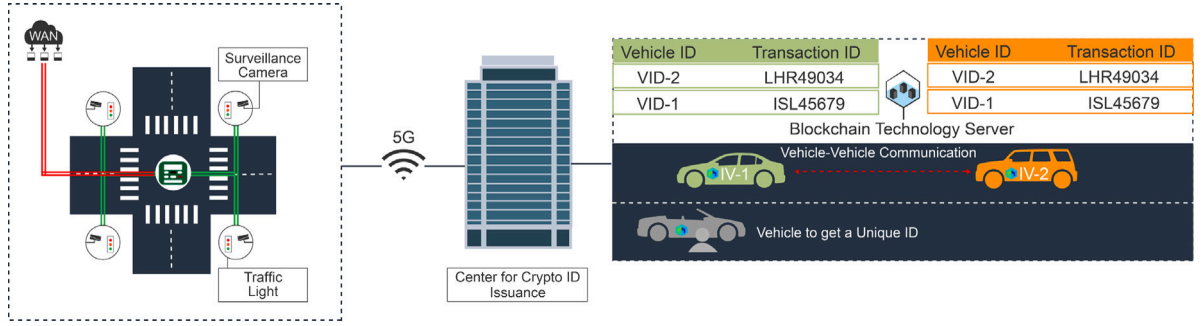


Fig. 10. Testing scenario for conducting the experiment.

where T_{mc} denotes traffic management center, and V_{pi} is the location of the vehicle.

Theorem 2. *The proposed EBH-6G protects against identity attacks (impersonation attacks), when an attacker A has the capacity γ_c to impersonate the vehicle's identity.*

Proof of Theorem 2.

Assume there is a competition between attacker A and a valid vehicle V_v (challenger). The attacker can fake the identity of the vehicle. However, there is protection provided by the consortium blockchain network and 6G technology. The proposed EBH-6G approach is fundamentally safe against adaptive forged-blocks and identity attacks in the presence of consortium blockchain technology. Let there be an attacker A who can fake a valid block $(M_e, P_s, M_c, R_n, t_c)$ in the competition.

Given an instance of elliptic curve discrete logarithm problem ($ECDLP$) used in consortium blockchain, which demonstrates $(ECDLP) \cdot T_{mc}(I, d) = R_{p1} = S_k \cdot R_{p2}$, where R_{p1} and R_{p2} are two random points on an elliptic curve E over function F modulo q can be illustrated as $\frac{E}{Fq}$. Thus, the goal is to make challenger stronger that can solve ($ECDLP$) with a non-negligible probability by employing an attacker A as the subordinate. Thus, attacker A can lose the competition, and impersonation process cannot be accomplished by attacker A .

6. Experimental results

Four traffic lights and four surveillance cameras are installed at the intersection as part of the testing scenario. The data bus depicted in Fig. 10 connects each device to a microcontroller. To maintain the connection, 6G was combined with Wi-Fi. A privacy-preserving model is implemented on the blockchain technology server. The programmed modules are written in C++ and include the OpenCV library to implement the vehicle detection module and the Raspberry Pias GPIO programming interface to interact with the traffic lights. The GCC compiler set is used to build program that support cross-platform features. The testing scene is shown in Fig. 10; thus, we can test the initial results of the proposed EBH system with 6G and without 6G and compare them with other methods, including cost-efficient privacy-preservation on intelligent transportation (CPIT) [36] and blockchain-based conditional privacy-preserving authentication protocol (BCPPA) [35]. Based on the experimental results, the following metrics were observed:

- Anomaly Detection Probability
- End-to-End Delay
- Average Transmission Delay

6.1. Threat model

Threat modeling is a process that aids in accurately assessing and understanding the attack surface, categorizing threats according to risk, and guiding the perceived process. Improving security posture is the purpose of threat modeling. The main objective of the proposed approach is to safeguard data privacy when communicating between vehicles. As a result, the privacy threat model is employed to protect data privacy using the framework of CVSS v4.0 [43]. We now quickly go over our work's supporting threat model. The drivers of the vehicle have unrestricted access to the vehicle, which is often their own. They typically do not know how the vehicle works internally. Certain vehicle models enable the addition of non-safety-related software components to the head unit or allow additional applications to communicate with the vehicle. Drivers should include everyone authorized to operate the vehicle, not just the legal owner or their family members. A malicious mechanic can work on multiple automobiles at once without restriction. They also know a great deal about how vehicles work internally. They can therefore simply alter the hardware and software components of vehicles. Furthermore, they can alter data that is stored inside the vehicle. Most of the time, drivers are unable to determine what changes were made to their vehicle after it was picked up from the repair facility. An attacker may be eager to take the owner's belongings from within the vehicle, as well as parts of the vehicle or the vehicle itself. By attaching a rogue

electronic control unit and sending fake messages, an attacker may try to take over the entire system and maybe open the doors, disable the immobilizer, and start the engine. Professional crooks should invest in expertise and instruments because numerous vehicles have similar technologies and thefts of vehicles can yield substantial profits. One could obtain the tools and knowledge by hacking or by working with malevolent mechanics. A remote attacker might potentially disrupt numerous vehicles randomly for a variety of reasons, such as the desire for a sense of dominance. Any of the easily accessed interfaces found on a vehicle, such as Bluetooth connecting mobile devices to the head unit, wireless networks for Vehicle-to-X communication (IEEE 802.11p), or cellular networks typically utilized to link the vehicle using the internet to a back-end system, could be targeted by an attacker to maximize their impact. In addition to public interfaces, our threat model implies that an attacker has full access to a vehicle's wired and wireless network. An attacker can add or remove network connections, thus altering the network. In terms of data manipulation, if an attacker is successful in changing the data, it will alter the default features and seriously harm the vehicle and its owner. The five potential attacks on the vehicles that have been considered include dusting attacks, de-anonymization, contaminated message attacks, impersonation/ blackmail Scams, and identity theft. These five attacks are associated with data privacy. Thus, the objective is to describe the dangers that these attacks pose. Threats pose potential risks to the data privacy of the vehicles. Privacy threats have an impact on how personal information about communicating vehicles is collected from supplementary sources (such as social media and data leaks). The loss of messages is not a direct result of the exploitation of privacy threats on their own, but it may encourage additional attacks. Anonymity or pseudosymmetry are key components of consortium blockchain that can be used to address these attacks.

1. **Dusting Attack:** It entails the uninvited transmission of incredibly brief messages to a sizable collection of vehicle addresses. The attacker can correlate the various wallet addresses that the leader controls by keeping an eye on what happens next. A dusting attack's ultimate objective is to connect the dusted addresses to the identity of the targeted vehicle. Sending the malicious link to many vehicles, sometimes even hundreds of thousands of addresses on the network, is a new kind of malicious activity used by con artists. These attacks are motivated by a variety of factors. These attacks' main objective is to follow the wallets' data paths closely enough to identify the vehicle of the wallet and operate a focused phishing attack on the victim to obtain the vehicle owner's private information.
Threat Agents: Planned Crime and Offenders, Businesses.
Consequences: Expose of Private Data.
Countermeasures: An in-depth understanding of the vehicle's personal information is necessary for defense against dusting attacks. Avoid letting anyone have control over your communication by ignoring the dust message via consortium blockchain.
2. **De-Anonymization:** It entails the investigation of already-existing spy messages, online networks, etc. to determine a person's or organization's real-world or virtual identity as a result of communication. Attackers might discover, for instance, the victim's past private communications, financial discussions, and secret communications. This knowledge might be employed as a springboard for additional assaults.
Threat Agents: Planned Crime and Offenders.
Consequences: Expose of Private Data.
Countermeasures: (a) refraining from posting private information online (b) utilizing a consortium blockchain that provides privacy by design, the vehicles can reduce the risk of de-anonymization. (c) Using services for mixing (e.g., Wasabi which makes vehicle data storage affordable, simple, secure, and fast). However, users must develop a thorough technical understanding of the privacy properties of vehicle communication if they want to completely avoid De-Anonymization.
3. **Contaminated message Attack:** These contaminated messages are purposefully sent to a targeted vehicle by an attacker who is in possession of preexisting information obtained through criminal activity in order to link the victim and their wallet addresses to the crime. Existing messages in the victim's wallets might then lose some of their fungibility as a result. Certain vehicles will not accept these messages. As a result, the victim's vehicle might be the subject of a criminal probe.
Threat Agents: Planned Crime and Offenders.
Consequences: The importance of protecting vehicle information cannot be overstated because the attack necessitates victim knowledge. Once the affected vehicle has been located, the contaminated message can either be cleaned using mixing services or sent back to the sender. Another option is to maintain distributed shared databases using the consortium blockchain for vehicles' confirmation and restricting unauthorized access to them.
4. **Impersonation/Blackmail Scam:** The victim is duped into thinking a well-known organization wants to give them an award for nothing. The victim is persuaded to send sensitive information to the attacker at his or her request. The vehicle is led to believe by a scam that the attacker is in possession of sensitive information about the victim. For instance, they may release browser history and videos of the victim watching porn, if the victim does not pay a ransom. The victim's personal information is frequently included in this kind of scam in order to make the threat seem more credible.
Threat Agents: Planned Crime and Offenders.
Consequences: Loss of Finance, Damage of Character.
Countermeasures: Avoiding deals that seem "too good to be true" or that demand action be taken quickly. The vehicle user should use the four-eye principle and seek advice from a reliable source if they are unsure. Furthermore, consortium blockchain with use of edge computing modeling can provide guarantee of transparency, data integrity, and tracking.
5. **Identity Theft:** According to Know-Your-Vehicle (KYV) regulations, safe-keeping exchanges must enquire about the actual identities of vehicles. Attackers can make money by selling the data victims give to exchanges or third-party providers, using it to launch targeted attacks, or by assuming the victims' identities.

Threat Agents: Planned Crime and Offenders.

Consequences: Expose of Private Data.

Countermeasures: Consortium blockchain can be employed through peer-to-peer exchanges, which do not require vehicles to go through a KYV process, as opposed to centralized exchanges. When utilizing the centralized exchange, less information should be shared. For instance, decreasing the risk of exposure by using a driver's license instead of an ID.

Theorem 3. *The proposed approach may be resistant to attack due to consortium blockchain.*

Proof. Assume that an EBH-6G provides instances $(U, V = xU)$, where U, V are two vehicles restricted by consortium blockchain B_c and there is an adversary A_d that can forge message M_f with Pseudo Identity ID_p and corresponding signature S_c given as ID_p, M_f, S_c .

The challenger γ is set as a subroutine with probability to address the threat of attacker A_d by using EBH-6G. Thus, threat of an attacker can be void. Therefore, the outdated message can be avoided by checking the message expiry by the receiver. Let T_r be the receipt time of the message, T_d specifies the message departure time, the time difference between the vehicle's clock and the system clock is indicated by t_1 , and the network delay is indicated by t_2 . If $T_r - T_d < t_1 + t_2$, then receiving vehicle acknowledges the message. Otherwise, it indicates that the message has expired, and the recipient will reject it. Furthermore, the message's signature ensures the message's integrity and the message owner's legitimacy. Because of the consortium blockchain, Theorem 3 has demonstrated that the signature used in the proposed approach cannot be forged. As a result, malicious attackers are unable to forge valid signatures of the consortium blockchain.

6.2. Description of scenarios

An on-board unit (OBU) is a device that communicates with the roadside vehicle unit (RSVU) and other vehicles. Internal vehicle communication is not taken into account. RSVU and OBU have been subjected to five attacks (identity theft, de-anonymization, impersonation/blackmail scam, contaminated attack, and identity theft attack). The attacker may try to exploit any potential vulnerability to target RSVU or vehicles. These five attacks are classified as having the potential to be used for three metrics (anomaly detection probability, end-to-end delay, and average transmission delay), specifically for the priority vehicle OBU. Malicious vehicles, on the other hand, are permitted to be registered in the vehicular network. We assume that RSVU should not be included or handled by any unauthorized vehicle. Only the legitimate authority has control over the RSVU. However, a situation has arisen in which the RSVU can be compromised, resulting in an attack on the connected vehicles for data compromise. In any attack scenario, compromised RSVU vehicles could endanger the connected vehicle network and jeopardize vehicle safety. We assume in the vehicle management system that each vehicle is linked to the others in order to share information with RSVU. Another assumption is that vehicles are either autonomous or manual, but they are linked. The experiment is based on critical scenarios that necessitate close attention to avoid any potentially dangerous situations.

Scenario1: luminary Vehicle: The authentic vehicle requests that the PPA's authentic server broadcast its authenticity to other vehicles. The PPA serves as the controller for all authenticated vehicles' records. When the broadcast messages reach the authenticated vehicles, they respond with their authenticity. The PPA verifies the legitimacy of the vehicles that responded. When the vehicles' authenticity is confirmed, the PPA broadcasts a list of all authenticated vehicles. As a result, the vehicles can communicate with authenticated vehicles.

Scenario2: Special Nuclear Material Vehicle (SNMV): It contains highly radioactive materials, such as spent nuclear fuel, etc. Transporting such materials necessitates special precautions. The SNMV can be attacked in a variety of ways. For example, attackers can generate multiple identities, causing SNMV to believe the road is congested, resulting in path diversion. As a result, such diversion can allow attackers to gain access to SNMV, which can have serious consequences.

Scenario3: Emergency Service Provider Vehicle (ESPV): Emergency Service Provider Vehicle (ESPV): This is the vehicle's sensitive movement on the road. To avoid certain unanticipated conditions, the ESPV should arrive on time. In a typical connected vehicle scenario, the ESPV receives all information about traffic congestion and road conditions when it initiates from the source point. The global positioning system can direct the ESPV on an efficient path to the destination, allowing the vehicle to arrive in the shortest amount of time. The attacker can redirect the target to ESPV and spread a false message to limit its movement and prevent it from reaching its destination. The attacker's goal is to halt the ESPV's movement instill fear and panic.

6.3. Anomaly detection probability

The anomaly detection probability can be used to identify malicious activities in the heterogeneous network. Communicating vehicles execute two types of actions: legitimate or malicious. The primary goal of these actions is to identify the effectiveness of a privacy-preserving blockchain-enabled model in the presence of 6G, which has security shortcomings that are addressed by the blockchain privacy-preserving model. Also, the behavior of transmitting vehicles is identified. When malicious activities are identified by detecting vehicles (DV s), collected information is exchanged with adjacent vehicles. A vehicle that has a higher anomaly detection probability (ADP) can detect a malicious vehicle in the network more accurately than others. ADP can be defined as the ratio of malevolent messages to the total number of generated messages. Let us assume Vehicle-1 (V1) generates total transmitted messages and is the message that is tampered with by the sender.

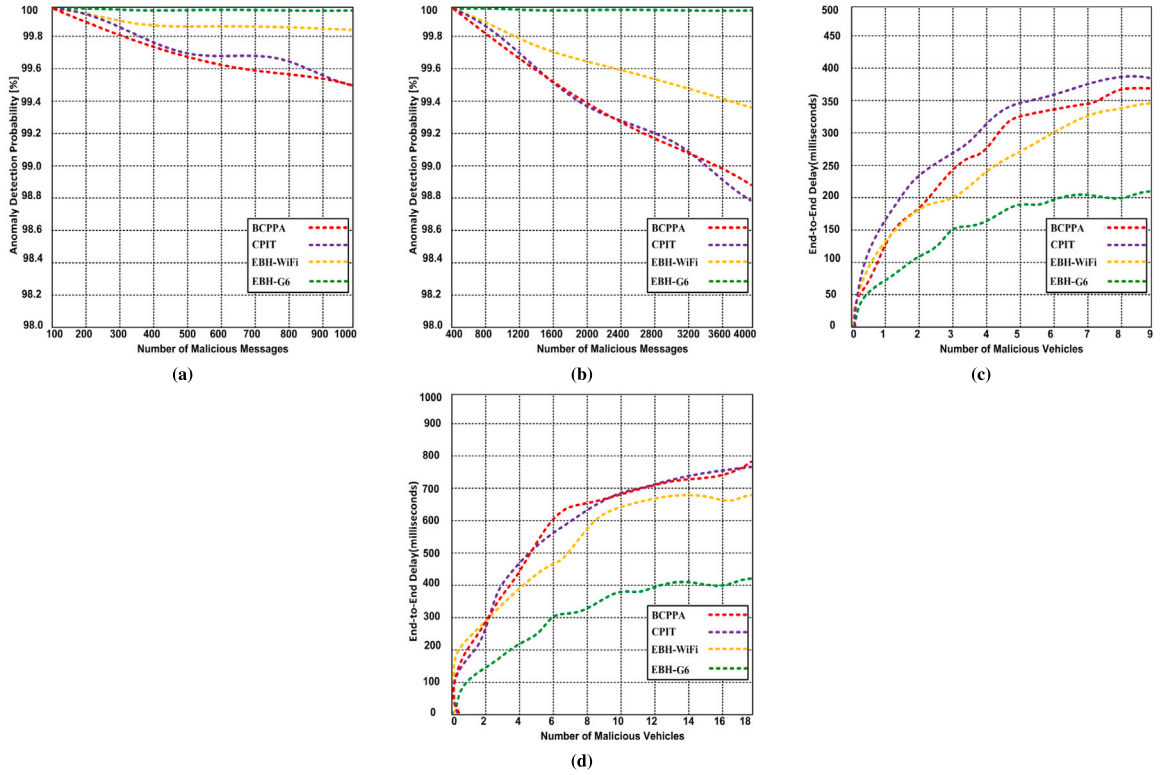


Fig. 11. (a) ADP of proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT, and BCPPA) with 1000 malicious messages. (b) ADP of the proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT and BCPPA) with 4000 malicious messages. (c) End-to-end delay of the proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT and BCPPA) with 9 malicious vehicles. (d) End-to-end delay of the proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT and BCPPA) with 18 malicious vehicles.

Table 2

Metrics describing the proposed EBH method and other methods.

Metrics	BCPPA	CPIT	EBH-Wi-Fi	EBH-6G
Anomaly Detection Probability with 1000 malicious messages	99.49%	99.49%	99.85%	100%
Anomaly Detection Probability with 4000 malicious messages	98.9%	98.8%	99.37%	100%
End-to-End Delay with 9 malicious Vehicles	372 ms	381.2 ms	347.2 ms	209.34 ms
End-to-End Delay with 18 malicious Vehicles	783 ms	772 ms	681 ms	413 ms
Average transmission delay with maximum 144 vehicles	127.2 ms	102.1 ms	90 ms	67.2 ms
Average transmission delay with maximum 270 vehicles	128.4 ms	104.8 ms	90.2 ms	68.7 ms

ADP can be computed as:

$$ADP = \frac{M_{temp}(V1) \times 100}{M_t(V1)} \quad (39)$$

In Fig. 11a, the ADP of the proposed EBH with 6G and EBH with only Wi-Fi, including CPIT and BCPPA, is shown. Results show that the proposed EBH-LiFi achieves an ADP of 100%, while other methods and the proposed EBH-Wi-Fi achieves a lower ADP. However, the ADP of EBH-Wi-Fi is still higher than that of the CPIT and BCPPA methods. In Fig. 11b, more malicious messages are generated. However, more malicious messages do affect the ADP rate. Results thus show that the integration of 6G and blockchain technology can solve the problem of malicious activities.

6.4. End-to-end delay

End-to-end delay relates to the quality of service (QoS) of PP and describes the total end-to-end delay when messaging between valid vehicles and adjacent vehicles. Because the attacker model [44] is used to continuously delay messages, the end-to-end delay is an important parameter to understand the performance of the proposed EBH when messages are delayed by malicious vehicles. Preferably, the EBH model with a lower end-to-end delay is anticipated in the heterogeneous network.

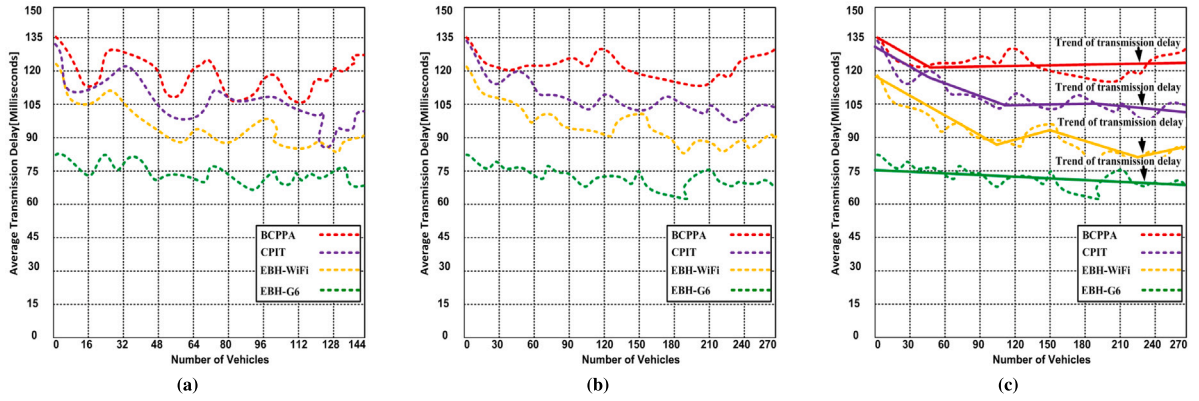


Fig. 12. (a) Average transmission delay of the proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT and BCPPA) with 144 vehicles. (b) Average transmission delay of the proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT and BCPPA) with 270 vehicles. (c) Average transmission delay trend of the proposed EBH-6G, EBH-Wi-Fi and competing methods (CPIT, and BCPPA) with 270 vehicles.

The end-to-end delay is the difference between the message generation time and message delivery time. Thus, the end-to-end delay can be calculated as:

$$\rho = (T_d - T_g) + T_{Ac} \quad (40)$$

where ρ : End-to-End delay; and T_{Ac} : Time for message acknowledgment.

Results in Fig. 11c show that the proposed EBH-6G produces an end-to-end delay of 209.34 ms, while the proposed method with Wi-Fi produces an end-to-end delay of 347.2 ms. Conversely, the BCPPA and CPIT methods produce end-to-end delays of 372 and 381.2 ms, respectively. When the number of malicious vehicles increases, the end-to-end delay increases, as shown in Fig. 11d. The proposed EBH-6G has a lower end-to-end delay (413 ms) compared to other methods (681, 772, and 783 ms for EBH-Wi-Fi, CPIT, and BCPPA, respectively). These results confirm that using 6G can markedly reduce end-to-end delay. We also argue that a lower end-to-end delay can save a substantial amount of energy. Thus, the claim of energy efficiency can be justified by the lower end-to-end delay.

6.5. Average transmission delay

The average transmission delay refers to the required amount of time for a router to insert the packet in the wire. Thus, the average transmission delay A_{td} can be calculated as:

$$A_{td} = \frac{l\gamma}{t\delta} \quad (41)$$

where $l\gamma$ is the length of the packet, and $t\delta$ is the transfer rate.

In this experiment, an average transmission delay between the vehicles was described to ensure how much delay occurs using the 6G network. Figs. 12a-c show that the proposed EBH method either with 6G or Wi-Fi produces a lower average transmission delay compared to other counterparts. Fig. 12a shows that the proposed approach produces a 67.2 millisecond delay with a 6G network and a 90 millisecond delay with Wi-Fi. Other contending approaches produce higher transmission delays even when using Wi-Fi and blockchain technology over edge cloud computing with a maximum of 144 vehicles. The contending methods CPIT and BCPPA produce 102.1 and 127.2 millisecond delays, respectively. When the number of vehicles increases, the impact of transmission delay is observed to be relatively the same, as shown in Fig. 12b.

The overall trend of the proposed method and the other methods is shown in Fig. 12c, describing how the proposed and contending methods behave with an increasing number of vehicles. The proposed method reduces the overall minimum average transmission delay, and due to its lower transmission delay, better throughput was produced. The primary reason for obtaining better performance is the use of consortium blockchain technology, 6G networks, edge cloud computing and IoT devices. Table 2 shows the overall performance of the proposed and other methods.

7. Conclusion

consortium Blockchain-enabled heterogeneous 6G is used in this study for a vehicular management system to improve energy efficiency, increase communication speeds, and mitigate potential threats. This paper explicitly discusses the heterogeneity provision of 6G technology that solves the problems of energy efficiency, latency, slower communication, connectivity, and coverage. Conversely, this method addresses transmission interruption, transmission failure, and transmission snooping in 6G using the consortium blockchain-enabled privacy preservation model to support the vehicular management system. The proposed EBH is tested

with and without 6G, and compared with other methods (CPIT and BCPA). Experimental results demonstrate that the proposed EBH produces a 100% anomaly detection probability with a limited number of malicious messages and an extended number of malicious messages, while other methods produce markedly lower anomaly detection probabilities. Additionally, the proposed EBH produces a shorter end-to-end delay than the other methods. Thus, the proposed EBH has the capability to improve energy efficiency, increase communication speeds, and manage potential threats. In future research, the proposed EBH will be investigated in more detail, and the performance of several QoS metrics will be determined.

CRedit authorship contribution statement

Abdul Razaque: Writing – review & editing, Writing – original draft, Validation, Software, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Meenhoon Khan:** Writing – original draft, Visualization, Software, Data curation, Conceptualization. **Joon Yoo:** Writing – review & editing, Supervision, Project administration, Investigation. **Aziz Alotaibi:** Writing – review & editing, Visualization, Formal analysis. **Majid Alshammari:** Writing – review & editing, Visualization, Formal analysis. **Muder Almiani:** Writing – review & editing, Formal analysis, Data curation.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Abdul Razaque reports was provided by Satbayev University. Abdul Razaque reports a relationship with Satbayev University that includes: employment. Abdul Razaque has patent pending to Licensee. Author was previously employed at IITU Kazakhstan.

Data availability

The authors do not have permission to share data.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) Grant funded by the Korea government (MSIT) (NRF-2021R1F1A1063640 and the researchers also would like to acknowledge Deanship of Scientific Research, Taif University for funding this work).

References

- [1] H. Brian, T. Simra, K. Bharath, A. Fathi, B. Mohamed, S. Tara, A. Razaque, A comprehensive review on blockchains for internet of vehicles: Challenges and directions, *Comp. Sci. Rev.* 48 (2023) 100547.
- [2] M.L. Bouchouia, L. Houda, J. Ons, M. Jean-Philippe, B.J. Wafa, P. Jonathan, Z. Zonghua, A survey on misbehavior detection for connected and autonomous vehicles, *Veh. Commun.* (2023) 100586.
- [3] D. Liu, J. Ni, X. Lin, X. Shen, Transparent and accountable vehicular local advertising with practical blockchain designs, *IEEE Trans. Veh. Technol.* 69 (12) (2020) 15694–15705.
- [4] da Silva, A. Rodrigo, Nelson, L. da Fonseca, Location of fog nodes mounted on fixed-wing UAVs, *Veh. Commun.* 41 (2023) 100600.
- [5] S. Jaiswal, D.K. Sharma, T. Jaiswal, B. Basumatary, M. Tiwari, T. Tiwari, Real time analysis of intelligent placing system for vehicles using iot with deep learning, *Mater. Today: Proc.* (2021).
- [6] J. Yoon, Deep-learning approach to attack handling of IoT devices using IoT-enabled network services, *Internet Things* 11 (2020) 100241.
- [7] J. Gu, H. Wang, G. Ding, Y. Xu, Z. Xue, H. Zhou, Energy-constrained completion time minimization in UAV-enabled internet of things, *IEEE Internet Things J.* 7 (6) (2020) 5491–5503.
- [8] G. Punyavathi, M. Neeladri, M.K. Singh, Vehicle tracking and detection techniques using IoT, *Mater. Today Proc.* (2021).
- [9] Z. Zeng, M.D. Soltani, Y. Wang, X. Wu, H. Haas, Realistic indoor hybrid WiFi and OFDMA-based LiFi networks, *IEEE Trans. Commun.* 68 (5) (2020) 2978–2991.
- [10] U. Arshad, M.A. Shah, N. Javaid, Futuristic blockchain based scalable and cost-effective 5G vehicular network architecture, *Veh. Commun.* 31 (2021) 100386.
- [11] F. Busacca, G. Faraci, C. Grasso, S. Palazzo, G. Schembra, Designing a multi-layer edge-computing platform for energy-efficient and delay-aware offloading in vehicular networks, *Comput. Netw.* 198 (2021) 108330.
- [12] J. Gao, K.O.-B.O. Agyekum, E.B. Sifah, K.N. Acheampong, Q. Xia, X. Du, M. Guizani, H. Xia, A blockchain-SDN-enabled internet of vehicles environment for fog computing and 5G networks, *IEEE Internet Things J.* 7 (5) (2019) 4278–4291.
- [13] R. Shahzadi, M. Ali, H.Z. Khan, M. Naeem, UAV assisted 5G and beyond wireless networks: A survey, *J. Netw. Comput. Appl.* (2021) 103114.
- [14] E.J. Oughton, W. Lehr, K. Katsaros, I. Selinis, D. Bublely, J. Kusuma, Revisiting wireless internet connectivity: 5G vs Wi-Fi 6, *Telecommun. Policy* 45 (5) (2021) 102127.
- [15] Z. Du, C. Wu, T. Yoshinaga, K.-L.A. Yau, Y. Ji, J. Li, Federated learning for vehicular internet of things: Recent advances and open issues, *IEEE Open J. Comput. Soc.* 1 (2020) 45–61.
- [16] J. Andel, V. Šimák, F. Škultéty, D. Nemec, IoT-based data acquisition unit for aircraft and road vehicle, *Transp. Res. Proc.* 55 (2021) 969–976.
- [17] X. Wang, S. Han, L. Yang, T. Yao, L. Li, Parallel internet of vehicles: ACP-based system architecture and behavioral modeling, *IEEE Internet Things J.* 7 (5) (2020) 3735–3746.
- [18] A. Mekrache, A. Bradai, E. Moulay, S. Dawaliby, Deep reinforcement learning techniques for vehicular networks: recent advances and future trends towards 6G, *Veh. Commun.* (2021) 100398.
- [19] H.H. Jeong, Y.C. Shen, J.P. Jeong, T.T. Oh, A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications, *Veh. Commun.* (2021) 100349.

- [20] A.-M. El-Shorbagy, 5G technology and the future of architecture, *Procedia Comput. Sci.* 182 (2021) 121–131.
- [21] Y. Jin, J. Cai, J. Xu, Y. Huan, Y. Yan, B. Huang, Y. Guo, L. Zheng, Z. Zou, Self-aware distributed deep learning framework for heterogeneous IoT edge devices, *Future Gener. Comput. Syst.* 125 (2021) 908–920.
- [22] H. Chen, L. Jiajia, W. Jiadai, X. Yijie, Towards secure intra-vehicle communications in 5G advanced and beyond: Vulnerabilities, attacks and countermeasure, *Veh. Commun.* (2022) 100548.
- [23] M. Almiani, A. AbuGhazleh, Y. Jararweh, A. Razaque, Ddos detection in 5G-enabled IoT networks using deep Kalman backpropagation neural network, *Int. J. Mach. Learn. Cybern.* (2021) 1–13.
- [24] A. Razaque, Y. Jararweh, B. Alotaibi, M. Alotaibi, S. Hariri, M. Almiani, Energy-efficient and secure mobile fog-based cloud for the internet of things, *Future Gener. Comput. Syst.* 127 (2022) 1–13.
- [25] D.L. Guidoni, G. Maia, F.S. Souza, L.A. Villas, A.A. Loureiro, Vehicular traffic management based on traffic engineering for vehicular ad hoc networks, *IEEE Access* 8 (2020) 45167–45183.
- [26] H. Xu, M. Guo, N. Nedjah, J. Zhang, P. Li, Vehicle and pedestrian detection algorithm based on lightweight yolov3-promote and semi-precision acceleration, *IEEE Trans. Intell. Transp. Syst.* 23 (2022) 19760–19771.
- [27] H. Wang, A.X. Wang, S. Xiao, J. Liu, Decentralized data outsourcing auditing protocol based on blockchain, *Ambient Intell. Human. Comput.* 12 (2021) 2703–2714.
- [28] A. Razaque, G. Bektymyssova, J. Yoo, A. Alotaibi, M. Ali, F. Amsaad, S. Amanzholova, M. Alshammari, Malicious vehicle detection using layer-based paradigm and the internet of things, *MDPI Sens.* 23 (2023) 6554.
- [29] M. Noussaiba, A. Razaque, R. Rahal, Heterogeneous algorithm for efficient-path detection and congestion avoidance for a vehicular-management system, *MDPI Sens.* 23 (2023) 5471.
- [30] S. Lai, R. Zhao, S. Tang, J. Xia, F. Zhou, L. Fan, Intelligent secure mobile edge computing for beyond 5G wireless networks, *Phys. Commun.* 45 (2021) 101283.
- [31] Y. Teng, Y. Cao, M. Liu, F.R. Yu, V.C. Leung, Efficient blockchain-enabled large scale parked vehicular computing with green energy supply, *IEEE Trans. Veh. Technol.* 70 (9) (2021) 9423–9436, <http://dx.doi.org/10.1109/TVT.2021.3099306>.
- [32] I. Rasheed, L. Zhang, F. Hu, A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing, *Comput. Netw.* 176 (2020) 107283.
- [33] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, Blockchain for secure and efficient data sharing in vehicular edge computing and networks, *IEEE Internet Things J.* 6 (3) (2018) 4660–4670.
- [34] S. Lee, D.-H. Choi, Dynamic pricing and energy management for profit maximization in multiple smart electric vehicle charging stations: A privacy-preserving deep reinforcement learning approach, *Appl. Energy* 304 (2021) 117754.
- [35] C. Lin, D. He, X. Huang, N. Kumar, K.-K.R. Choo, BCPA: a blockchain-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks, *IEEE Trans. Intell. Transp. Syst.* (2020).
- [36] S. Bao, Y. Cao, A. Lei, P. Asuquo, H. Cruickshank, Z. Sun, M. Huth, Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems, *IEEE Access* 7 (2019) 80390–80403.
- [37] M. Li, J. Gao, L. Zhao, X. Shen, Deep reinforcement learning for collaborative edge computing in vehicular networks, *IEEE Trans. Cogn. Commun. Netw.* 6 (4) (2020) 1122–1135, <http://dx.doi.org/10.1109/TCCN.2020.3003036>.
- [38] J. Wang, D. Feng, S. Zhang, J. Tang, T.Q.S. Quek, Computation offloading for mobile edge computing enabled vehicular networks, *IEEE Access* 7 (2019) 62624–62632, <http://dx.doi.org/10.1109/ACCESS.2019.2915959>.
- [39] A. Zappone, M. Di Renzo, F. Shams, X. Qian, M. Debbah, Overhead-aware design of reconfigurable intelligent surfaces in smart radio environments, *IEEE Trans. Wireless Commun.* 20 (1) (2020) 126–141.
- [40] O.S. Ogundoyin, Ran anonymous lightweight authentication scheme with scalability for trustworthy pervasive social networking, *Cyber Security Technology* 3–4 (2017) 225–250.
- [41] S.J. Horng, S.F. Tzeng, Y. Pan, X. Wang, T. Li, M.K. Khan, B-specs+: batch verification for secure pseudonymous authentication in vanet, *IEEE trans on information forensics and security* 8 (2013) 1860–1875.
- [42] Z. Tu, A.X. Wang, W. Du, Z. Wang, M. Lv, An improved multi-copy cloud data auditing scheme and its application, *King Saud. Univ.-Comput. Inf. Sci.* 35 (2023) 120–130.
- [43] Common Vulnerability Scoring System SIG, MS Windows NT kernel description, 2022, URL <https://www.first.org/cvss/>.
- [44] F. Ahmad, V.N. Franqueira, A. Adnane, TEAM: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks, *IEEE Access* 6 (2018) 28643–28660.