Journal of Artificial Intelligence and Data Science Techniques

ISSN: 3029-2794

Volume 01 Issue 01 (February) 2024

An Enclosed Privacy-Preserving Plan for Safeguarding Communications in Intelligent Transportation Systems

Noorayisahbe Binti Mohd Yaacob[1], Sampath Rajaram[2]

[1] School of Computer Science & Engineering, Faculty of Innovation & Technology, Malaysia
[2]Mohamed Sathak A.J. College of Engineering, India
noorayisahbe.mohdyaacob@taylors.edu.my

Abstract:

Intelligent Transporting Systems (ITS) aims to offer car roadside assistance and mobile communications. ITS safely integrates information and communication technology and real-time vehicles to provide dependable and private communications. The network's intruder-less situation and service demand determine how private users may remain. This article presents a contained privacy-preserving strategy (CPPS) to maintain user privacy over a sustainable period. According to the privacy level of the vehicle, the suggested method establishes rules for user access. This workable method makes regulated service access without raising the overhead of adversary exposure possible. State learning classifiers determine whether to allow service access and revoke user permissions. The learning technique defines Different vehicle states, which use various security elements to avoid privacy leaks and the influence of intruders. To maximize the communication rate, the state allocation considers the vehicle's requirements and service access failures. Access time, adversary impact, response time, and service durability are the measures used to assess the effectiveness of the suggested strategy.

Keywords: Access Control, ITS, Privacy-Preserving, Q-Learning, Vehicle Communication.

1. Introduction

An Intelligent Transportation System is a new technology that gives travelers a safe, comfortable, and smart experience. This is done by connecting smartphones, roadside infrastructure, and vehicles to provide a safe and convenient service to drivers [1]. Vehicles are communicating and exchanging information with each other from vehicles and tool booths. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) use the edge infrastructure. V2V will exchange the information of one vehicle to another, like position, speed, location, etc. [2].

V2I enables will transmission of information from the roadside unit to complement V2V. V2V and V2I technologies will use dedicated short-range communication to exchange information with one another. Vehicle to everything (V2X) is widely used for communication processes like traffic jams, routing, and accidents [3]. Transmit Management System (TMS) provides approximate information about the position of the vehicles around the traveler and it leads to verifying the security of the person. TMS gives efficient and reliable services to travelers. An Incident Management System is used to find out the incidents or accidents that occur in the traveling route of a person. With the help of this traveler, avoid traffic jams and take another convenient route to reach the destination. Emergency management system helps to find out the risk and how to avoid the risk. This system mostly indicates the natural disasters in the route [4, 5].

Intelligent Transport System (ITS) combines intelligence and information technologies. It provides mobility, efficiency, comfort, and safety to the travelers. Security in transportation is critical because of the emergence and advancement of the technologies

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

[6]. Vehicular ad-hoe network (VANET) is one of the main mobile ad-hoe networks which are used for fast communication between the vehicles and the roadside units. VANET helps the travelers to have a safe journey [7]. If an accident occurs in the travelling road, it will indicate to take other route and helps to save time from the traffic jams. Breach detection systems are used to detect the attacks in the system, but cannot be prevented [8]. Digital signature algorithm is used to overcome from the security issued in ITS applications. IPS and IDS are used to monitor the entire suspicious system [9]. Variable Message Signs (VMS) are used to deliver messages to the user about the safety and routing during travelling time [10]. It mainly helps to find a better way or route to travel and will indicate the vehicle's speeding. Wireless Sensor Network (WSN) is used to identify the problems with the help of the collected information from ITS. It helps to provide efficient communication activities [11].

Privacy is one of the main things which are attracted to the people to use Intelligent Transportation System (ITS). Nowadays both the public and private sector were providing privacy policies, and this is the main reason for the success of ITS [12]. The data which are collected from the users are stores in a database. Differential privacy applied for the protection on the floating car data which are stored and processed in traffic data centers. The main goal is to preserve travelers' data from the database to minimize the identity of the records [13]. It focuses on the protection of floating car data which are stored and processed in central traffic data center. It helps to identify the traffic conditions and to detect the speed of the vehicles around the travelling road. Laplace mechanism is used to achieve differential privacy [14]. Emergent intelligence (EI) technique is used to analyze, collect and share information during the privacy process of ITS. EI is adaptive to complicated and dynamic systems to provide the behaviors for transportation during travelling. Local Differential Privacy (LDP) is another vision of differential privacy to protect traveler’s data from unauthorized parties. It helps the users from giving personal information to the unauthorized person at appropriate time [15, 16].

2. Related works

To alter the authentication of network Al-Shareeda et al. and Ozguner et al. [17] has introduced a context-aware authentication scheme. It helps to checks the context of the vehicle in specific period. It mainly focuses on the Public Key Infrastructure (PKI) and Group Signature (GS) to determine low communication authentication. When compared with the other communication scheme, the proposed scheme is much more effective and faster and increases the performance of the authentication throughout the lifetime of the network.

Vehicular Ad Hoc Network (VANETs) uses the Public Key Infrastructure (PKI) to authenticate the integrity of traffic message. But one main issue in VANETs is the efficiency. To overcome this issue Ali et al. and Li et al. [18] has introduced an efficient scheme named as Identity based Conditional Privacy Preserving Authentication (ID-CPPA) which is based on the Vehicle-To-Infrastructure (V2I). This scheme will allow the Road-Side Unit (RSU) to authenticate the services and it helps to increase the efficiency of the network. When compared with computational schemes, the proposed scheme is

more efficient and adaptive for the network.

In this world of automation, wireless network and VANETs are widely used in application. This leads to some sort of privacy issues of the users. To protect privacy issues Feng et al. and Wang et al. [19] has proposed a new method named as Privacy Assessment method with Uncertainty consideration (PAU). It helps to eliminate the attacks in nodes. The real time data from V2V and historical data from cloud are used to evaluate the nodes in PAU. While experimenting PAU in mix-zone, privacy preserving is achieved and improved.

One of the fundamental factors of intelligent transportation system is the Vehicular Ad Hoc Network (VANET). But the main challenges in VANET are the security and privacy issues. To overcome this issue in VANET, Zhong et al. [20] has proposed a new method named as privacy-preserving authentication scheme by using full aggregation. Trace authority approach is used to track the identity of the users during the communication service. The cost of privacy is reducing with the help of the Road Side Unit by pre-calculating the data of the service.

Vehicular Ad Hoc Network (VANETs) is the one which is used in wireless sensor network. It helps to service efficiently and conveniently in transportation. But one of the problems in VANETs is the security and privacy issues. To overcome the privacy issues in VANETs, a protocol named privacy-preserving anonymous authentication was proposed by Zhang et al. [21]. It helps the user to send message and get information from the Road Side Unit (RSU) in a convenient and efficient way by without any further delay. A key exchange function is used to produce the session key to secure communication between the vehicles and RSC. The result in the experiments has increased the feasibility of the protocol.

In transportation, Internet of Things (IoT) is used to provide the interaction between the user and the network. In this Internet of Vehicles (IoV) is one of the main factors which is used for the interaction, because it is fast and reliable when compare with the others. Although it is reliable, privacy issue is a main problem in IoV. Jinila et al. [22] has proposed privacy preserved and secured architecture (PPSA) to protect the privacy issues. When compared with other approach, PPSA has increased in the performance and privacy of the users are protected.

Vehicular Ad Hoc Network (VANET) is a wireless network which is used to provide better services and performance in traffic environment for the users. The main challenge in VANET is the security and performance of the network. Jiang et al. [23] has proposed SAES, named a Self-checking authentication scheme with higher efficiency and security for VANET. To reduce the authentication of vehicles Group Signature is used. Trusted Authority (TA) is used to reduce the cost of authentication. The results of experiments show the efficiency of the scheme and also increased the performance of the network when compare with the existing schemes.

Vehicular Crowdsensing is one of the methods which is used to gather the information about the traffic event in wireless sensor network. To ensure the privacy and trust of the users, Xu et al. [24] has invented a new framework TPSense, for the trustworthiness evaluation and privacy preserving method. By using the maximization algorithm, convert the data to evaluate the user's problem. This framework is used to trace both the real and systemic problems. Results shows that the TPSense is more trust worthiness and

reliable for the vehicles.

To provide efficient and feasible services for the user Vehicular Ad Hoc Network (VANETs) are widely used in transportation application by using the wireless sensor network. But at the same time the leakage in privacy issues is also a main problem in VANETs. Cai et al. [25] has proposed a scheme which is based on ring signcryption named conditional privacy protection for VANETs. This scheme is used to analyze the privacy problem in the network. Results have shown that the scheme is more efficient and secured when compared with the existing methods.

Privacy preserving is main concern in Internet of Things related application. Here Sfar et al. [26] has proposed a game theory-based privacy preserving model for transportation. The game theory model acts as conductor between the receiver and the sender in network. First it describes the elements of the theory and find a convenient way to secure the privacy of the users. The result of the experiment shows the efficiency of the proposed model.

The problems like security and privacy issues in Vehicular Ad Hoc Network (VANETs) have to be addressed before the deployment of the process. Alshudukhi et al. [27] has proposed a lightweight authentication with conditional privacy-preserving scheme by using elliptic curve cryptography to secure the commination in VANETs. Road Side Unit (RSU) and Tamper-proof device (TPD) are combined by the scheme to tract the security issues. The public patterns and the keys of the network are loaded in both RSU and TPD to avoid further issues. The proposed scheme is cost efficient when compared with the existing schemes.

Wireless transportation system widely uses the integrated service system named Internet of connected Vehicles (IOV) to collect information before the process of the service. IOV mainly focus on the security of the intelligent terminals in the network. Wei et al. [28] has discovered a protocol named multi-model implicit authentication which is based on intelligent terminal for IOV. To authenticate the vehicle, it uses the password of the vehicles as a key factor. By this the security of the user will be protect by the attackers. This framework is experimented with the existing schemes and the results shows better protection in the security of the users.

Al-Shareeda et al. [29] has proposed a method based on elliptic curve cryptography (ECC) named privacy-preserving communication scheme based on VANET. This scheme is used to analyze the security and privacy issues in VANETs. ECC and identity-based encryption scheme is used to address the problems in the network. Compared with the existing methods, the proposed model is much more secured and increases the performance of the whole network.

Chen et al. [30] presented a new approach to securing IoT communications using deep packet inspection (DPI) within network middleboxes. It uses privacy-protecting methods, lightweight cryptographic operations, and a dispute-resolution framework. The study includes both formal proof of security and experimental validation in the actual world. The process safeguards the privacy and security of your data without compromising either. There will be no disruptions in communication thanks to the built-in form for handling disagreements. Scalability considerations for large IoT devices and intricate network topologies require more study.

IoT will collect the history of the service and maintain the operation of the service. This

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

will lead to privacy issues in wireless sensor network. Privacy-preserving and continuous data collection scheme has been proposed by Kong et al. [31] for maintaining the data in Vehicular Fog-cloud. The main purpose for the proposed scheme is to maintain the data of the vehicles and observe the data regularly sequentially. When compared with the traditional schemes, the proposed method is more feasible and the security issues are reduced.

3. Proposed Scheme

The proposed scheme aims at maximizing vehicle's service endurance by reducing the adversary impact in the mobile environment. The adversary considered in this scheme is the man-in-middle that interrupts the services between vehicles and service providers. In the service allocation process, vehicle's state is retained if the allocated service sustains regardless of the adversary density. For an ease of understanding, the proposed scheme's functions are illustrated in Figure 1.

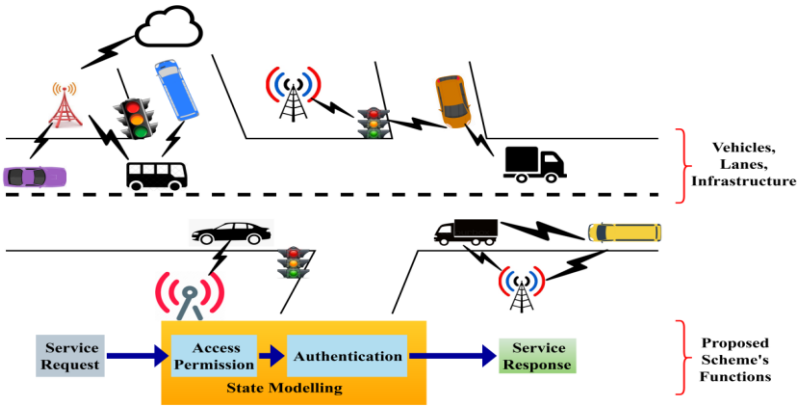

Fig 1. CPPS Function Illustration

The vehicles are interconnected, through access points and other infrastructures units. Therefore V2V and V2X communications are familiar in the proposed scenario. The functions are classified as state modeling and service processes. In the state modeling, access permission and authentication are administered. The classifier learning process defines the states and functions. Contrarily, the request and response are performed in the other process. In the function validation, the man-in –the middle adversary model is considered. A schematic representation of the same is illustrated in Figure 2.

A man-in-the middle intruder causes response, communication, connectivity and access failures. It depends on the position and density of the adversary in an ITS scenario. The proposed scheme has to confront the aforementioned issues, without degrading the communication performance.

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

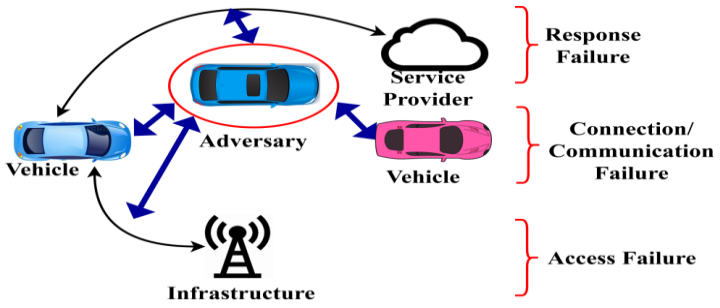

Fig 2. Adversary Impact Representation

First, the permission grant and service access is defined for a vehicle using equation (1):

$$\left.\begin{aligned} \forall\, V, R \in t, G = \begin{cases} 1, \text{if } \rho_I . \rho_S = 1 \\ 0, \text{if } \rho_I = 0 \text{ or } \rho_S = 0 \end{cases} \\ \text{such that} \\ p\ dt = \sum_{i=1}^{t} \frac{\Delta R}{R} = 1 \\ \text{and} \\ p(t) = \begin{cases} G.\, pdt - \frac{\tau \rho_I}{\rho_S}, \text{if } \rho_I < \rho_S \\ G.\, Pdt - \frac{\rho_S}{\rho_I}, \text{if } \rho_S < P_I \end{cases} \end{aligned}\right\} \quad \text{(Eq. 1)}$$

In equation (1), the variables V, R and t represent vehicles, requests, and time. For a response (ΔR), the available service providers (s) responds if both the infrastructure and S are available. The availability of infrastructure and service provider is defined as ρ_I and ρ_S. The grant process is defined as G and the permission P with respect to ΔR and failure (τ) is formulated in any instance is retained at a high level. This increases the service endurance, by reducing errors. The permission grants for $G = 1$ and 0 is independently considered for defining as state. First, the state is defined as $\forall\, V$ and R, the $G = 1$ and hence $\rho_I . \rho_I = 1$. In the proposed scheme, three states are defined namely grant, deny, and pending. The grant state ensures service distribution to the V enduring its span. The deny state halts the service distribution due to privacy violation and adversary impact. Contrarily, the pending state defines the actual vehicle's involvement in service sharing. This means it possesses the states of either grant of deny. If a grant occurs, it augments the service endurance; a deny increases service failures. Initially, the service level for a vehicle is defined as in equation (2)

$$\left.\begin{aligned} \hat{S} = \frac{\rho_I}{\rho_S} + \left(1 - \frac{\Delta R}{R}\right) + \prod_{i=1}^{t} P\ dt - \tau_i \\ \text{where } \tau = (R - \Delta R) \end{aligned}\right\} \quad \text{(Eq. 2)}$$

The service level $\hat{S}$ defines the flexibility provided to the vehicle V throughout $i = 1$ to t such that $G = 1$. If $G=0$, then $\tau > \rho$ di $\forall i \in [1t]$ and hence the service failure is accounted. Based on $\hat{S}$, the service grant state of a V is defined as $\{\alpha_G, \alpha_D, \alpha_p\}$ where in the grant, deny and pending are represented. A common coalition between the states represented in Figure 3.

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

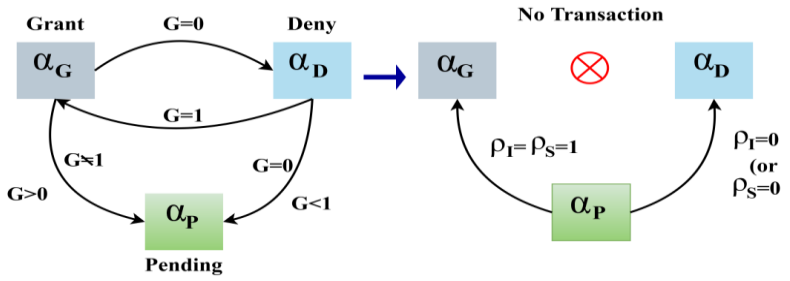

Fig 3. State Coalition Representation

In the state coalition, grant to deny and vice versa transaction relies on G alone. Where as $\alpha_p - \alpha_G$ and α_P to α_D transactions are decided based on ρ_I and ρ_S. Therefore the occurrence due to vehicle movement and handoffs in different $\rho_I = 1$ requires the above intermediate transactions. The transaction between α_p and α_D, and α_P and α_G is defined using equation (3)

$$\left.\begin{aligned} \prod_{P-D} = \rho\left[P(t) + \frac{\rho_S}{\rho_I}1 - P(t)\middle|\ \hat{S}, t \times G\right] \\ \left[\prod_{P-G} = \rho G + \frac{\Delta R}{R}(1-\rho_S)\middle|\hat{S}, (1-\rho_I)\right] \end{aligned}\right\} \quad \text{(Eq.3)}$$

In equation (3), the variables $\prod_{P-D}$ and $\prod_{P-G}$ denotes the transaction for the appropriate states. This is connected with $\hat{S}$ such that the service is sustained and hence the access failures and connected failures are reduced. The state models for transactions are used for providing different authentication formats. It depends on the state and action as defined in $\rho_I = 1$ or $\rho_S = 1$. Contrarily, if $\rho_I = \rho_S = 1$, then the ΔR is high, reducing τ; the alternate case is the privacy preserving. If a transaction $\prod_{P-D}$ is observed, then partial transaction authentication is required. Contrarily, if $\prod_{P-G}$ is observed, then a complete authentication sequence including V and S is required. The first preserves the V, disconnecting τ induced failures, whereas the later part requires V and S authentication preserving service endurance. The authentication for $\prod_{P-D}$ is discussed as follows. In this process, a conventional bilinear mapping-key based authentication is used. For a service grant process where $\rho_S = \rho_I = 1$, the bilinear pairing between V and I is defined as $(B \times B): \rightarrow [A_{prim}, S_{prim}]^G = [A_{prim}]^G$. Here the A_{prim} and S_{prim} refers to the vehicle's and service providers primitives for privacy. The primitives include a non-replicated key (k), a random generator α, and $\hat{S}$. Therefore the A_{prim} and S_{prim} are defined as in equation (4)

$$\left.\begin{aligned} &\forall\, G \in t, \\ &A_{prim} = [V, (G, K)\|(\hat{S}.\alpha)\oplus B^{\alpha}] \\ &S_{prim} = \left[S, K\frac{\|\alpha\|}{V}, \rho_s \oplus \frac{1}{B}\right] \\ &\text{provided} \\ &\left\{(G, K)\|\hat{S}.\alpha\|.\rho_s \oplus \frac{1}{B}\right\} = (G.k)^{\alpha}.\left(\frac{1}{B}\right)^{\alpha} \end{aligned}\right\} \quad \text{(Eq.4)}$$

The "provided" condition is the congruency in verifying the privacy between different V and I, and (I, S). If the congruency is retained, then the state is retained as $\prod_{P-D}$ alse $\prod_{P-G}$ is observed. This congruence-based privacy preserving between V

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

and I and S is presented in Figure 4. This illustration is observed for t before privacy breach/ communication failure occurs.

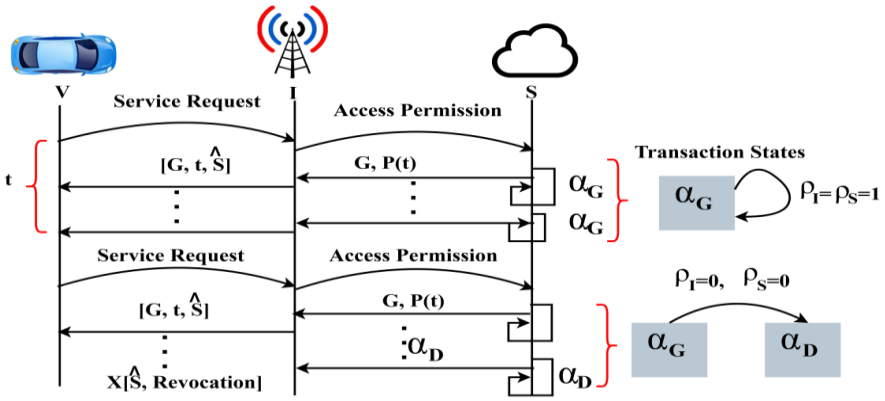

Fig 4. Privacy Preserving Authentication

The above Figure presents the validation between different transactions states wherein $\rho_I = \rho_S = 1$ or 0 is considered. There are two possibilities in providing authentication and privacy preserving (i.e.) $\prod_{G-G}$ (i.e.) α_G is alone true and α_G to α_D is experienced. In the first case, a complete privacy is to be retained for V and services. As discussed earlier, in the second transaction, v′s privacy and authentication is alone expected. Therefore, by pursuing equation (4), the primitives are exploited in maximizing the communication rate. In leakes privacy experiences, the primitives (of V) are revoked, suspending it from the I connection. Thus the changes are reverted using the states and in a reconnection, the $\prod_{P-D}$ or $\prod_{P-G}$ is considered. Therefore the first authentication covering, V, I and S is given by equation (5).

$$\left.\begin{aligned} [A_{prim}, S_{prim}] &= \left[\frac{\Delta R}{R}, \|\hat{S}\|, K\right] \oplus [B]^{\alpha} \\ [A_{prim}(t)] &= (G, K)\|\hat{S}\|.\left[\frac{1}{B}\right]^{\alpha}.P\,dt \\ [S_{prim}(t)] &= \left[\frac{1}{B}\right]^{\alpha}.K \oplus \hat{S} \\ &\text{and} \\ \prod_{G-G} &= \left[P\,dt.\frac{\Delta R}{R}, 1\right], \forall\,(1, t) \end{aligned}\right\} \quad \text{(Eq.5)}$$

In equation (6) the modifications are pursued between S, I, and hence the privacy is retained for $\hat{S}$. This ensures intruder less access to the services under high communication rate. Therefore the privacy between V, I and I is high, and the service access is restored. Contrarily to state transaction is retained in α_G such that $\prod_{G-G}$ is used for verifying t. In the other authentication, partial privacy is ensured where in $\prod_{G-P}$ is induced. The process illustrated in Figure 4 (i.e.) $\rho_I = \rho_S = 0$ represents the failure in t and therefore an adversary impact is experienced. Therefore, the partial privacy requirements are retained based on the previous state. If the previous state is α_n, then new validation and authentication is initiated. If the previous state is α_p, then the probability is either α_G or α_D. Therefore, the partial privacy (for V alone) is

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

retained. In this scenario, the privacy is preserved based on $\prod_{G-G}$ and from this if the V requires authentication, it performs A_{prim} and S_{prim} exchange. This is induced in t $\forall$ authentication, concealing the communication. This partial privacy is ensured in $\prod_{P-D}$ and $\prod_{G-P}$ transactions. The process is defined using equation (6) for both the transactions.

$$\left.\begin{array}{c} [A_{prim}, S_{prim}] = (1-\rho_S)(1-\rho_I) \oplus (G, K) \\ A_{prim} \forall P(t) = \{(1-\rho_I) \oplus G \| K \|\} \frac{\hat{S}}{t} \\ S_{prim} \forall P(t) = (1-\rho_S) \oplus \left[\frac{1}{B}\right]^{\alpha} . \hat{S} \\ \text{Validate} \\ A_{prim} \forall P(t) = S_{prim} \forall P(t+1) \text{or } P\, dt \end{array}\right\} \quad \text{(Eq.6)}$$

The above validation ensures the $\rho_I = 1$ or 0 whereas $\rho_S = 1$ or 0 need not be verified. This reduces the communication cost provided for V2V and V2I information exchange. The above is valid until $\prod_{P-P}$ or $\prod_{D-D}$ is not achieved in any t. Hence the communication rate is expected to be high in the above case. The contrary part requires a proper classification of revoked/ persisting V in the communication scenario. Here, V's revocation does not require the above authentication, reducing the communication cost. It depends on α_G to α_D transactions for providing a denial from service access. First, the ρ_S is verified proceeded by ρ_I requirement and hence revocation with the last known $\hat{S}$ is achieved. The process verifies the current and previous state is expected to be in α_G for new communication. The transaction under different $\rho_I = 0$ or 1 and $\rho_S = 0$ or 1 is defined as in equation (7)

$$\prod_{P-D} = \frac{\rho_I}{\rho_S}(1-\tau) + \frac{\Delta R}{R} \Big| \prod_{P-G} = (1-\tau).G\left(\frac{1}{R}\right)\Big\} \quad \text{(Eq.7)}$$

The chance that leads to modification in different t is evaluated using equation (3) and (7). In equation (7), $\hat{S}$ is not accounted as the service level is unknown (unavailable) in α_P state. The process for different state transaction based on V to S communication is illustrated in Figure 5.

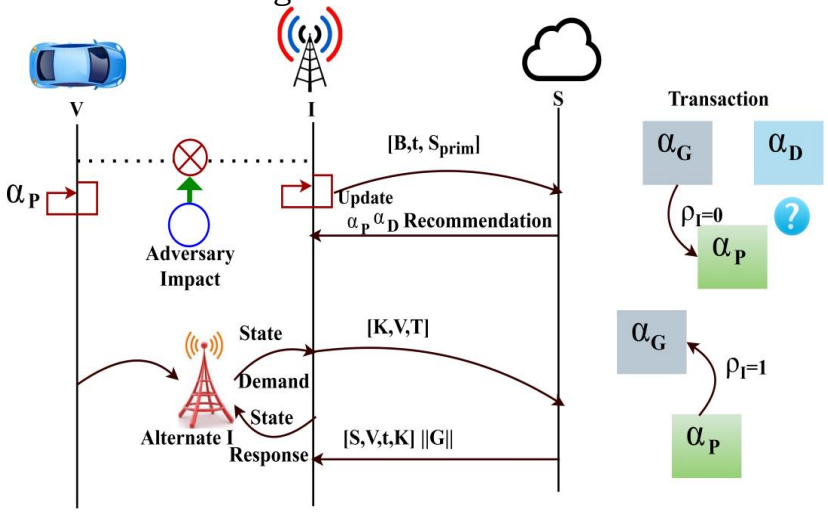

Fig 5. Different State Transactions

Journal of Artificial Intelligence and Data Science Techniques

ISSN: 3029-2794

Volume 01 Issue 01 (February) 2024

As in the above illustration, α_P to α_G is verified through a new I and here the previous state demand and response are required. The change in state is observed for any t with precise k for $G = 1$. Therefore, the $\rho_I = 1$ is retained within $\prod_{P-G}$ transaction. Therefore vehicle revocation case is not required. Contrarily, the discrepancy due to B and τ by equating equations (3) and (7) induces a revocation. Therefore,

$$\left.\begin{array}{l}\left.\begin{array}{c}\rho\left[P(t)+\frac{\rho_S}{\rho_I}\{1-P(t)\}\right]=\frac{\rho_I}{\rho_S}(1-\tau)\frac{\Delta R}{R}\ \forall \prod_{P-D} \\ \text{and} \\ \rho\left[G+\frac{\Delta R}{R}(1-\rho_S)\right]=(1-\tau).G\left(\frac{1}{R}\right)\forall \prod_{P-G}\end{array}\right\}\text{Same State} \\ \left.\begin{array}{c}\rho[P(t)]=\frac{\Delta R}{R}[\text{as } \rho_I=\rho_S=1 \text{ and hence } \tau=0] \\ \text{and} \\ t=1-\left[\frac{\rho(G)}{G}.R\right]\ [\text{as } \rho_I=\rho_S=1 \text{ but } \rho_S=0]\end{array}\right\}\text{Transaction}\end{array}\right\} \quad \text{(Eq.8)}$$

In the above equation, two different constraints are balanced (i.e.) G and (ρ_I, ρ_S). If both the constraints are satisfying, then same state is retained else a transaction is required. This transaction ensures revocation of the same across different intervals. Therefore $\tau \neq 0$ whereas $\tau = 0$ to $\tau \neq 0$ has to be verified in different t. Thus the V is suspended from the communication due to adversary impact. If the adversary impact is overcome, then the validation pursues a partial validation preventing the impact over V. Therefore the revocation denies S access for multiple t and it persists to be the same, preventing different verification and privacy patterns.

User Revocation: The revocation process distinguishes a change in service access and vehicle's state transactions. In the revocation process the constraints in equation (8) is validated wherein equation (1) with $\rho_I = 1$ or $\rho_S = 1$ is modified. Hence in this case, the change is performed with an augmentation in multiplet.

However this occurs in different t and therefore, adversary impact is reduced. The $v's$ state is retained in the previous transaction, preventing privacy leakage. For a new vehicle request, the permission is denied in the same interval, a persisting vehicle is revoked of its permissions/ access from the current t. The revoked process is defined by equation (9)

$$\left.\begin{array}{c}\forall\ \rho_S=0, \\ \prod_{P-G}=\left(1-\frac{\tau}{R}\right)*\left(\hat{S}-\frac{\tau}{V}\right) \\ \text{such that} \\ (1-\tau)\frac{G}{R}=\left(1-\frac{\tau}{R}\right)\times\left(\hat{S}-\frac{\tau}{V}\right)\ [\text{equation (7)with above}] \\ (1-\tau)G=(R-\tau)\left(\hat{S}-\frac{\tau}{V}\right) \\ G=\left(\frac{R-\tau}{1-\tau}\right)*\left(\hat{S}-\frac{\tau}{V}\right) \\ G=R*\left(\hat{S}-\frac{1}{V}\right)\ [\text{after } \prod_{P-D}, \tau=0, \text{as no transmission}]\end{array}\right\} \quad \text{(Eq.9)}$$

The grant is defined in the above equation for R requests and if a V retains its state in α_D, then $R = 0$ and hence $G = 0$. This means the V is revoked from ρ_I and ρ_S, deviating service access. On the other hand revoked users are analyzed for their

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

liability and hence the authentication follows A_{prim}, S_{prim}. In equation (4) the partial authentication is induced for preserving v′s privacy regardless of $\rho_I = 1$ or $\rho_S = 1$. Pursued by this, the revoked user is allocated with a service until the condition (transaction) is equation (8) is achieved. This defines a new $\hat{S}$ for the user/ vehicles in the communicating scenario. In Table 1, the G for different "t" is presented.

Table 1: G FOR DIFFERENT "T"

"t"	Γ_{P-D}	Γ_{P-G}	Service Endurance (%)	G
1	0	43	98.3	1
2	5	36	96.45	0.96
3	3	40	91.58	0.69
4	6	38	93.21	0.841
5	8	25	90.56	0.73
6	9	14	89.36	0.58
7	10	15	87.45	0.43
8	11	8	84.91	0

The G observed at an average for different "t" is presented in Table 1. This is based on $\prod_{P-D}$ observed in different states available. The service endurance is maximized if $\prod_{P-G}$ is high provided $\rho_s . \rho_I = 1$ and the constraint in equation (8) is satisfied. Contrarily, the G requires $\prod_{P-D}$ and $\hat{S}$ for providing flaw less disseminations. The above factors reduce the adversary impacts, containing multiple non-feasible factors in "t". Table 2 presents the service endurance and communication cost for different vehicle density

Table 2: SERVICE ENDURANCE AND COMMUNICATION COST

Vehicle Density	Access Grant	Service Failure (%)	Communication Cost (Bytes)	Service Endurance (%)
20	1	0	410	98.3
40	0.95	3.36	639	97.02
60	0.81	5.69	931	95.4
80	0.73	9.48	1523	91.26
100	0.62	12.54	1958	89.58
120	0.43	15.3	2394	84.91

An analysis for service failure, communication cost, and service endurance is presented in Table 2. Based on the G factor defined in two equations, the endurance is retained. The communication cost increases if G is high and hence the service failure is less. These two factors under $\prod_{P-G}$ and $\rho_S . \rho_I = 1$ maximizes service endurance without increasing the communication cost. Figure 6 presents the analysis for service endurance and access failure for different probabilities.

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

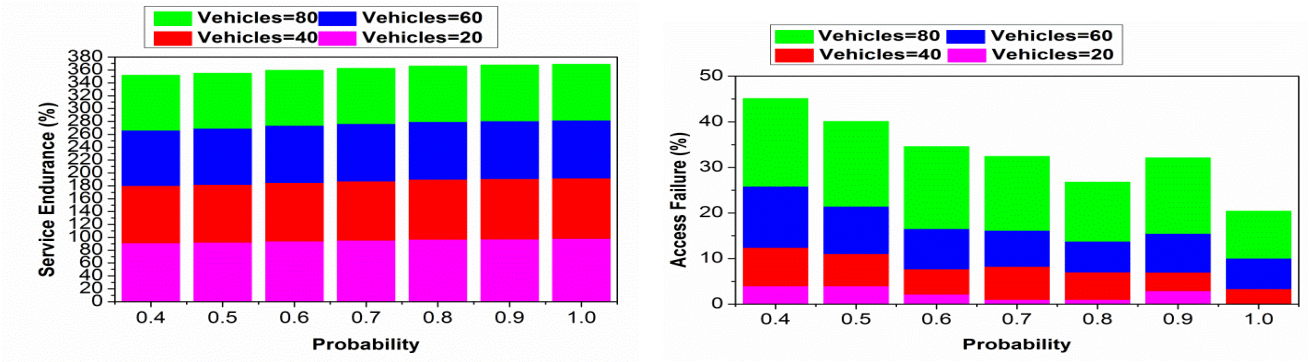

Fig 6. Service Endurance and Access Failure Analysis for Probability

Figure 6 presents an analysis for service endurance and access failure for different probabilities. The probability considered is $\rho_I . \rho_S = 1$ wherein the individual; ratios may vary. As the endurance increases, access failure decreases confined to the $\hat{S}$. In the maximizing probability the V determines the available "t" and hence a process is defaced. Therefore, less is the vehicle density, high is the endurance and less is the failure. The independent and joint state definitions and Π_{P-G} determinations reduce the failure in resource access. The proposed scheme balances V, G for different privacy contained constraints maximizing the performance. In Figure 7, the revoked V, access and response time for different transactions and vehicles is presented.

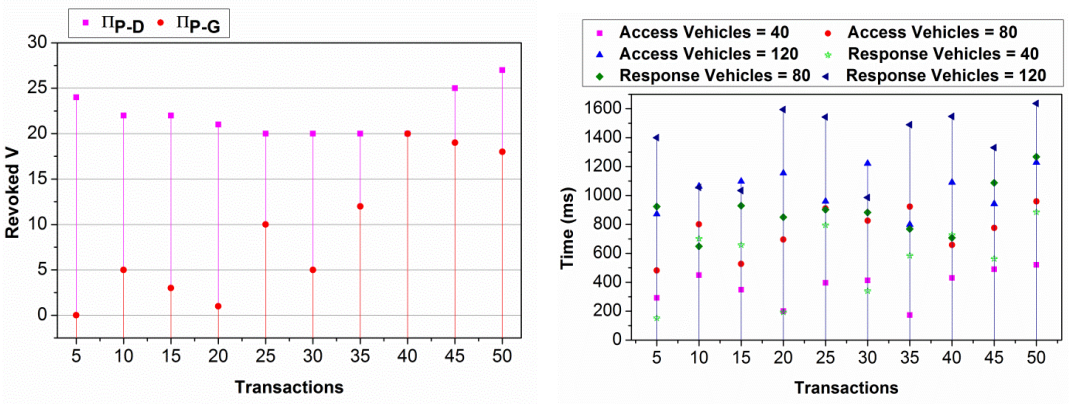

Fig 7. Revoked V and Time Analysis for Transactions

In Figure 7, the v′s revoked and time for different transactions are analyzed. The v's revoked are analyzed under Π_{P-D} and Π_{P-G} transactions. In Π_{P-D} the revocation is high as Π_{G-P} id achieved first and hence the vehicle is not included in the communication. Contrarily, Π_{P-G} reduces the revocation as both α_D vehicles and new ones are augmented for the communication. This requires different access and response time, controlling the privacy and $\hat{S}$. The changes are predominant in providing access to the Sand $\rho_s . \rho_I = 1$ is retained. Therefore the access is mapped to the S based on their incoming time and hence the response. In different Π_{P-G}, $\Pi_{P-D} \times \Pi_{G-P}$, access and response is provided at precise intervals.

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

4. Performance Assessment

This section analyzes the proposed scheme's performance using comparative analysis. The experiment is modeled using vehicular SIM considering 130 vehicles distributed in a highway with 3 intersections. A vehicle is allocated a maximum of 9 instances, for service sharing augmentation. Three vehicle states and 50 transactions are considered for identifying the performance for access time, adversary impact, response time, service endurance, and communication cost. The methods ID-CPPA [18], TPSense [24], and LAPPS [27] are accounted for the comparative analysis from the related works section.

a. Access Time

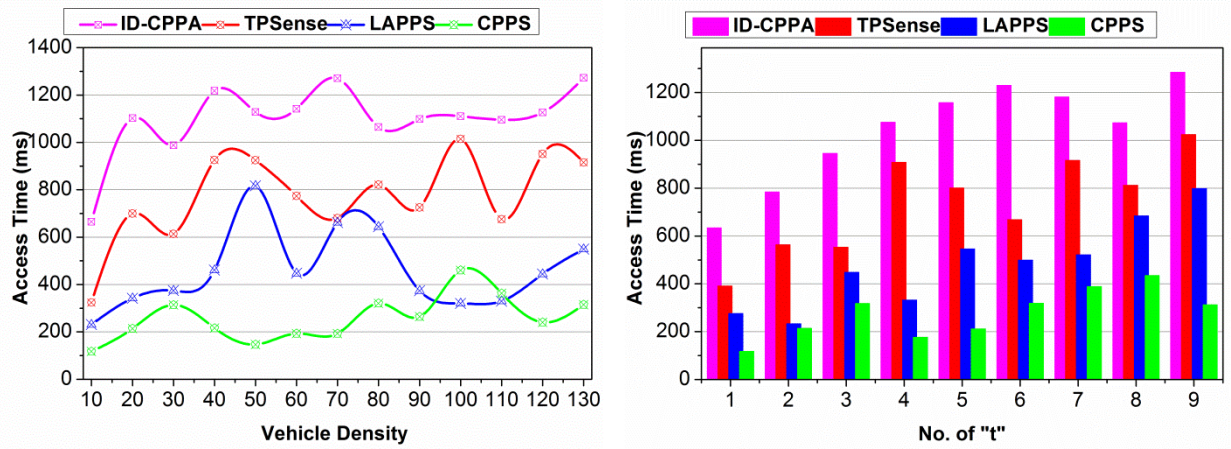

Fig 8. Access Time Comparisons

Figure 8 presents the comparative analysis for access time for different vehicle density and "t". The access time is comparatively less for different t and V by maximizing request process rate. In the proposed scheme, the $v's$ are integrated based on transactions defined by α_D and α_P. The pending state provides additional delay for the R in different t. First, if α_p tends to α_G, then $G = 1$ is acquired and hence access time is less. Contrarily, if $\tau \neq 0$ is observed, then the partial privacy preserving feature is instigated for maximizing access. The $\hat{S}$ is retained for the previous case whereas the $\hat{S}$ is defined from 1 for the second case. In G assessment based on $\prod_{P-G}$ balancing as in equation (9) and (8), the $\rho_S = 0$ or $\rho_I = 1$ is first attained. If $\rho_S = 1$ is achieved, then τtends to 0 and hence the revocation is denied. Therefore, access to service is provided instantaneously without reducing ΔR. Besides the state learning based allocations reduces the adversary impact and thereby frequent disconnections. This turns out in $\prod_{P-G}$ and $\prod_{G-G}$ independently. Therefore the $v's$ requests are momentarily analyzed without additional communication cost. The split in $\rho[P(t)]$ and τ as in equation (8) defines the access level without intersection. Hence the proposed scheme incorporating above features, reduces the access time.

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

b. Adversary Impact

The proposed scheme achieves less adversary impact compared to the other methods. An illustration of the same is presented in Figure 9 for different v and "t". The considered impact of the man-in-middle adversary is combated using transactions and state modeling. First, the G for a V is designed as 1 such that $\rho_I . \rho_S = 1$ is satisfied. There are two cases of adversaries considered (i.e.) the location of the adversary is to be considered. In Π_{P-D} and Π_{P-G}, the states are retained and new identity based privacy features are retained. Therefore regardless of the adversary density and location, the transaction defines its impact. For $\hat{S}$ defined in multiple instances of Π_{P-D} and Π_{P-G}, $\rho_s = \rho_S = 1$ is verified. Based on this condition validation, $(P_s \oplus \frac{1}{B})$ ensures secure communication between the v′s. Therefore a "t" that breaks the closure in this instance reduces the adversary impact. In this context, the V is suspended from I and hence $\rho_I = 0$. This means the least possible chance of v′s privacy is ensured. Further privacy post the transaction verification maximizes high security, reducing the adversary impact.

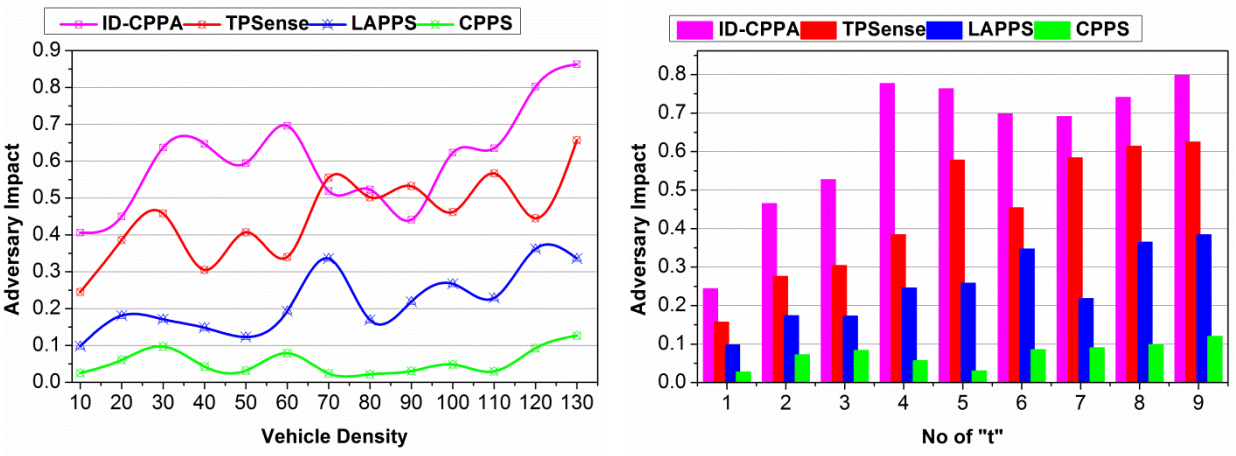

Fig 9. Adversary Impact Comparisons

c. Response Time

The proposed scheme achieves less response time compared to the other methods (Refer to Figure 10). The access is concurrent and swift for different V under contained privacy. In the permission delegation, ρ_I and ρ_S constraints are satisfied for maximizing ΔR. However if an adversary impact is observed, then the transaction determines the V state. Here, $\frac{\Delta R}{R}$ is the reward factor that maximizes the communication rate without compromising time. In the privacy retaining case, the independent/ joint authentication for V and session "t" is administered. Therefore, G = 1 and hence service response is high. For the R in "t", the ΔR is congruent at some far "t" and therefore response time is less. On the other hand, an independent privacy retaining vehicle need not ensure a false communication. This is confirmed based on $\hat{S}$

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

and the final validation is performed based on (A_{prim}, S_{prim}). IT provides a durable communication security, preventing communication τ. Therefore, the passive communication support and interruption in V2V or V2X is less in the proposed scheme requiring less response time.

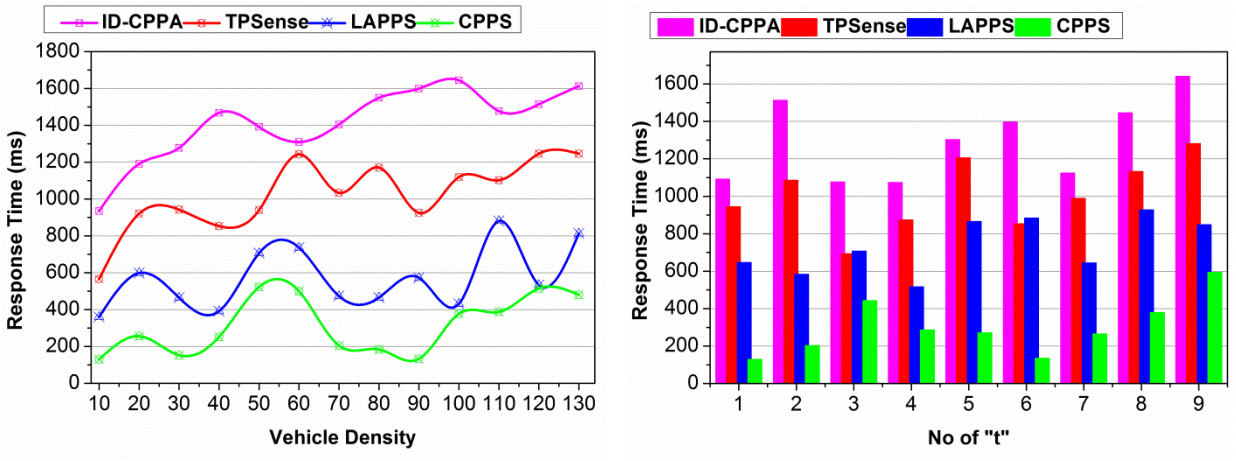

Fig 10. Response Time Comparisons

d. Service Enduranc

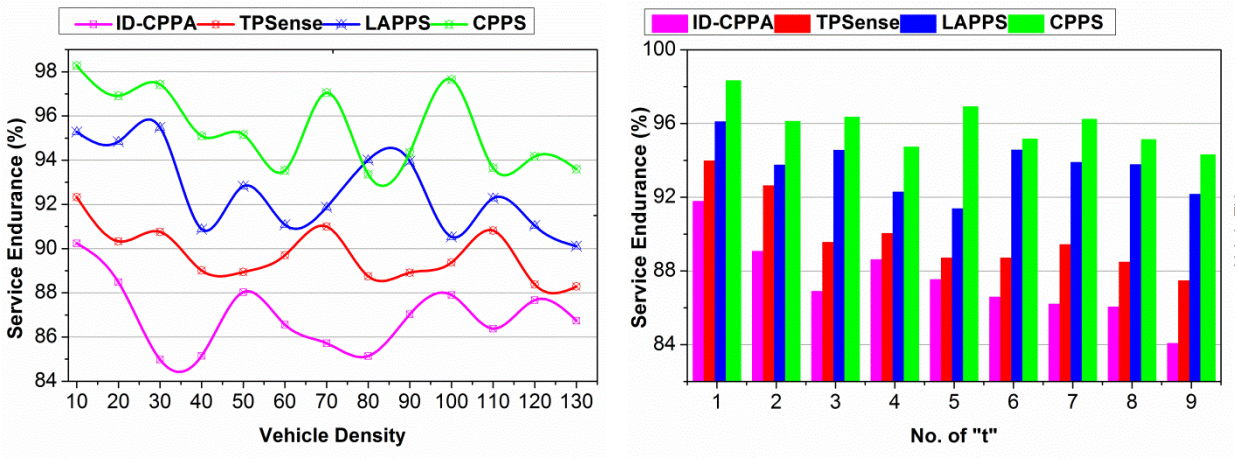

Fig 11. Service Endurance Comparisons

The proposed scheme retains the communication session without additional computation/ overhead. This is achieved by providing independent authentication and privacy stings between v's and S. First, ρ_I based assessments provide $[G, t, \hat{S}]$ features in A_{prim} for security the "t. Pursued by this process, $P(t)$ in S_{prim} retains the session endurance until ΔR is received. Therefore, the change in different verification phases for (t) and $G - G$ as in equation (5). The validation is performed for A_{prim} in t and S_{prim} in $(t + 1)$ for $P\,dt$ such that $P_I = 0$ or $P_S = 0$ is identified. If this is identified, then a new I

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

is allocated for ΔR and therefore service is retained. Contrarily, if ΔR is not achievable, then the privacy of V is retained, preventing further R failures. Thus the Π_{P-D} or Π_{P-G} is decided for further communicating "t". This improves the session's endurance, reducing the adversary impact. Similarly, the state analysis in equation (8) determines the requirement or end of a "t". The transaction requiring V is disconnected from the session and hence the communicating "t" is retained. This prevents false transmissions and paused "t" maximizing the endurance. A comparative analysis for service endurance is presented in Figure 11.

e. Communication Cost

The inclusion of adversaries in a "t" requires altering session and new I for communication. This requirement is reduced in the proposed scheme by performing two different assessments. First, the validation is preceded based on privacy maximizing $\frac{\Delta R}{R}$. The $\hat{S}$ is defined as high for service access and hence the dissemination are masked above the required α. This is verified until $\rho_I - \rho_S = 1$ is satisfied. Contrarily A_{prim} ensures a reliable communication with $\rho_I = 0$.

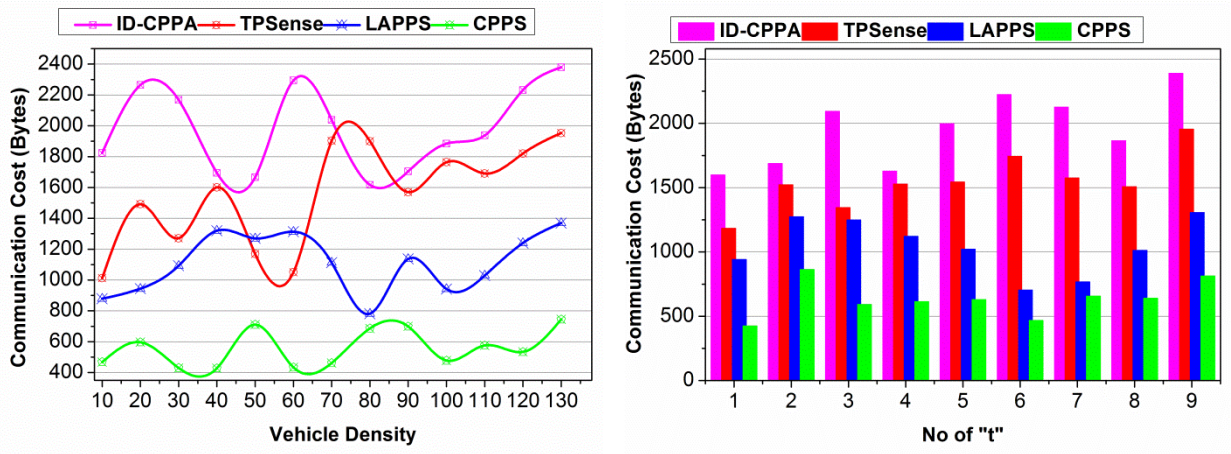

Fig 12. Communication Cost Comparisons

Therefore additional requirement for the "t" is not mandatory, pursuing the Π_{G-G}. This ensures no additional control data between V′s and I′s. The second validation is the state identification defined through equation (7). The $\frac{\Delta R}{R}$ maximization is required for $\rho_I = 0$ or 1 without increasing the adversary impact. In equation (8) the transaction validation is performed for balancing multiple ΔR constraints, reducing false rate. The v is revoked from the communication provided $\tau \neq 0$ and $t < P\,dt$ in $\rho_S = 0$ condition. This requires some communication message to be shared between the v′s or I′s for establishing the communication. In the overall process, the revocation is less confining additional control messages reducing communication cost (Refer to Figure 12).

Journal of Artificial Intelligence and Data Science Techniques
ISSN: 3029-2794
Volume 01 Issue 01 (February) 2024

5. Conclusion

This article proposed a contained privacy preserving scheme for improving the service endurance of intelligent transportation systems. First, the service levels for the vehicles are defined based on which the access and distribution is modeled. For this purpose, the vehicle's state is modeled that pursues different transactions under which the security constraints are satisfied. User service granting and access control levels are modeled based on response reward using the state transactions. Secondly, the privacy between the vehicles and service providers are retained based on independent authentication, preventing the adversary impact. Therefore, the state transactions are relied for mitigating leaky privacy issues, considering different security features. Different from the conventional methods, partial privacy for vehicle's state preserving and failure prevention is incorporated in this method. From the experimental analysis, it is seen that the proposed scheme reduces access time, adversary impact, response time, and communication cost by 23.29%, 16.1%, 17.59%, and 18.95% respectively. This is observed for different communication time instances of the vehicles.

6. References

[1]. Li, C., Wang, S., Li, X., Zhao, F., & Yu, R. (2020). Distributed perception and model inference with intelligent connected vehicles in smart cities. Ad Hoc Networks, 103, 102152.
[2]. Fouchal, H. (2020). Sharing pseudonyms between intelligent transport system stations. Journal of Computational Science, 47, 101236.
[3]. Rahal, R., Korba, A. A., & Ghoualmi-Zine, N. (2020). Towards the Development of Realistic DoS Dataset for Intelligent Transportation Systems. Wireless Personal Communications, 115(2), 1415-1444.
[4]. Sobb, T., Turnbull, B., & Moustafa, N. (2023). A Holistic Review of Cyber–Physical–Social Systems: New Directions and Opportunities. Sensors, 23(17), 7391.
[5]. Kamil, I. A., & Ogundoyin, S. O. (2019). A big data anonymous batch verification scheme with conditional privacy preservation for power injection over vehicular network and 5G smart grid slice. Sustainable Energy, Grids and Networks, 20, 100260.
[6]. Jaballah, W. B., Conti, M., & Lal, C. (2020). Security and design requirements for software-defined VANETs. Computer Networks, 169, 107099.
[7]. Mikavica, B., & Kostić-Ljubisavljević, A. (2021). Blockchain-based solutions for security, privacy, and trust management in vehicular networks: a survey. The Journal of Supercomputing, 1-56.
[8]. Chavhan, S., Gupta, D., Garg, S., Khanna, A., Choi, B. J., & Hossain, M. S. (2020). Privacy and security management in intelligent transportation system. IEEE Access, 8, 148677-148688.
[9]. Ahmed, N., Deng, Z., Memon, I., Hassan, F., Mohammadani, K. H., & Iqbal, R. (2022). A survey on location privacy attacks and prevention deployed with IoT in vehicular networks. Wireless Communications and Mobile Computing, 2022.
[10]. Mosunmola Aroke, O., Sylvester Onuchukwu, I., Esmaeili, B., & Flintsch, A. M. (2022). Countermeasures to reduce truck-mounted attenuator (TMA) crashes: a state-of-the-art review. Future transportation, 2(2), 425-452.
[11]. Xie, G., Yang, L. T., Wu, W., Zeng, K., Xiao, X., & Li, R. (2020). Security Enhancement for Real-Time Parallel In-Vehicle Applications by CAN FD Message Authentication. IEEE Transactions on Intelligent Transportation Systems.

Journal of Artificial Intelligence and Data Science Techniques

ISSN: 3029-2794

Volume 01 Issue 01 (February) 2024

[12]. Hu, P., Wang, Y., Li, Q., Wang, Y., Li, Y., Zhao, R., & Li, H. (2020). Efficient location privacy-preserving range query scheme for vehicle sensing systems. Journal of Systems Architecture, 106, 101714.

[13]. Bouchelaghem, S., & Omar, M. (2020). Secure and efficient pseudonymization for privacy-preserving vehicular communications in smart cities. Computers & Electrical Engineering, 82, 106557.

[14]. Zhao, P., Zhang, G., Wan, S., Liu, G., & Umer, T. (2020). A survey of local differential privacy for securing internet of vehicles. The Journal of Supercomputing, 76(11), 8391-8412.

[15]. Zhang, J., Yang, F., Ma, Z., Wang, Z., Liu, X., & Ma, J. (2020). A decentralized location privacy-preserving spatial crowdsourcing for Internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 22(4), 2299-2313.

[16]. Hammoudeh, M., Epiphaniou, G., Belguith, S., Unal, D., Adebisi, B., Baker, T., ... & Watters, P. (2020). A service-oriented approach for sensing in the Internet of Things: intelligent transportation systems and privacy use cases. IEEE Sensors Journal.

[17]. Al-Shareeda, S., & Ozguner, F. (2020). Alternating authentications to match the situational context of an intelligent communicating vehicle. Vehicular Communications, 23, 100248.

[18]. Ali, I., & Li, F. (2020). An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. Vehicular Communications, 22, 100228.

[19]. Feng, X., & Wang, L. (2019). PAU: Privacy Assessment method with Uncertainty consideration for cloud-based vehicular networks. Future Generation Computer Systems, 96, 368-375.

[20]. Zhong, H., Han, S., Cui, J., Zhang, J., & Xu, Y. (2019). Privacy-preserving authentication scheme with full aggregation in VANET. Information Sciences, 476, 211-221.

[21]. Zhang, X., Wang, W., Mu, L., Huang, C., Fu, H., & Xu, C. (2021). Efficient Privacy-Preserving Anonymous Authentication Protocol for Vehicular Ad-Hoc Networks. Wireless Personal Communications, 1-17.

[22]. Jinila, Y. B., Sheeba, G. M., & Shyry, S. P. (2021). PPSA: Privacy preserved and secured architecture for internet of vehicles. Wireless Personal Communications, 118(4), 3271-3288.

[23]. Jiang, H., Hua, L., & Wahab, L. (2021). SAES: A self-checking authentication scheme with higher efficiency and security for VANET. Peer-to-Peer Networking and Applications, 14(2), 528-540.

[24]. Xu, Z., Yang, W., Xiong, Z., Wang, J., & Liu, G. (2021). TPSense: a framework for event-reports trustworthiness evaluation in privacy-preserving vehicular crowdsensing systems. Journal of Signal Processing Systems, 93(2), 209-219.

[25]. Cai, Y., Zhang, H., & Fang, Y. (2020). A Conditional Privacy Protection Scheme Based on Ring Signcryption for Vehicular Ad Hoc Networks. IEEE Internet of Things Journal, 8(1), 647-656.

[26]. Sfar, A. R., Challal, Y., Moyal, P., & Natalizio, E. (2019). A game theoretic approach for privacy preserving model in IoT-based transportation. IEEE Transactions on Intelligent Transportation Systems, 20(12), 4405-4414.

[27]. Alshudukhi, J. S., Al-Mekhlafi, Z. G., & Mohammed, B. A. (2021). A Lightweight Authentication With Privacy-Preserving Scheme for Vehicular Ad Hoc Networks Based on Elliptic Curve Cryptography. IEEE Access, 9, 15633-15642.

[28]. Wei, F., Zeadally, S., Vijayakumar, P., Kumar, N., & He, D. (2020). An intelligent terminal based privacy-preserving multi-modal implicit authentication protocol for internet of connected vehicles. IEEE Transactions on Intelligent Transportation Systems.

[29]. Al-Shareeda, M. A., Anbar, M., Manickam, S., & Yassin, A. A. (2020). Vppcs: Vanet-based privacy-preserving communication scheme. IEEE Access, 8, 150914-150928.

[30]. Chen, D., Wang, H., Zhang, N., Nie, X., Dai, H. N., Zhang, K., & Choo, K. K. R. (2022). Privacy-preserving encrypted traffic inspection with symmetric cryptographic techniques in IoT. IEEE Internet of Things Journal, 9(18), 17265-17279.

[31]. Kong, Q., Lu, R., Yin, F., & Cui, S. (2020). Privacy-preserving continuous data collection for predictive maintenance in vehicular fog-cloud. IEEE Transactions on Intelligent Transportation Systems.