International Journal of Intelligent Transportation Systems Research (2021) 19:285–298
https://doi.org/10.1007/s13177-020-00234-1

A Collaborative 1-to-n On-Demand Ride Sharing Scheme Using Locations of Interest for Recommending Shortest Routes and Pick-up Points

Oladayo Olufemi Olakanmi[1] · Kehinde Oluwasesan Odeyemi[1]

Received: 3 May 2020 / Revised: 6 October 2020 / Accepted: 12 October 2020 / Published online: 6 January 2021
© Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract
Ride-sharing offers a cheaper means of transportation to riders whose routes are similar to the driver's route within an acceptable time. It is a new paradigm in the urban road transportation system to reduce traffic and enhances the economy of car owners. Unlike 1-to-n ride-sharing that allows n-rider to share rides with a driver, 1-to-1 ride-sharing does not maximize the advantages of ride-sharing. However, the major challenge of 1-to-n ride-sharing is how to match a minimum number of riders with a driver without compromising their privacy, and solves how to synchronize car owners' destinations with their riders' destinations without incurring a delay. Meanwhile, most of the existing ride-sharing schemes are developed for 1-to-1 ride-sharing services, where a rider shares a ride with a driver. In this paper, an effective collaborative ride-sharing scheme is proposed for 1-to-n ride sharing. Our scheme is capable of recommending optimal routes and pick-up points for riders and drivers using their previously visited location's record. It is also capable of providing a single but centralized ride-sharing public management system for every car owner. Thus, eliminates the inefficient disjointed private carpooling form of 1-to-1 ride sharing. It consists of a trust model that is used for computing trust value for riders and drivers, and a similarity model to compute the similarity between locations and riders or drivers. More so, it allows more than a driver to provide collaborative ride-sharing for a rider in case the rider's destination is farther than the driver's destination. The scheme is analyzed, the experimental and analysis results show that our scheme is not only secure but also with low computational latency.

Keywords Taxi-call system · Ride sharing · Autonomous vehicle · Authentication · Privacy preservation · Point of interest

1 Introduction

1-to-n ride-sharing is a new paradigm used to ease urban road transportation problems. It involves multiple riders using the same vehicle to arrive at similar or different destinations. Unlike car sharing, it shares routes and cars amongst different individuals. It offers a demand-based mode of transportation to riders to increase the economy of the car owners without hindering their daily activities. The emergent of different ride-sharing service providers such as Uber, Lyft, and Taxify, etc. is awakening interest in how transportation in urban areas can be shifted from public and taxi transportation to 1-to-n ride sharing. This makes every car owner contributes to peoples' mobility without increasing traffic. Ride-sharing solves some of the fundamental issues in taxi and public transportation. For example, it reduces crimes associated with bus stops and terminals; it is cheap and involves a safer means for payment. Besides, the ride-sharing does not rely on set schedules, and services provided for a few areas.

However, according to Furuhata et al. [1], some major issues will affect the seamless adoption of 1-to-n ride-sharing by a significant percentage of commuters. Some of these challenges range from lack of attractive design for pricing or incentive mechanism, proper ride arrangement, and inadequate trust among the n-rider and driver. Also, Preeti et al. [2] showed pick-up and drop-off points as another important factor to be considered for effective ride sharing. Therefore, 1-to-n ride-sharing schemes must be able to cope with these challenges, especially the last two while the first challenge can be left open-ended for the driver and n-rider. However, ride-sharing schemes for the existing ride-sharing systems are fixed. That is, they fundamentally depend on static and pre-determined pickup points such as existing bus stops or riders' or drivers' determined

✉ Oladayo Olufemi Olakanmi
olakanmi@mit.com

Kehinde Oluwasesan Odeyemi
kesonics@yahoo.com

[1] Office 6 Faculty Building, Electrical and Electronic Engineering Department, University of Ibadan, Ibadan, Nigeria

pick-up points. This ride-sharing arrangement is inefficient, especially in a case where the driver's route and time are not fixed. It affects the performance of ride-sharing.

In most cases, a rider's drop-o point may be farther than the driver's destination. This requires the driver to negotiate a ride with another driver on behalf of his riders whose destinations are farther than his destination. This form of ride-sharing is called multi-hop or collaborative 1-to-n ride sharing. Collaborative 1-to-n ride-sharing enhances the performance of 1-to-n ride-sharing systems by increasing the minimum number of riders for a driver. However, collaborative 1-to-n ride-sharing has several performance limitations such as delay, trust, and security. Also, privacy is another major issue in the ride-sharing system. It creates fears for riders and drivers towards the seamless adoption of ride-sharing. To protect their location privacy, most times, riders select pick-up and drop-off point a few distances away from their sources and destination, respectively. Believing that the added or subtracted distance from their sources and destinations will protect their privacy, however, this incurs overheads.

In this paper, we propose a novel 1-to-n ride-sharing ride scheme for effective ride sharing. The scheme is capable of a collaborative 1-to-n ride-sharing and capable of recommending the shortest routes and pick-up points for riders and drivers using their previously visited location's records. This provides effective privacy-preserving matching of a driver with n-rider by using their trust values and previously visited location's records. This guarantees the secure selection of the shortest route consisting of pick-up points with a minimum number of riders.

The remainder of this paper is organized as follows. In Section II, the related works are examined; Section III discusses the system model and primitives. Section IV discusses the proposed mutual authentication scheme for the multiple providers' based car-sharing system, meanwhile, security analysis and performance evaluations are discussed in Sections V and VI, respectively. Finally, the conclusion is drawn in Section VII.

2 Related Works

The ride-sharing system allows a car owner to share his car with riders along his route at a time instance determined by the car owner. There is a distinct difference between car and ride-sharing. Ride-sharing involves riders along the owner's route at an instant of time determined by the driver while car-sharing involves riders who determine the car owner's route at any instant of time. Although ride-sharing is more advantageous than car-sharing, however, its major problem is how to maximize the number of riders for a driver and ensure the privacy and safety of the users and owners. These have led to fundamental issues such as the selection of optimal pick-up and/or drop-off points, how many points to be considered and their locations, and how to choose the best route that consists pick-up point with a minimum number of riders. Besides these, Nirbhay [3] highlighted other issues such as security, real-time matching, data inconsistency, low tolerance for error, key distribution, network scalability, and privacy as the major metrics affecting ride-sharing.

Several schemes have been developed to overcome the issues highlighted in [3]. Examples of these are schemes in [2, 4–10], and [11]. Preeti Goel et al. [2] presented a scheme that chooses optimally fixed locations of pick-up points to maximize car occupancy rates and preserving user safety and privacy. Their scheme puts forth a selection of pick-up points based on map partitioning into Voronoi cells to select the maximum number of pick-up points suchthat every Voronoi cell has roughly the same number of individuals points based on map partitioning into Voronoi cells to select the maximum number of pick-up points such that every Voronoi cell has roughly the same number of individuals as required by the K anonymity threshold. Also, He et al., [4] proposed a privacy-preserving ride-matching scheme for selecting feasible ride partners in ride-sharing services. The proposed scheme consists of three components that perform initialization ride request or offer generation and a three-step ride selection. However, their scheme does not guarantee trust levels for both riders and drivers. Also, Ta et al. [5] proposed a ride-sharing model that makes sure that the driver's ratio of the shared route's distance to the driver's total traveled distance exceeds the expected rate when sharing with a rider. Their proposition considers multiple drivers, multiple riders, and multiple drivers using the best-first algorithm. However, the privacy of the driver and riders are not considered in the scheme. Sheri et al. [11] proposed a privacy-preserving ride-sharing organization scheme using the k Nearest Neighbours (kNN) encryption scheme, bloom filter, and group signature with data security inclusive. The scheme prevents linking of the encryption of the trips data, sent at different times, by allowing users to frequently update their keys. However, the computational time is reduced when the number of users is greater than seventy- five.

Meanwhile, Farin et al. [6] proposed a framework and payment security system for a dynamic vehicle pooling system such that any type of vehicle can be pooled. This scheme provides security, accessibility, and identification of users while utilizing the empty seats of any type of vehicle. However, it does not guarantee data privacy. Febbraro et al. [12] proposed a user-based relocation methodology in which users may accept to leave the car in a different location in exchange for fare discounts. Hence, formulating a two-stage optimization for alternative distinction proposed to users and for maximizing the profit of car-sharing operators. While the user-based relocation increases profit, other parameters such as security, data privacy among others are not given due consideration in the scheme. To address the dynamic scheduling of ride-sharing requests, Bathla et al. [13] proposed a four-way model for the taxi ride-sharing problem and develop a distributed taxi ride-sharing (TRS) algorithm. Their model assumes a synchronous wireless messaging system with real-time responses, thereby increasing taxi occupancy and profit for drivers and savings passengers. However, data privacy, the security of both the driver and passenger remains a drawback for this model. Andrea et al. [14] also proposed a dissimilarity function between pairs of paths based on the construction of shared paths and a fussy relational clustering algorithm for determining groups of similar paths is executed. This scheme studies the similarities between the user's path to match similar riders by applying the data mining technique to improve ride-sharing services and friend- recommendation and community discovery systems. Shen et al. [15] proposed a clustering-based request matching and route planning algorithm that considers spatial-temporal distances between ride requests on road networks. Also, Zhuo Wei et al. [16] proposed a secure key sharing system consisting of key generation, key transmission, and key management. Their proposed scheme issues digital keys and authorize users through a key management module installed onboard of cars, and authenticating with a near field communication chip and a smartphone application. However, their system does not consider the security and privacy of the users.

Maintaining trust and privacy also is critical in social networks and ride-sharing. To solve this in social networks, Liu et al. [17] proposed a privacy-preserving framework to boost data owners' willingness to share their data with untrusted entities using partially homomorphic encryption to evolve two protocols for protecting the private data of every party involved in the recommendation. Also, Mayadunna and Rupasinghe [18] proposed a trust framework to calculate the node trust values for social network users by applying reinforcement learning methods. After calculating the user's trust value, their framework uses a technique that is analogous to a collaborative filtering recommendation algorithm to calculate the user's trust score. While trusted and untrusted users could be identified based on their trust value, the method enables maintenance of the user's privacy and confidentiality. Similarly, a decay-based trust model and a secure and privacy-preserving taxi service framework for car-sharing are proposed in [19]. The decay-based trust model monitors and improves the quality of service rendered to passengers. Meanwhile, Yang et al. [20] proposed a latent social trust network model to improve recommendations. In the scheme, trust information in the social network is employed through collaborative filtering to alleviate the problems of malicious attacks.

Determining the shortest route is also one of the ways of enhancing performance in any network. Samanthulla et al. [21] proposed a privacy-preserving shortest path discovery over the encrypted graph (PSPEG) data. The scheme was experimented with protocols under single and federated cloud environments by considering security, accuracy, efficiency, and flexibility as crucial requirements. According to the authors, PSPEG protocol under a federated cloud environment proved more efficient from the end-users' perspective than the standard single cloud setting. However, PSPEG under a federated cloud environment is more secure but with higher computational power than PSPEG under a standard single cloud setting.

Also, secure authentication ensures confidentiality and integrity in ride-sharing. Many authentication schemes had been proposed for vehicular ad hoc networks (VANETs) and other networks. Examples of these are in [22–24]. Azeez et al. [22] proposed an efficient anonymous authentication scheme to avoid malicious vehicles entering into the VANET. In this scheme, a conditional tracking mechanism to trace the vehicles or roadside units that abuse the VANET was developed. This allows the scheme to revoke the privacy of misbehaving vehicles to provide conditional privacy in a computationally efficient manner. Meanwhile, Xiaodong et al. [25] identified some unique design requirements in the aspects of security and privacy preservation for communications between different communication devices in vehicular ad hoc networks. They proposed a secure and privacy-preserving protocol based on group signature and identity-based signature techniques.

Meanwhile, despite all these research efforts on solving the security and privacy issues in VANETs, few works are done on ride-sharing and none of these delves into how to recommend a privacy-aware optimal route for drivers, and pick-up point for drivers and riders for effective ride-sharing using their previous locations of interest. Besides, most of the schemes employed certificates and signatures for authentication; this increases their computational costs through the certificates and signatures verification process.

2.1 Problems and the Innovation of this Paper

Problems:

- Optimal recommendation of pick-up points for the drivers with the minimum number of potential riders is an issue in 1-to-n ride sharing.
- Optimal recommendation of pick-up points for the riders such that the riders get rides at the recommended pick up points is also an issue in ride-sharing.
- To determine the shortest routes for the drivers such that their ride-sharing capacity is met during 1-to-n ride sharing.
- Security of data and privacy of the drivers and riders are the major performance issues in 1-to-n ride sharing.
- None of the existing ride-sharing systems supports collaborative 1-to-n ride-sharing for the riders with drop-o points farther than their drivers' destinations.

Innovation of this Paper:

- In this work, we propose a novel 1-to-n ride-sharing scheme capable of recommending short route, pick-up

and drop-off points for drivers and riders, and performing collaborative 1-to-n ride sharing.
- A model for determining similarity between drivers or riders and their previously visited locations.
- A model for determining the trust values of drivers and riders to filter off untrusted riders and drivers from the ride-sharing system.
- A secure and privacy-aware scheme is proposed to address security and privacy challenges in 1-to-n ride sharing.

3 Primitive and System Model

3.1 Primitives

In this scheme, an additive cyclic group G of an elliptic curve E over a prime field F_q of generator P and prime order q is used. In addition, a function H with n-bit output and l-bit key for $l, n \in Z_p$ is used. H is a deterministic function that takes two inputs, the first of arbitrary length, the second of length l bits, and outputs a binary string of length n formally defined as $H : \{0, 1\}^* X \{1, 0\}^l \rightarrow . \{0, 1\}^n$.

3.2 System Model

The system model as shown in Fig. 1, consists of five entities; Car Owner (CO), Rider (RD), City Transport Management (CTM), Recommender (RCR), and Social and Location Network (SLN).

- City Transport Management (CTM): This is an independent entity that manages the trust data of car owners and riders. Although, ready to collaborate with RCR during recommendation, however, hides the identities of the owners of the secure trust data from all other entities. CTM keeps the previous trust data of drivers and updates the new trust values for the drivers after every service delivery. It is also responsible for the registration of car owners and riders at their point of entry into the ride-sharing system. The trust network among drivers and riders is modeled by CTM as a direct graph $G = (J, E)$, where J is the set of nodes in the trusted network representing riders and drivers in the system, and E is the set of edges that represent trust values between drivers and riders or drivers and drivers. The matrix V_C, extracted from G, contains the trust values between drivers and riders. The trust value $0 \leq \mathsf{F}_{i,j} \leq 1$ represents the trust value of the rider or driver i on the rider or driver j such that $\mathsf{F}_{i,j} = \mathsf{F}_{j,i}$. If $\mathsf{F}_{i,j} = 0$, it indicates that i distrusts j, however if $\mathsf{F}_{i,j} = 1$, it indicates i completely trust j. For every service rating made by i on j after any service, $\mathsf{F}_{i,j}$ is updated using the developed update model in Eq. 1
- Car Owner (CO): This is a car owner who is ready and willing to share its ride with the riders along his route at a specified instant of time. He requests from RCR for the shortest route containing a minimum number of potential riders.
- Rider (RD): This is a potential rider in the ride-sharing system. He is capable of sharing a ride with any car owner whose riding route and time match the rider. He/She can request from RCR a convenient pick-up point at a particular time instant.
- Recommender (RCR): It enables RDs and COs to obtain their pick-up points and the shortest route, respectively. It ensures collaborative ride-sharing for riders. RCR performs recommendation for RDs and COs with the help of SLN and CTM. RCR requests for the location, destination, and takes off time from the drivers to recommend the shortest route for the driver and pick-up points for riders. Both SLN and CTM are ready to collaborate with RCR by releasing the privacy protected trust and check-ins records of all the authorized drivers and riders in the system.
- Social and Location Network (SLN): SLN provider such as Google map provides the location visited records (LVR) of the RDs as the set $Rd_S = \{rd_1, rd_2, .., rd_n\}$ and as the set $CO_S = \{co_1, co_2, .., co_n\}$ for COs and for set of locations $Y_S = \{y_1, y_2, .., y_n\}$ closer to set of PuP $P_S = \{p_1, p_2, .., p_n\}$ at set of time $T_S = \{t_1, t_2, .., t_n\}$. SLN evolves M_{rd} and M_{co} as the LVR matrices for all the registered RDs and COs from all these sets. Each of the matrices contains element $m_{i,j}$ that represents the number of visitations that RD rd_i or CO co_i has ever done at location y_j.

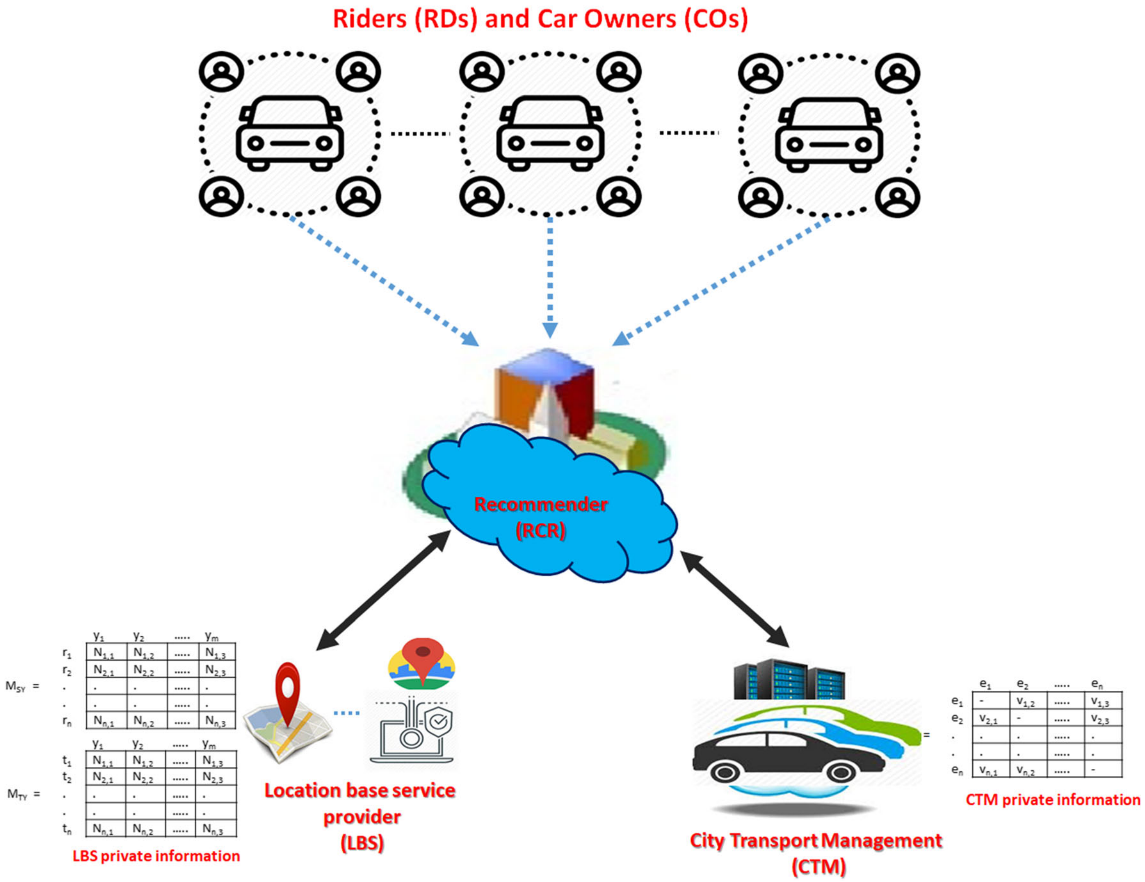
3.3 Assumptions

The following assumptions, which had been proved in cryptographic research, are made to ascertain the security of the scheme.

1. Discrete Logarithm (DL) Problem: Given $P \in (Z_q)$ and $Q = aP\, mod\, q$, to Find a Is a Discrete Logarithm Problem

2. Computational Diffie-Hellman (CDH) Problem: The CDH Problem States that the Computation of abP Given P; aP and bP for some $a, b \in Z_q$ Is Intractable

Past research works had shown that the CDH problem is intractable, and DL is also intractable if the order of the group is unknown to the adversary [26]. That is, there is no polynomial-time algorithm to solve DL and CDH problems with non-negligible probability.



$$M_{SY} = \begin{array}{c|c|c|c|c|}
 & y_1 & y_2 & ..... & y_m \\
\hline
r_1 & N_{1,1} & N_{1,2} & ..... & N_{1,3} \\
\hline
r_2 & N_{2,1} & N_{2,2} & ..... & N_{2,3} \\
\hline
. & . & . & ..... & . \\
\hline
. & . & . & ..... & . \\
\hline
r_n & N_{n,1} & N_{n,2} & ..... & N_{n,3} \\
\hline
\end{array}$$

$$M_{TY} = \begin{array}{c|c|c|c|c|}
 & y_1 & y_2 & ..... & y_m \\
\hline
t_1 & N_{1,1} & N_{1,2} & ..... & N_{1,3} \\
\hline
t_2 & N_{2,1} & N_{2,2} & ..... & N_{2,3} \\
\hline
. & . & . & ..... & . \\
\hline
. & . & . & ..... & . \\
\hline
t_n & N_{n,1} & N_{n,2} & ..... & N_{n,3} \\
\hline
\end{array}$$

$$= \begin{array}{c|c|c|c|c|}
 & e_1 & e_2 & ..... & e_n \\
\hline
e_1 & - & v_{1,2} & ..... & v_{1,3} \\
\hline
e_2 & v_{2,1} & - & ..... & v_{2,3} \\
\hline
. & . & . & ..... & . \\
\hline
. & . & . & ..... & . \\
\hline
e_n & v_{n,1} & v_{n,2} & ..... & - \\
\hline
\end{array}$$

Fig. 1 System architecture

3.4 Security Requirements

The proposed scheme for 1-to-n ride-sharing must be mutual authentication-secured and authenticated key exchange-secured, and once the above problems are intractable and difficult then the scheme met the following security requirements.

- There is no adversary who can forge authorized ride-sharing and riding tokens in the matching and mutual authentication phases if the DL and CDH problems are intractable, and the used key-based hash function exhibits one way-ness.
- There is no adversary who can forge or compromise 2-way key exchange parameters and shared symmetric key in the setup and key management phase, DL and CDH problems are difficult.
- There is no adversary who can forge a recommendation request packet if the DL and CDH problems remain intractable.

4 Collaborative 1-to-N on-Demand Ride Sharing Scheme

The 1-to-n ride-sharing scheme involves three stages; trust and similarity models stage, 1-to-n ride-sharing shortest routes and PuPs recommendation stage, and mutual authentication between RD and CO stage. Figure 1 shows the system model consisting of all the entities as described in the previous section. Table 1 contains the definitions of all the symbols and notations used in the scheme.

4.1 Trust and Similarity Models

Trust values and service ratings of the COs and RDs, respectively are one of the performance factors of an effective collaborative ride-sharing system. In this subsection, we developed a trust and rating model to determine the trust values of all the involved entities in the system. After ride-sharing, the car owner rates the conducts of his RD(s), and the RD(s) also do the same for the CO, then send the rating to CTM. CTM aggregates all the success ratings $\varphi_{a\rightarrow b}$ and failure rating $\varphi'_{a\rightarrow b}$ as given by, say RD a to CO b or vice versa from initial time t_0 to the current time t_f. It then evolves the trust value of a to b as shown in equation 1. To avoid a cold start problem at the onset of the ride-sharing system, CTM evenly assigns the smallest trust values to all the registered RDs and COs to create initial trust.

$$\chi_{a\longmapsto b} = \frac{\sum_{t_0}^{t_f} \varphi_{a\longmapsto b}}{\sum_{t_0}^{t_f} \varphi_{a\longmapsto b} + \sum_{t_0}^{t_f} \varphi'_{a\longmapsto b}} \quad (1)$$

$$\mathrm{F}_{a\longmapsto b} = \chi_{a\longmapsto b} + \mathrm{F}'_{a\longmapsto b} e^{[\chi_{a\to b}]}$$

Where $F_{a \to b}$ is the trust value of a on b, while $F'_{a \longmapsto b}$is the previous trust value of a on b.

Also, a similarity model is formulated for RCR, based on RDs' locations visited record (LVR), to determine the likely locations and destinations of RDs during recommendation. The likely locations of RDs are determined by computing a similarity metric $\beta_{a \longmapsto l}$ between the RDs and several locations in the RDs' LVRs using Eq. 2. The similarity model is associated with trust value vectors and LVR. Usually, the likely location of the RD at a given time is the location with the highest similarity metric, and taken as the PuP of the RD at that given time.

$$\beta_{a\mapsto l} = \frac{M_{ty}(a,l)}{M_{sy}(a,l)} \left(M_{ty}(a,l) + M_{sy}(a,l) \right) \sum_{a,b\in U, a\neq b} \mathrm{F}_{a\mapsto b} \quad (2)$$

where $M_{ty}(a, l)$ is the total number of check-ins made on location l at time t and $M_{sy}(a, l)$ is the total number of check-ins a has ever made on location l up till the current time. Both $M_{ty}(a, l)$ and $M_{sy}(a, l)$ are extracted from matrices M_{SY} and $M_{TY.}$

4.2 1-to-n Ride Sharing Shortest Routes and PuPs Recommendation

The 1-to-n ride sharing shortest routes and PuPs recommendation stage consists of three phases; the setup, recommendation of optimal routes and PuPs using LVRs, and matching RDs with CO for 1-to-n ride sharing phases. Each of these phases is described as follows:

4.2.1 Set-up Phase

To set up the ride sharing system, RCR registers each RD and CO by randomly generating as its master key and computes pseudonym and authentication parameters for each RD and CO as:

- RCR computes and publishes its public key C_{rcr} as $C_{rcr} = \beta P$, randomly generates $a \in Z_q^*$, and computes and publishes its 2-way public exchange parameters $q_{rcr} = aC_{rcr}$
- RCR requests the unique identity of each RD and CO to compute their pseudonyms as:

$\mathcal{F}_{rd} = H_\beta(Id_{rd})$ for RD, and $\mathcal{F}_{co} = H_\beta(Id_{co})$ for CO.

Keeps $\mathcal{F}_{rd}$; Id_{rd} and $\mathcal{F}_{co}$; Id_{co} but sends $\mathcal{F}_{rd}$ to RD and $\mathcal{F}_{co}$ to CO.

- Each RD i generates a unique random number $b_i \in Z_q^*$, computes and publishes its 2-way public exchange parameters q_{rd} as: $q_{rd} = b_i C_{rcr}$
- CTM generates a unique random number $d \in Z_q^*$,, computes and publishes its 2-way public exchange parameters q_{ctm} as: $q_{ctm} = dC_{rcr}$
- Also, each CO j generates random number $b_j \in Z_q^*$, computes and publishes its 2-way public exchange parameters q_{co} as $q_{co} = b_j C_{rcr}$

For secure exchange of information between RCR and any of the RD, CTM, and CO, RCR generates a symmetric shared key (*ssk*) with each of these entities, and they too, in turn, generate their *ssk* with RCR as follows:

- Each RD i computes its *ssk* with RCR as $ssk_{rd \longmapsto rcr} = b_i q_{rcr}$and RCR also computes its *ssk* with the RD as $ssk_{rcr \longmapsto rd} = aq_{rcr}$ such that $ssk_{rd \longmapsto rcr} = ssk_{rd \longmapsto rcr}$
- Each CO j computes its *ssk* with RCR as $ssk_{co \longmapsto rcr} = b_j q_{rcr}$ and RCR also computes its ssk with the CO as $ssk_{rcr \longmapsto co} = aq_{co}$ such that $ssk_{co \longmapsto rcr} = ssk_{rcr \longmapsto co}$
- CTM also computes its *ssk* as $ssk_{ctm \longmapsto rcr} = dq_{rcr}$ while RCR computes its *ssk* with the CTM as $ssk_{rcr \longmapsto crm} = aq_{ctm}$such that $ssk_{ctm \longmapsto rcr} = ssk_{rcr \longmapsto ctm}$

4.2.2 Recommendation of Optimal Routes and PuPs Using LVRs

In this phase, a recommendation based algorithm to solve the shortest routes and matching problem in 1-to-n ride-sharing is developed. Algorithm 1 recommends pick-up points for RDs and shortest routes for COs based on their LVRs.

The recommendation phase involves social and location network (SLN), which has the previous location records of the RDs and COs at every instant of time; city transport management (CTM,) which keeps the records of COs and RDs; and RCR who executes the algorithm.

To request for a best shortest route for CO or best PuP for RD from RCR, the scheme executes the following procedure:

- CO composes its request packet consisting of L_{co}; D_{co};; T_{co};, encrypts it, using its $ssk_{co \longmapsto rcr}$, as $Erq_{co} = E_{ssk_{co\longmapsto rcr}}(L_{co}; D_{co};; T_{co}) \| \mathcal{F}_{co}$, and sends it to RCR. RD also composes its request packet consisting of L_{rd}, D_{rd}, T_{rd}, Rq_{type} encrypts it as $Erq_{rd} = E_{ssk_{rd\longmapsto rcr}}(L_{rd}; D_{rd},\ \ T_{rd}, Rq_{type}) \| \mathcal{F}_{rd}$. On receiving Erq_{co} and Erq_{rd}, RCR decrypts Erq_{co} using $ssk_{rcr \longmapsto co}$, and Erq_{rd} using $ssk_{rcr \longmapsto rd}$.

Table 1 Symbols and Notations

Notation	Description
Z_p	set of integer of order p
G	additive cyclic group of order q
$F_{a\mapsto b}$	trust value of entity a on b
RD, CO	Rider and car owner
M_{SY}	location visitor record matrix of RDs and COs
M_{TY}	location visitor record matrix of CO
$\varphi_{a\mapsto b}$	success rating of entity a on b
$\varphi'_{a\mapsto b}$	failure rating of entity a on b
$M_{ty}(a, l)$	total number of check-ins entity a made on location l at time t
$M_{sy}(a, l)$	total number of check-ins entity a has made on location l up till the current time
C_{rcr}	RCR public key
$qrcr$, $qctm$, qrd	exchange public parameters of RCR,CTM, and RD, respectively
$H(.)$	One-way collision-resistant non-key based hash function
L_{co}, D_{co}	current location and destination of CO
L_{rd}, D_{rd}	current location and destination of RD
P	generator of cyclic group G
$\beta_{a\longmapsto l}$l	similarity metric of entity a and location l
$ssk_{rcr\mapsto rd}$, $ssk_{co\mapsto rcr}$	symmetric shared key between rcr and rd, co and rcr
$ssk_{rcr\mapsto ctm}$	symmetric shared key between rcr and ctm
MSY; MTY	check-in record matrices
e	bilinear function
$\|$	concatenation operator
D_0	connected distance matrix
Q_0	pick up points matrix
ϑ	authentication code
RSQ	ride sharing token
wrd, wco	authentication session parameters of RD and CO,
$\beta_{rd\mapsto co}=\beta_{co\mapsto rd}$	riding secret key between RD and CO
$\gamma_{co}=\gamma_{rd}$	riding tokens of CO and RD
$\mathcal{F}_{co}$, $\mathcal{F}_{rd}$	pseudonyms of CO and RD, respectively

- RCR then requests for the encrypted trust value matrix $E_{ssk_{ctm\longmapsto rcr}}(V_c)$ of RDs and COs from CTM and $M_{ty}(a, l)$, $M_{sy}(a, l)$ of RDs and COs from matrices M_{SY} and M_{TY} resided with LBS.
- RCR generates graph B by requesting for encrypted V_c, matrices M_{SY} and M_{TY} from CTM and SLN, respectively. Then, decrypts and generates similarity metrics between each of the registered RDs and all the locations in M_{ty} using Eq. 2. It selects the best PuP for each RD, as the location with the highest similarity metric, to evolve the list of predictive best PuP for all the registered RDs at time t. The list with the current location of the RD and destination of the CO is then used to form graph

$B \in G$. Each best PuP in B is connected with edges to its neighboring best PuP(s) as shown in Fig. 2, where $D_{i,j}$ represents the distance between the connected PuPs i and j.

- RCR then generates connected distance matrix D_0 and PuP matrix Q_0. It formulates $n \times n$ matrix Q_0 whose elements are the predecessor node i of all the connecting PuPs i and j of the graph B otherwise the element is represented as '-'. Once $n \times n$ matrix Q_0 is generated, RCR executes algo-rithm 1 to generate the shortest route between the CO's initial location and its destination in such a way that the shortest route has a minimum number of potential RDs along the CO's route. Line 1 of algorithm 1 generates the distance matrix D^k which contains the shortest distance be-tween PuPs using the improved Floyd technique. Using procedure 1, it first finds the shortest route between the CO's location and the RD's location. Then, finds the shortest route between the RD's location and CO's destination by repeating procedure 1. Aggregation of these two shortest routes forms the shortest route between the CO and his final destination through the RD's PuP. The optimal route must contain the RD's pick up point and/or his destination.

Meanwhile, algorithm 2 is used by COs to determine the type of ride-sharing. If the RD's destination is the subset of the shortest route, then the ride-sharing is a normal 1-to-n ride-sharing otherwise collaborative 1-to-n ride sharing. Collaborative ride-sharing involves the original CO handling over his RD to another CO so that the RD completes his ride to his final destination.

4.3 Mutual Authentication between RD and CO

After matching, the CO initiates mutual authentication with the RD or second CO in case of collaborative ride sharing through the following steps:

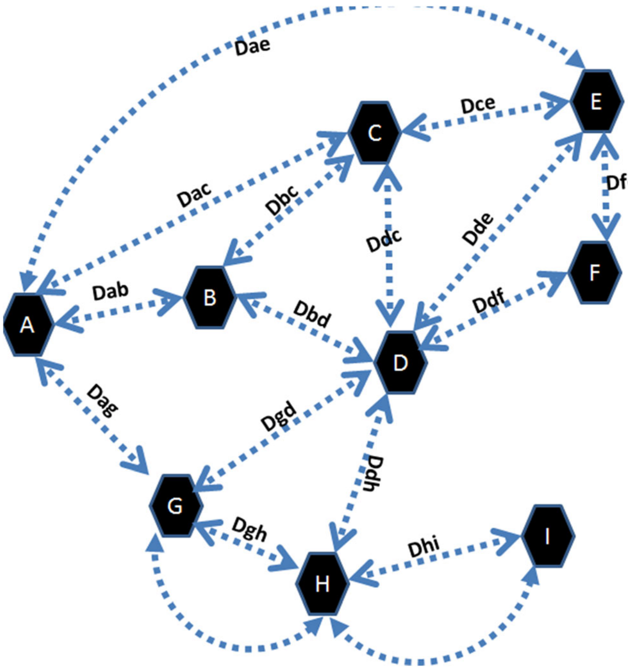


Fig. 2 Predictive graph for best pick-up-points of the registered RDs

Algorithm 1 Optimal Ride Sharing Route

Input: CO-request, RD-request, D_0, Q_0

Output: $CO_{shortest-route}$, Z, RD-PuP

```
RCR computes nxn matrix $D_k$ whose elements are the distance between nodes $i$ and $j$, and nxn matrix $Q_k\ for\ k = 1,2\ldots N$, whose elements are the predecessor nodes of all the nodes in the shortest paths of a graph G

 {To generate shortest route matrices $D_k$ and $Q_k$ }
for $k = 1;\ k\ \ n;\ k++$ do
    for $i = 1;\ i\ \ n;\ i++$ do
        for $j = 1;\ j\ \ n;\ j++$ do
            $D_{k+1}[i][j] = \min(D_k[j];\ D_k[i][k] + D_k[k][j])$
            if $D_{k+1}[i][j] \neq D_k[i][j]$ then
                $Q_{k+1}[i][j] = k$
            end if
        end for
    end for -
end for
PROCEDURE 1:
{To generate the optimal route $Z_{rd\rightleftharpoons co}$ and its distance $D_{rd\rightleftharpoons co}$ }
$Z_{rd\rightleftharpoons co} = \{\}$
$D_{rd\rightleftharpoons co} = 0$
$Z_{rd\rightleftharpoons co}[0] \leftarrow L_{co}$   {assign the current location of the CO as the  first element $Z_{rd\rightleftharpoons co}$}
$b \leftarrow L_{rd}$          {assign the location of the RD to temporary variable b}
$m \leftarrow 0$
while $Z_{rd\rightleftharpoons co}[m] = L_{rd}$ do
    $Z_{rd\rightleftharpoons co}[m+1] = Q_n(Z[m], b)$
    $D_{rd\rightleftharpoons co} \leftarrow D_{rd\rightleftharpoons co} + D_n(Z_{rd\rightleftharpoons co}[m], L_{rd})$  {compute the distance between the CO and RD}
    $m \leftarrow m + 1$
    if $Z_{rd\rightleftharpoons co}[m] == Z_{rd\rightleftharpoons co}[m-1$ then
    $Z_{rd\rightleftharpoons co}[m] \leftarrow b$
    Exit
    else
    continue
    end if
end while
END PROCEDURE 1 { compute shortest route between RD's location $L_{rd}$ and CO's destination $D_{co}$ }
If $L_{rd} \neq D_{co}$ then
$L_{rd} = L_{co}$                    {replace Co’s location $L_{co}$ with RD’s location $L_{rd}$}
$L_{rd} \leftarrow D_{co}$                          {replace $L_{rd}$ with $D_{co}$}
$D^*_{rd\rightleftharpoons co} = D_{rd\rightleftharpoons co}$
$Z^*_{rd\rightleftharpoons co} = Z_{rd\rightleftharpoons co}$
$D_{rd} \leftarrow D^*_{rd}$
Repeat PROCEDURE 1
**else**
    Exit
**End if**
CO-shortest-route ← $Z_{rd\rightleftharpoons co}||Z^*_{rd\rightleftharpoons co}$
CO-shortest-distance ← $D_{rd\rightleftharpoons co}||D^*_{rd\rightleftharpoons co}$
```

Algorithm 2 Optimal RD for ride sharing

```
Input: $D_{co}$; $D_{rd}$
Output: r$equest_{type}$
    if $D_{rd} \subset D_{co}$ and $T_{rd} \subset T_{co}$ then
        match RD and CO for normal ride-sharing
    else
        the CO matches the RD for collaborative ride-sharing
        the CO negotiates RD for another CO
end if
```

4.2.3. Matching of RDs with CO for 1-to-n ride sharing

On getting to the RD's best PuP, both the CO and RD send matching requests to RCR, who then generates matching parameters for the RD and CO as described below.

- RCR randomly generates a unique authentication code #, symmetrically encrypts and sends it as $\vartheta_{rd} = \vartheta \oplus ssk_{rcr \to rd}$ and $\vartheta_{co} = \vartheta \oplus ssk_{rcr \to co}$.
- matches them by sending the ride sharing token $RSQ_{rd} = Rqs \| \mathcal{F}_{rd} \| t_s \| q_{rd} \| \vartheta_{co}$ to the RD and $RSQ_{co} = Rqs \left\| t_s \| q_{rd} \| \vartheta_{rd} \right\| CO_{shortest-route}$to the CO. However, if it is a collaborative RD sharing, RCR sends: $RSQ_{old} = Rqs \| \mathcal{F}_{new} \| t_s \| q_{new} \| \vartheta_{new}$ to the old CO and sends $RSQ_{new} = Rqs \| \mathcal{F}_{new} \| t_s \| q_{new} \| \vartheta_{new}$ to the new CO.

Step 1: RD and CO randomly generate $\phi_1 \in Z^*$ and $\phi_2 \in Z^*$, respec-tively. RD computes and publishes its authentication sessional parameter as $w_{rd} = \phi_1 P$, and CO also computes and publishes authentication sessional parameter as $w_{co} = \phi_2 P$. On receiving CO's w_{co}, RD computes its riding secret key with CO as $\beta_{rd \mapsto co} = \phi_1 w_{co}$ while CO also computes its riding secret key with RD as $\beta_{co \mapsto rd} = \phi_1 w_{rd}$ such that $\beta_{rd \mapsto co} = \beta_{co \mapsto rd}$

Step 2: The RD and CO use their corresponding ssk with RCR to decrypt the received ϑ_{co} or ϑ_{rd} from RCR to obtain ϑ.

Step 3: To authenticate the CO by RD, CO performs the following

- generates unique riding token γ_{co} as: $\gamma_{co} = H_{\beta_{co \mapsto rd}}(\vartheta)$
- CO then symmetrically encrypts the riding token as $E_{\beta_{co \mapsto rd}}(\gamma_{co})$, and sends it to the RD.
- The RD, using its session secret key with CO, $\beta_{co \mapsto rd}$ decrypts the received $E_{\beta_{co \mapsto rd}}(\gamma_{co})$, and generates his own $\gamma_{rd} = H_{\beta_{rd \mapsto co}}(\vartheta)$. If $\gamma_{co} = \gamma_{rd}$then CO has been successfully authenticated and move to the next step.

Step 4: To authenticate the RD by CO, RD performs the following:

- RD computes his unique riding token γ_{rd} as: $\gamma_{rd} = H_{\beta_{rd \mapsto co}}(\vartheta)$
- RD, using its session secret key $\beta_{rd \mapsto co}$, encrypts the riding token as $E_{\beta_{rd \mapsto co}}(\gamma_{rd})$, and sends it to the CO.
- CO decrypts the received $E_{\beta_{rd \mapsto co}}(\gamma_{rd})$, and compare it with his own γ_{co}. If $\gamma_{co} = \gamma_{rd}$, RD is successfully authenticated

5 Security and Privacy Analysis

In this section, we show that the proposed ride-sharing scheme achieves all the necessary security requirements to allay the fear of the COs and RDs on the adoption of 1-to-n ride sharing.

1. Integrity: Integrity during ride-sharing is guaranteed by the scheme through the following ways.

Table 2 Computational costs of various cryptographic operations

Cryptographic operation	Symbol	Execution time
Point multiplication	T_{sm}	0.6 ms
SHA-256 hash function	T_{hash}	7:81X10 ^{4}ms
Symmetric key encryption or decryption	$T_{\mathrm{enc=dec}}$	10:51X10 ^{4}ms
bilinear pairing	T_{bp}	1:6 ms
Modular exponential (Di e Helman)	T_{ex1}	13:22 ms
Modular exponential (Chinese remainder theorem)	T_{ex2}	12:66 ms

(a) Authenticity: The mutual authentication between RDs and COs with the involvement of RCR not only ensures that only the registered COs and RDs partake in ride-sharing but also done with the matched RDs and COs. The scheme achieves this using the unique ride-sharing token # generated by the RCR to match the CO with the RD. This is encrypted with the *ssk* of the matched RD and CO, and RCR to ensure its integrity. Also, riding token $\gamma_{co} = H_{\beta_{co\leftrightarrow rd}}(\vartheta)$ or $\gamma_{rd} = H_{\beta_{rd\leftrightarrow co}}(\vartheta)$ depends on the key-based hash function, whose security depends on one way characteristic of the key-based hash function and intractability of DL and CDH problems, respectively. Therefore, no attacker can impersonate registered and matched RD or CO by forging ride-sharing and riding tokens during ride-sharing in as much the DH and CDH problems remain intractable and the used hash function has one-way property.

(b) Confidentiality: Apart from other integrity requirements achieved by the proposed scheme, we engaged symmetric encryption with a secure key distribution approach to provide confidentiality. The major problem of symmetric encryption is key distribution; we solved this using a 2-way key exchange approach. The approach security de-pends on the scalar multiplication whose security depends on DL and CDH problems. These problems had been proved to be intractable, therefore there is no way the unique authentication code ϑ, which is encrypted with $ssk_{rcr\mapsto rd}$ whose security is anchored on intractable problems.

2. Privacy: We preserve RDs' and COs' privacy by ensuring all the request transactions are done using their pseudonyms. In the scheme, each entity is given a non-linkable pseudonym generated from $\mathcal{F}_{rd} = H_{\beta}(Id_{rd})$ for RD, and $\mathcal{F}_{co} = H_{\beta}(Id_{co})$ for CO. The pseudonym depends on the hash function H and master key β, and once the hash function exhibits one-way property and is randomly generated, no adversary can forge pseudonym, thus privacy is maintained.

6 Performance Analysis

In this section, we analyze the efficiency and cost of the proposed scheme based on the computational cost of the

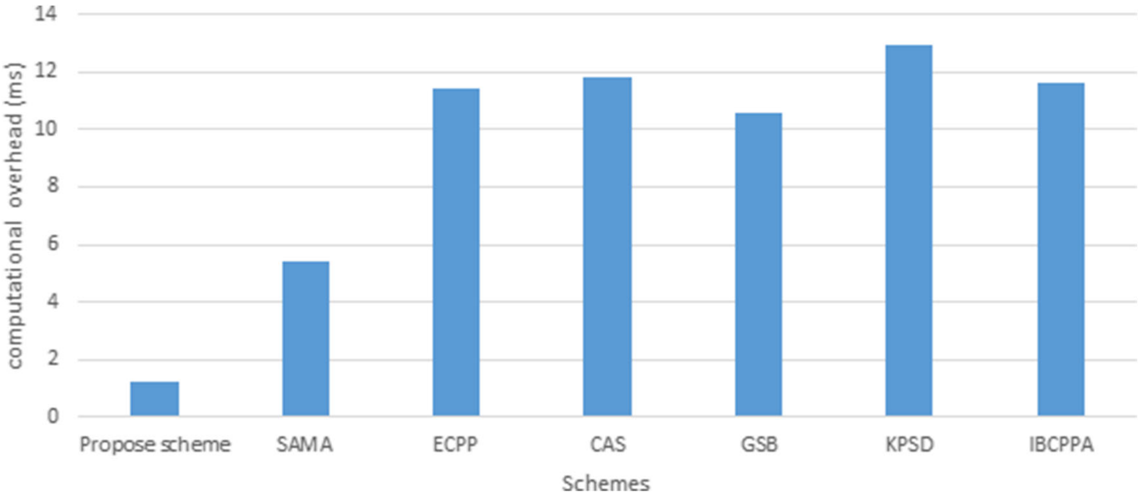


Fig. 3 Comparison of computational overheads of the proposed scheme authentication with other vehicular ad-hoc networks' (VANETs) authentication schemes

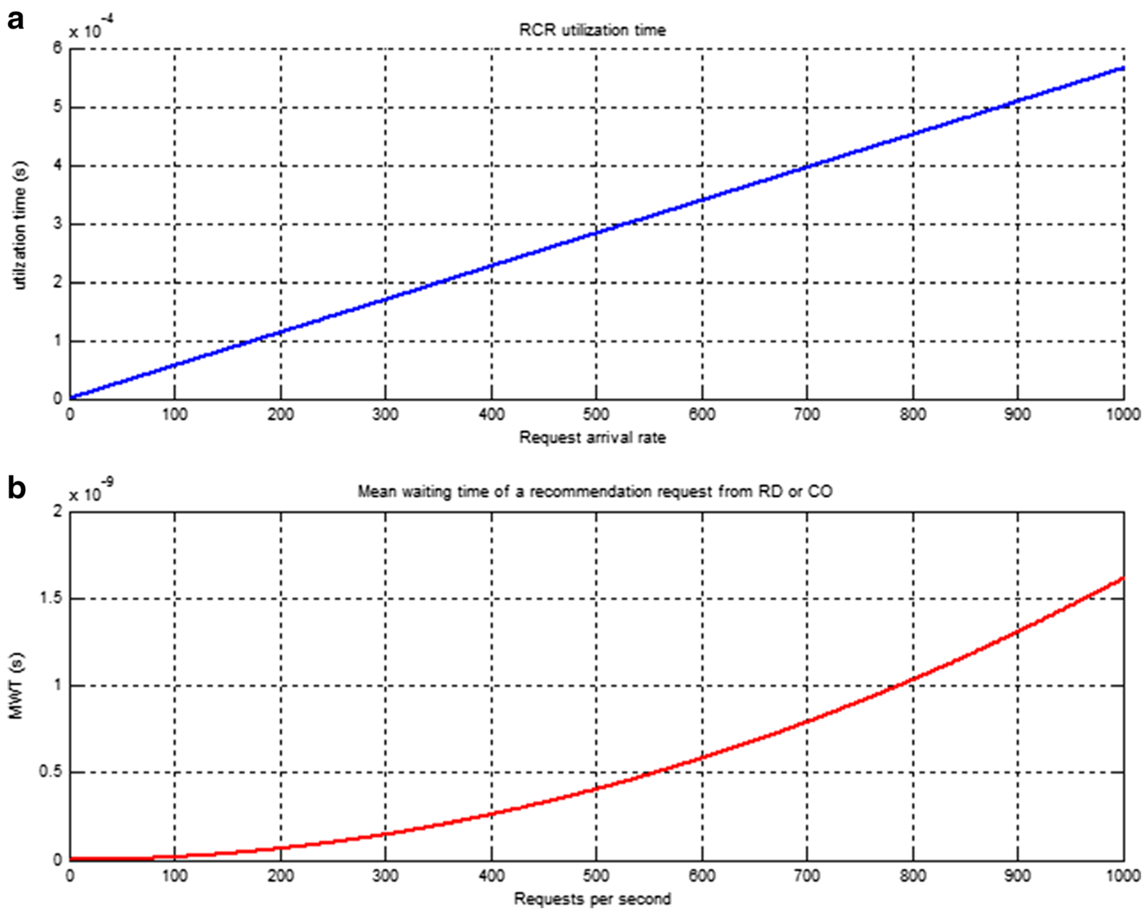


Fig. 4 Utilization time and Mean waiting time of RCR for different recommendation request in the proposed scheme

proposed mutual authentication, fairness of service and capacity in terms of mean waiting time (MWT), and capacity overshoot of the scheme. The computational cost signifies the computational complexity of the mutual authentication of the scheme and is used to determine whether RDs and COs will be able to handle the computational requirement of the scheme. Meanwhile, the capacity and fairness of service show how the RCR can handle different numbers of recommendation requests from CO and RD, and the matching capabilities of RD and CO.

6.1 Computation Cost

To analyze the computation cost incurs on mutual authentication, we simulate each of the cryptographic operations used in the proposed scheme and the schemes in [24, 28–32], using a cryptoPP library [33, 34] implemented on Intel(R) Core (TM)i3 2.73GHz. We assumed all the symmetric and asymmetric encryptions are implemented using the Advance encryption standard with cipher block chaining (AES-CBC) as adopted in [35]. Also, SHA-256 is adopted for all the key and non-key based hash operations. The execution times of all the cryptographic operations are summarized in Table 2. In the pro-posed scheme, each RD takes $2T_{sm} + T_{hash} + T_{enc} = 1.2ms$, while CO takes $2T_{sm}+T_{hash} + T_{enc} = 1.2ms$for mutual authentication. Meanwhile, RCR takes $T_{xor} + 4T_{enc} + T_{alg} = 5.6750e^{-3}ms$ for every recommendation request.

Mean-while, SAMA, ECPP, CAS, GSB, KPSD and IBCPPA, schemes take $5.4ms$, $11.4ms$, $11.8ms$, $10.6ms$, $12.9ms$ *and* $11.6m$, respectively to authenticate an entity for a message service request. Referencing Figure 3, the proposed scheme's authentication procedure has the lowest computational overhead compared to the authentication schemes in SAMA [24], ECPP [28], CAS [29], GSB [30], KPSD [31], and IBCPPA [32].

6.2 Capacity and Fairness of Service

The capacity of RD, CO, and RCR and fairness of service in the proposed scheme are evaluated. Figure 4 shows the utilization and mean waiting time of RCR and RD or CO, respectively for different request arrival rates. To analyze the capacity of each entity in the scheme, we use the mean waiting time (MWT) and *rth*

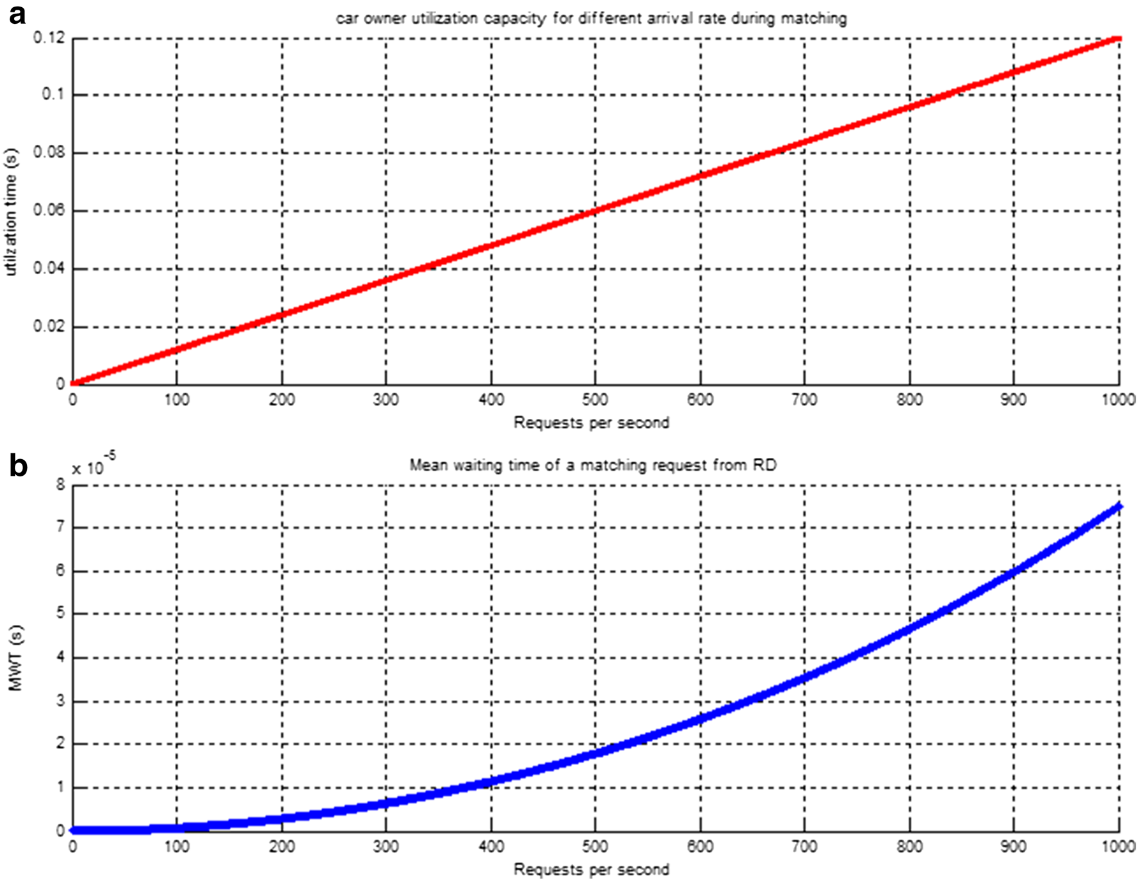


Fig. 5 Utilization time and Mean waiting time of RD for different matching request in the proposed scheme

percentile. The rth percentile is the probability that fewer k number of RDs or COs are in the RCR's queue, fewer RDs are in the CO's queue, and fewer COs are in the RD's queue for different utilizations and queue lengths. This is used to determine the capacity of RCR and CO. Meanwhile, MWT indicates the amount of time either RD's or CO's request wait before being serviced. As indicated in Figures 4a and 5a, the utilization times of COs and RCR increase as they receive more requests from either RDs and/or COs. Referencing Figure 6, the best utilization of RCR is at 0.9. At this utilization, RCR has a queue capacity of 40 for ROs and COs. This shows that the RCR exhibits the characteristic of a good server, thus reducing delay during high traffic of service requests. All these indications show that none of the requests from any entity will be delayed due to high request-traffic in the proposed scheme.

7 Conclusion

1-to-n collaborative ride-sharing solves some of the fundamental issues in the public transportation system. It does not only offer a cheap means of mobility but also reduces crimes associated with bus stops and terminals in other city's public transportation systems. Additionally, it does not rely on set schedules and services provided for a few areas. However, its major problems are how to match the RDs and car owners, determine the shortest route, and ensure security and privacy. In this paper, we solve this by using RDs and car owners' previously visited location records to determine the daily route of the RDs and car owners without compromising their privacy. We came up with an algorithm that efficiently selects the shortest route with a high number of potential RDs for the car owners. Besides, the proposed trust and rating models for the collaborative 1-to-n ride-sharing can curtail abuse in the system. Besides, compared with other transportation schemes, 1-to-n collaborative ride-sharing solves most of the city's public transportation problems and increases the economy of the car owners and RDs. The results show that the mutual authentication procedure of the scheme has the lowest computational cost compared with other state-of-the-art authentication schemes. This reduces the service-delay of the proposed scheme as affirm by the insignificant increase of the mean waiting time as the number of requests increases.

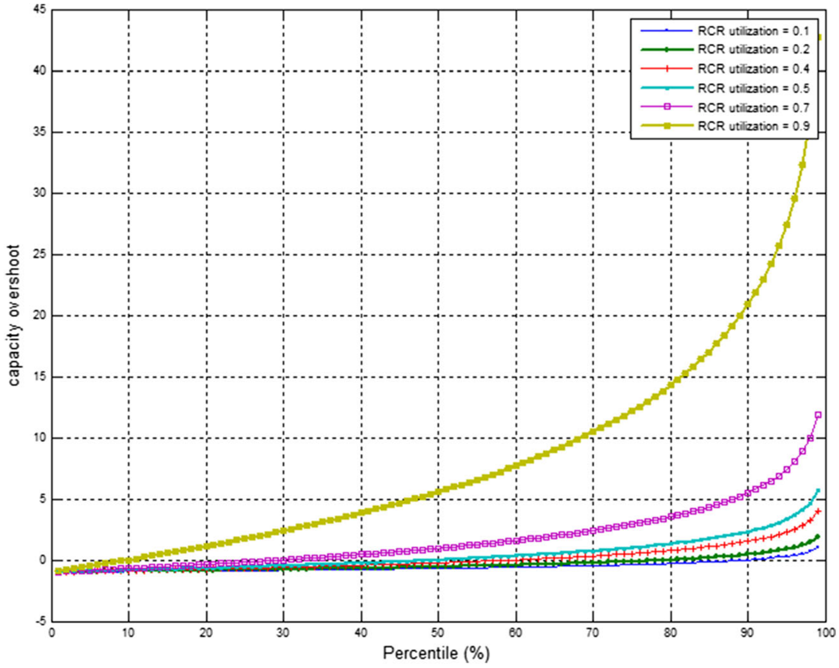


Fig. 6 Utilization time and Mean waiting time of RD for different matching request in the proposed scheme

References

1. Furuhata, M., Dessouky, M., Ordonez, F., Brunet, M., Wang, X., Koenig, S.: Ridesharing: the state-of-the-art and future directions. Transp. Res. B Methodol. **57**, 28–46 (2013)
2. Goel, P., Kulik, L., Ramamohanarao, K.: Optimal pick up point selection for Effective ride sharing. IEEE Trans. Big Data. **3**(2), 154–168 (2017). https://doi.org/10.1109/TBDATA.2016.2599936
3. Chaubey, N.: Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study. Int. J. Secur. Appl. **10**(5), 261–274 (2016)
4. He, Y., Ni, J., Wang, X., Niu, B., Li, F., Shen, X.: Privacy-preserving partner selection for ride-sharing services. IEEE Trans. Veh. Technol. **67**(7), 5994–6005 (2018)
5. Shao, J., Lu, R., Lin, X., Zuo, C.: New Threshold Anonymous Authentication for VANETs, in Proc. IEEE/CIC ICCC, Shenzhen (2015)
6. Farin, N.J., Rimon, M.N.A.A., Momen, S., Uddin, M.S., Mansoor, N.: A framework for dynamic vehicle pooling and ride-sharing system, pp. 204–208. 2016 International Workshop on Computational Intelligence (IWCI), Dhaka (2016)
7. Litman, T.: Autonomous vehicle implementation predictions Implications for transport planning. Transportation Research Board 94th an-Nual Meeting, Washington DC (2015)
8. Mustafa, A. Mustafa, N.Z., Georgios, K., Zhong, F.: Roaming electric vehicle charging and billing: an anonymous multi-user protocol, IEEE International Conference on Smart Grid Communications (SmartGridComm) (2014)
9. Zhao, T., Chen, C., Wei, L., Yu, M.: An anonymous payment system to protect the privacy of electric vehicles. Sixth International Conference on Wireless Communications and Signal Processing (WCSP) (2014)
10. Kokalj-Filipovic, S., Le Fessant, F.: Personal Social Graph as an Anonymous Vehicle for P2P Applications: The cost of renting trusted connections. 44th Annual Conference on Information Sciences and Systems pp. 1–6 (2010)
11. Sherif, A.B.T., Rabieh, K., Mahmoud, M.M.E.A., Liang, X.: Privacy-preserving ride sharing scheme for autonomous vehicles in big data era. IEEE Internet Things J. **4**(2), 611–618 (2017)
12. Di Febbraro, A., Sacco, N., Saeednia, M.: One-way Car-sharing profit maximization by means of user-based vehicle relocation. IEEE Trans. Intell. Transp. Syst. **20**(2), 628–641 (2019)
13. Bathla, K., Raychoudhury, V., Saxena, D., Kshemkalyani, A.D.: Real-Time Distributed Taxi Ride Sharing, 21st International Conference on Intelligent Transportation Systems (ITSC), pp. 2044–2051. Maui, HI (2018)
14. D'Andrea, E., Di Lorenzo, D., Lazzerini, B., Marcelloni, F., Schoen, F.: Path Clustering Based on a Novel Dissimilarity Function for Ride-Sharing Recommenders, pp. 1–8. IEEE International Conference on Smart Comput-Ing (SMARTCOMP), St. Louis (2016)
15. Shen, B., Cao, B., Zhao, Y., Zuo, H., Zheng, W., Huang, Y.: Roo: Route Planning Algorithm for Ride Sharing Systems on Large-Scale Road Networks, pp. 1–8. IEEE International Conference on Big Data and Smart Comput-Ing (BigComp), Kyoto (2019)
16. Wei, Z., Yanjiang, Y., Wu, Y., Weng, J., Deng, R.H. (2017). HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive, IEEE Access, **5**
17. Liu, A., Wang, W., Li, Z., Liu, G., Li, Q., Zhou, X., Zhang, X.: A privacy-preserving framework for trust-oriented point-of-interest Recom-mendation. IEEE Access. **6**, 393–404 (2018)
18. Mayadunna, H., Rupasinghe, L.: A trust evaluation model for online social networks, National Information Technology Conference (NITC), Colombo, pp. 1–6 (2018)
19. Olakanmi, O., Sekoni, O.: A trust based secure and privacy aware framework for efficient taxi and car sharing system. Int. J. Vehicular Telematics Infotainment Sys. **2**(1), (2018)
20. Yang, X., Wu, J., Dang, Y., Rong, L.: A product recommendation approach based on the latent social trust network model for collaborative filtering, pp. 178–185. IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Vienna (2016)
21. Samanthula, B.K., Rao, F., Bertino, E., Yi, X.: Privacy-Preserving Protocols for Shortest Path Discovery over Outsourced Encrypted Graph Data, pp. 427–434. IEEE International Conference on Information Reuse and Integration, San Francisco (2015)
22. Azeez, M., Vijayakumar, P., Deboarh, L.: EAAP: efficient anonymous authentication with conditional privacy-preserving scheme

for vehicular ad hoc networks. IEEE Trans. Intell. Transport. Syst. **18**(9), 2467–2476 (2017)
23. Olakanmi, O.: SAPMS: a secure and anonymous parking management system for autonomous vehicles. Int. J. Inform. Comput. Secur. **12**(1), 20–39 (2020)
24. Olakanmi, O., Dada, A.: SAMA: a secure and anonymous mutual authentication with conditional identity-tracking scheme for a unified car sharing system. Int. J. Autom. Control. **13**(1), (2019)
25. Lin, X., Sun, X., Ho, P.-H., Shen, X.: GSIS: a secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Technol. **56**(6), 3442–3456 (2007)
26. Olakanmi, O., Dada, A.: FELAS: fog enhanced look ahead secure framework with separable data aggregation scheme for efficient information management in the internet of things networks. J. Appl. Secur. Res. **14**(4), (2019)
27. Boneh, D., Gentry, C., Lynn, B., Shacham, H.: Aggregate and verifiably encrypted signatures from bilinear maps. Proceeding of Adv. Cryptol. Eurocrypt. **2003**, 416–432 (2003)
28. Lu, R., Lin, X., Zhu, H., Ho, P., Shen, X.: ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In: Proceeding of IEEE INFOCOM, pp. 1229–1237. (2008)
29. Gong, Z., Long, Y., Hong, X., Chen, K.: Two certicateless aggregate signatures from bilinear maps. Proc. 8th ACIS Int. Conf. Softw. Eng. Artificial Intell. Network Parallel Distrib. Comput. (SNPD). **3**, 188–193 (2007)
30. Lin, X., Sun, X., Ho, P.H., Shen, X.: GSIS: A secure and privacy-preserving protocol for vehicular communications. IEEE Trans. Veh. Tech-nol. **56**(6), 3442–3456 (2007)
31. Lu, R., Lin, X., Luan, T.H.: Pseudonym changing at social spots: An effective strategy for location privacy in VANETs. IEEE Trans. Veh. Technol. **61**(1), 86–96 (2012)
32. Shao, J., Lin, X., Lu, R., Zuo, C.: A threshold anonymous authentication protocol for VANETs. IEEE Trans. Veh. Technol. **65**(3), 1711–1720 (2016)
33. Shamus Software Ltd., Miracl library, Available: http://www.shamus.ie/index.php?page=home
34. Pairing-Based Cryptography Library. [Online]. Available: http://crypto.stanford.edu/pbc/
35. Gope, P., Hwang, T.: Lightweight and energy-efficient mutual authentication and key agreement scheme with user anonymity for secure communication in global mobility networks. IEEE Syst. J. **10**(4), 1370–1379 (2016)
36. Li, H., Dan, G., Nahrstedt, K.: Lynx: authenticated anonymous real-time reporting of electric vehicle information, pp. 599–604. IEEE International Conference on Smart Grid Communications (SmartGridComm), Miami (2015)
37. Jung, C.D., Sur, C., Park, Y., Rhee, K.-H.: A Robust and Efficient Anonymous Authentication Protocol in VANETs. J. Commun. Netw. **11**, 6 (2009).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Oladayo O. Olakanmi received B.Tech in Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria. He obtained M.Sc. in Computer Science and Ph.D. in Electrical and Electronic Engineering, University of Ibadan, Nigeria. He is a Senior Lecturer in the Department of Electrical and Electronic Engineering, University of Ibadan.

A visiting scholar in Tennessee Technology University, Cookeville, USA in 2016, and a Fellow of MIT-ETT in Massachusetts Institute of Technology (MIT), Cambridge, USA. He was a key member in several projects supported by Nigerian Communications Commission and University of Ibadan. His main research interests include applied cryptography, information security, and embedded systems. He has served as a program committee member in dozens of international conferences. He has published numerous publications in the area of applied cryptography, information security, and embedded systems.

Kehinde Oluwasesan Odeyemi received his B.Tech. degree in Electronic Engineering from Ladoke Akintola University of Technology Ogbomosho, Oyo State, Nigeria, in 2008. He later obtained an M.Eng. degree in the same field from the Federal University of Technology, Akure in 2012. He received his Ph.D. degree in Electronic Engineering at the University of KwaZulu-Natal, Durban, South Africa in 2018. Currently, he is in the department of Electrical and Electronic Engineering, University of Ibadan, Nigeria as a Lecturer. He is a member of The Council for the Regulation of Engineering in Nigeria (COREN). He has written several research articles and his research interests are in the antenna design, optical wireless communications, diversity combining techniques and MIMO systems.