Multiagent/Multiobjective Interaction Game System for Service Provisioning in Vehicular Cloud

Moayad Aloqaily, *Student Member, IEEE,* Burak Kantarci, *Senior Member, IEEE,* and Hussein T. Mouftah, *Life Fellow, IEEE*

***Abstract* — The increasing number of applications based on the Internet of Things (IoT), as well as advances in wireless communication, information and communication technology, and mobile cloud computing, has allowed mobile users to access a wider range of resources when mobile. As the use of vehicular cloud computing has become more popular due to its ability to improve driver and vehicle safety, researchers and industry have a growing interest in the design and development of vehicular networks for emerging applications. Vehicle drivers can now access a variety of on demand resources en route via vehicular network service providers. The adaptation of vehicular cloud services faces many challenges, including cost, privacy and latency. The contributions of this paper are as follows: First, we propose a game theory-based framework to manage on-demand service provision in a vehicular cloud. We present three different game approaches, each of which helps drivers minimize their service costs and latency, and maximize their privacy. Secondly, we propose a Quality-of-Experience (QoE) framework for service provision in a vehicular cloud for various types of users; a simple but effective model to determine driver preferences. Third, we propose using the Trusted Third Party (TTP) concept to represent drivers and service providers, and ensure fair game treatment. We develop and evaluate simulations of the proposed approaches under different network scenarios with respect to privacy, service cost and latency, by varying the vehicle density and driver preferences. The results show that the proposed approach outperforms conventional models, since the game theory system introduces a bounded latency of ≤ 3%, achieves service cost savings up to 65%, and preserves driver privacy by reducing revealed information by up to 47%.**

***Keywords* — Cloud computing, vehicular cloud computing, game theory, auction theory, quality of experience, mobile cloud computing, privacy, service provisioning, latency.**

I. Introduction

Over the past two decades, development and introduction of cloud-based solutions and architectures has transformed the Information and Communication Technology (ICT) [1] field, and cloud and mobile cloud computing have been the main areas of study [2][3]. Cloud-based frameworks have motivated research communities and industry to explore the benefits of migrating to other cloud-inspired environments, such as vehicular clouds.

Vehicular cloud computing has become a significant topic of research over the past few years, since cloud-inspired operation of vehicular networks can involve domains such as Intelligent Transport Systems (ITS), safety, surveillance systems and emergencies [4][5]. Vehicular cloud also has a wide-range of on-demand applications and services, including multimedia streaming, content sharing, traffic management, road safety and storage. Important related work on vehicular clouds is intended to design, evaluate and develop new solutions that provide services to drivers in case of emergencies, such as collisions, traffic jams and safety alarms [6]. Other objectives include making drivers more comfortable and enhancing access to information en-route.

Typically, any smart vehicle can act as a mobile storage and/or a processing unit, thanks to the many available on-board resources and services which provide an ideal environment for public service and safety. Although vehicular clouds have a broad range of benefits and advantages for various domains and applications, several obstacles need to be addressed before they can become widely adopted. From the standpoint of vehicle drivers, privacy, service cost and latency are the most crucial challenges to be addressed in such environments [7][8][9].

The security and privacy challenges inherent with vehicular cloud systems have been studied less closely than other issues. Besides the security of the communication medium, the main drawback with security and privacy is the lack of control over data stored and/or processed over virtual and distributed resources [10]. Service cost and latency are other concerns for drivers, since these affect each other in on-demand service provisioning [11][12].

Due to vehicle mobility and the unpredicted topology of the vehicular network, it is very challenging to control the aforementioned three aspects [13] simultaneously. A vehicular network consists of several vehicles moving at higher speeds than in typical mobile cloud environments, which makes it very difficult for the driver and the service provider to manage the network connections. Frequent topology changes can cause extended delays, which means increased cost for drivers. The use of a reliable, well recognized Trusted Third Party (TTP) between drivers and service providers to handle the communications will resolve these potential aspects of the greater problem.

An auction-driven, multi-objective provisioning framework, with the support of the existing trusted third party approach and the Quality-of-Experience (QoE) model, has been proposed to address these challenges [14]. Auction interactions require an $n \times n \times n$ auction model, and the drawbacks of these models include delay and auction complexity. The delay has a significant impact on service charges, since drivers are charged by time used.

In this paper, we propose using game theory concepts with a *QoE-awareness* system model, to provide drivers with provisioning services in a vehicular environment at low latency, minimum cost and minimal driver information revealed. *QoE-awareness* collects requirements and preferences, and defines a QoE value for every service provider, trusted third party and driver in each game. Our proposed framework is a Multiagent/Multiobjective Interaction Game System (MMIGS) for on-demand provisioning services in vehicular clouds. Through simulations, we evaluate the proposed framework in different network scenarios, with respect to driver privacy, service cost and latency. The results show that the proposed framework provides improvements over other conventional models in terms of these metrics. Service cost and privacy improved by 65% and 47%, respectively. Though these improvements mean drivers will experience some extra delay, using QoE-awareness has helped reduce such delays an average of 3%, compared to the total delay in other models.

The balance of the paper is organized as follows. Section II summarizes the related work in this area. Section III provides an overview of the QoE-based framework. Section IV presents the game-based of the QoE framework. Section V and VI describe the proposed game system models and analysis of the outcomes, respectively. Section VII provides performance evaluation and simulation results. And Section VIII presents the conclusions and discusses future directions.

II. RELATED WORK

Vehicular clouds offer a wide range of benefits for various environments and applications, though many open issues and challenges remain unresolved. In this section, we review the main challenges and notable solutions.

Security and privacy issues in vehicular communications have been explored by many academic researchers and by industry. Various solutions for these concerns have been proposed, including pseudonym identity, anomaly detection schemes, public or anonymous keys and digital signature verification, and have been widely investigated [15][16][17][18][19][20].

In [15], the authors proposed a framework called personal data vaults, which was designed to control and protect the stream of users' personal data. The use of this framework allows only the main owners access to their data, and though it is an individually controlled method for data repositories it does not guarantee users' anonymity. One of the main objectives of privacy is to protect user identity, and sometimes hide it, yet there is no viable solution to address the anonymity issue in vehicular clouds. Researchers in [16] studied the importance of information collection in smart cities, and identified the privacy threats. They proposed a privacy-enhancing architecture using an adaptive pseudonymization technique, to provide real-time awareness and enhance privacy security.

Pseudonym identity [17][18][19][20] has been considered a solution to protecting user identities. In [17], the authors proposed a protocol based on pseudonymity to reduce the possibility of discovering the identity of drivers from their sent data. Such a protocol could be considered for communication between vehicles when they share resources and data en-route. A feasible protocol that enables resource and data sharing between vehicle drivers and cloud providers has not yet been developed. Similarly, the authors in [18][19] proposed a non-pseudonym strategy based on Tamper Resistant Hardware (TRH) to avoid proliferation of vehicle identities. This approach has a negative impact on routing efficiency, and handling and discovering malicious vehicles trying to get the benefits of these protocols has not been addressed. Anomaly detection schemes can be considered for such problems [21][22].

Anomaly detection schemes can be used for data analysis, and to identify suspicious sources, monitor the normal behaviour of the network flow, and protect the vehicle network from potential attacks. The authors in [21] presented a detailed study of several anomaly detection schemes that could identify possible network intrusions. Anomaly detection can also be deployed to monitor vehicle network security, but continuous monitoring of network flow to identify suspicious sources could have a negative impact on latency, and lead to increased network overhead.

Other studies assessed the benefits of using public key encryption with keyword search (PEKs), and searchable encryption public key techniques. Key certification in PEKs is a complex process [23] as the public key certification is frequently updated, which could lead to communications overhead. Such a framework is also potentially vulnerable to inside keyword guessing attacks (KGA). Searchable encryption public keys [24] propose using a dual-server PEKs framework to address the vulnerability. It is important to note that encryption/decryption processes should be considered carefully, on order to prevent computation overhead or potential delays.

The authors in [25] classified the issues that emerged as a result of employing security and privacy in a vehicular cloud. In order to produce a system model for all vehicular technologies, integration of security/privacy features should be a part of the communication stack of any system platform.

Transferring data from service providers to vehicles without excessive delay is an issue that needs special attention, because a reasonable cost for vehicular service requests and data must be ensured. Cost efficiency and bounded delay are among the major challenges impacting the adoption of vehicular clouds. Vehicular clouds are also a major concern with respect to the mobility issue. Unpredicted moving vehicles produce virtually countless mobility scenarios. With poor Internet connectivity these scenarios are likely, and require special attention in such an environment.

Several researchers worked on cloud service pricing [26][27][28][29]. Some of these proposals should be revisited and tailored to vehicular clouds. To our knowledge, no one has considered the issue of cost efficiency in a vehicular cloud environment.

In [26], the authors proposed efficient dynamic scheduling to enable energy savings and reduce delay. A pricing mechanism to optimize mobile users and service providers and reduce their total costs for both non-cooperative and cooperative scenarios was suggested in [27].

In [30], a message dissemination scheme for VANETs was proposed to provide high message delivery ratio and decreased delays. A directional greedy approach creates a group of candidate nodes that hold the message to ensure optimal reliability. The authors in [31] proposed a repetition-based broadcast protocol for reliable broadcasting that guarantees a minimum number of broadcasts by signalling neighbouring nodes to transmit the same message at the same time. This scheme relies on cooperative diversity and a virtual antenna array. Similarly, in [32] the authors proposed a contention-based packet forwarding scheme for data dissemination in VANETs that introduces lower network overhead. This, in turn, helps decrease delays.

The studies mentioned above prove that there are no collaborative works in process that jointly address all these challenges. Exploring the shortcomings of privacy and security is an integral aspect of this research. Provision service delay and service cost issues in vehicular clouds have been examined less comprehensively, even though they are as important as security and privacy challenges. Although drivers could have serious concerns about service pricing and latency, the state of the art does not offer any legitimate and available solutions for service-price matching.

In this paper, we introduce a comprehensive framework supported by game theory concepts that meets most driver requirements, and addresses the identified challenges.

III. QUALITY OF EXPERIENCE (QOE) FRAMEWORK

Currently, QoE has been materialized and used with different research spaces, each of which introduces its own definition. For example, the International Telecommunication Union (ITU) defined QoE as, "*the overall acceptability of an application or service, as perceived subjectively by the end-user*"[33]. It is also worth mentioning that QoE emerged as a broader concept than QoS. The authors in [34] defined QoE as a multi-disciplinary field available to practitioners to evaluate systems, services or applications independently, or during the design phase. For networking communities, there are several boundaries between QoS and QoE that are not clearly defined; the differences and commonalities between the two can be found in [34]. Our proposed QoE can be defined as vehicular experience for service provisioning, with the aim of providing the best rating for the best services, assuming that the QoS has been found satisfactory by drivers. This section explains the QoE framework to be used with the game approaches discussed in Section 4.

Figure 1 presents the QoE framework under study [14]. The framework is comprised of three main participants: vehicle drivers, trusted third parties and service providers. The architecture employs a trusted third party between the drivers and the service providers to act on their behalf. The QoE framework is set up in a hierarchical mode, to provide scalability and reduce congestion overhead among the participants. Our game system, introduced in the next section, shows that trusted third parties are cluster-heads, while vehicle drivers and service providers are cluster-participants. For example, a group of drivers and service providers are connected to their cluster-head (i.e. TTP). The TTP receives a service request from a driver, processes it, and delivers it to the particular driver. Cluster participants can choose to join or leave at their convenience. This model is based on our former work in [14][35], in which we applied clustering but the implementation was more complicated. Thus, instead of dealing with two cluster-heads at different stages, we simply select one cluster head to handle all the communications at once.

The trusted third parties in our architecture are well-known commercial organizations that purchase services from service providers and sell them to vehicle drivers. The third party responsible for delivering QoS to its users is trusted and reliable. The responsibilities of a trusted third party include relevant communication aspects, finding the best-fit service request, negotiations the services, searching for the best price, filtering bad or impractical service requests, controlling misbehaviour by participants, and guaranteeing payment.

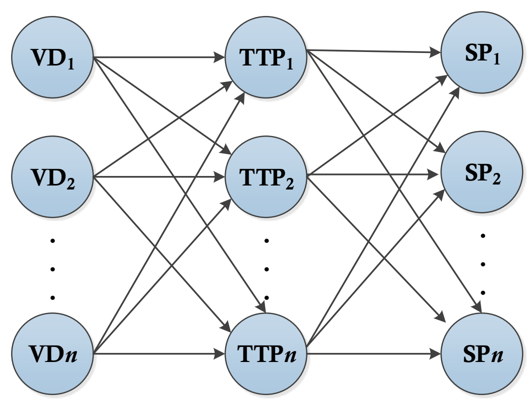


Figure 1: The QoE framework under study [14]

QoE is a weighted function of service provision delay (i.e. latency), service price (i.e. cost) and information revealed (i.e. privacy), as defined in Eq. 1 [14], [36]. In the equation, *D*, *P* and *I* represent the delay, price and information revealed, respectively. As shown, the sum of the coefficients in the equation equals one. QoE components are obtained via feedback from previously provisioned vehicles in a vehicular cloud, and formulated according to a weighted combination of the three key factors.

$$QoE = \alpha . D + \beta . P + \gamma . I \ \mid \ \alpha + \beta + \gamma = 1 \quad (1)$$

A driver who wants on-demand provisioning services has the option of joining a trusted third party. The drivers can do this randomly, or manually by assessing the available trusted third parties options. It is worth mentioning that each participant in this architecture has a QoE weight for every offered service, and the weight can be considered or refer to the participant's QoS. Typically, a driver requests a service from a trusted third party that will negotiate the service on his/her behalf prior to delivering it. Upon provision of the service to the driver, the trusted third party charges the vehicle driver based on the amount of usage. Thus, service providers receive their payment indirectly from the trusted third party, not from the driver. In this way, service providers will not be able to acquire a driver's identity or any other personal information. More importantly, when a QoE system completes a driver request, each participant provides recommendations based on their experience regarding the three QoE factors of delay, price and information revealed. In [1, 10] the recommendation is a numeric value based on user satisfaction, with ten representing the highest rank. Each party in the QoE framework has his own QoE reputation, which is the total average of recommendations received from other parties for each service provided by/to any party in the system. The recommendations are used to analyze and determine which service provider can offer the best price-delay-privacy combination, based on the driver's preference and requirements. The drivers can adjust the coefficients of the QoE function (i.e. α, β, and γ), or simply select one or more interests over others in the QoE.

Clearly, the QoE framework secures a driver's personal information, but this is not a concern since the trusted third party deals with the service provider. Trusted third parties provide as little driver information as possible to service providers, and in some cases may not need to provide any information. Moreover, drivers can request services based on their preferences. For example, they could choose fair price but less delay, or lowest price with acceptable delay. Thus, the objectives of the service cost and latency will be satisfied by the QoE framework.

IV. GAME-BASED OF THE QOE FRAMEWORK

In our earlier work, we developed an auction-based, multi-objective framework for service provision in vehicular clouds [14]. The multi-objective framework focuses on cost, latency and privacy, and it has shown promise since drivers are dynamically bound to the best fit available from a trusted third party. In addition, the trusted third parties can maximize their returns by selecting the best cluster of drivers. This solution can be applied and still be valid for a one level (two end) auction; that is, the buyer (driver) and the seller (trusted third party) at either end. Our one level (two end) auction has $n \times m$ participants, where n represents the number of drivers and m represents the trusted third parties. For example, at any time a number of drivers could be bidding on several services through different trusted third parties.

In [14], the proposed auction includes three main entities (i.e. drivers, trusted third parties and service providers), and at some point the trusted third parties must play the roles of buyer and seller at the same time; buying from the service providers and selling to the drivers. Such an auction-based solution assumes that the trusted third parties will provide the drivers with the promised services, and ignore the second level interactions between the trusted third parties and the service providers. Moreover, some drivers will be unable to bind to any available trusted third party, if none are willing to bind with them.

To address this issue and find the best cluster match (i.e. drivers with trusted third parties, and trusted third parties with service providers) for a single or multi-relationship auction, we ran a two-level (three end) auction with buyers (drivers and trusted third parties) and sellers (trusted third parties and service providers). These interactions require an $n \times m \times r$ auction model, where n represents the number of drivers, m represents the number of trusted third parties and r represents the number of service providers. The drawbacks of this model are the delay, the auction complexity, and the negative impact that the delay has on the service charges, since the drivers are charged by time used. These types of solutions are not feasible, as they can only be adopted if the delay is monitored and evaluated correctly. Moreover, an $n \times m \times r$ auction is very difficult to accomplish because the relationships can be different at each level, which means computational complexity and a need for high processing power. The outcomes can vary and often be unexpected.

Related work manages such problems with multi-agent game theory systems [37][38][39]. A description of possible solutions using different game model approaches are presented in this section.

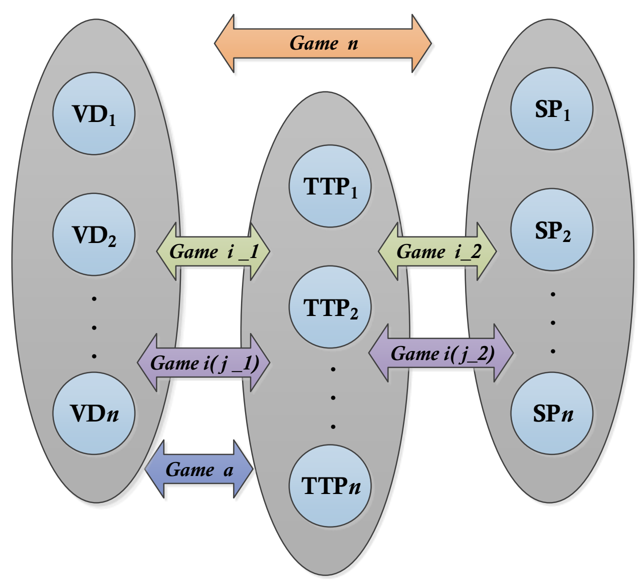


Figure 2: Game-based of the auction framework

To prove our concept using game theory we developed three different games, as shown in Figure 2. These are: *Game* *n*: a naive game between drivers and service providers; *Game i* and *j*: a Multiagent/Multiobjectives Interaction Game System (MMIGS) among all system participants; and *Game a*: an auction game between the drivers and trusted third parties.

A) Game Descriptions

Game n is a naive simple game between two players: the drivers and the service providers. It does not consider latency, cost or privacy, and does not introduce any QoE awareness between the players. A driver plays the game with several service providers, and one of the providers wins the game and provides the driver with the requested service.

Game i and *j* is a multiagent/multiobjective interaction game system with two possible levels of interaction, and negotiations between three main players: the drivers, trusted third parties and the service providers. This game ensures the driver will get the best price, minimal latency and enhanced privacy. In addition, the trusted third parties and the service providers play the game to maximize their returns; a win-win situation. MMIGS adopts the concept of the QoE awareness at each level of the game.

Game a is a sightless game between drivers and trusted third parties. It does not involve service providers, or implement any QoE awareness between the players. Trusted third parties are appointed by drivers to ensure they get basic QoS requirements, such as latency and cost. This is analogous to a situation where two players gamble without knowledge of the possible outcomes. Some aspects of *Game a* are similar to the former auction-based framework we presented in [14].

B) Objectives

The objectives of these proposed games are as follows: 1) to provide a comprehensive study of using the game model with different approaches; 2) to prove our concept of using the QoE framework with game-based; 3) to meet our proposed objectives for service provisioning in vehicular clouds; 4) to investigate the suitability of a game theory-based approach rather than an auction-based approach for our proposed QoE framework; and 5) to prove that using MMIGS is the best fit solution for service provisioning.

V. System Model

By its nature, game theory introduces beneficial intermediate results for all players [40], which is why we chose this approach and integrated it with our abovementioned QoE framework. Integrating the game theory-based approach with our QoE framework guarantees mutual benefits for all participants, and it is a more efficient system than other existing models. The system ensures that drivers get satisfactory service, and services providers (i.e. trusted third party and service providers) receive adequate profit. The following are explanations of the different theoretic approaches used for the proposed games.

A) "Game n" model

Game n is played between two players who have previously shared common knowledge about each other (e.g. utility charges, reputation, expected delay) without QoE awareness. It assumes the players are engaged in the game simultaneously, as in our previously proposed *Neutral mode* in [14]. However, the *Game n* model is built on a theoretical game approach, which was not the case with the previously presented neutral mode. The QoE-based approach is not included in this model, as shown in Figure 3.

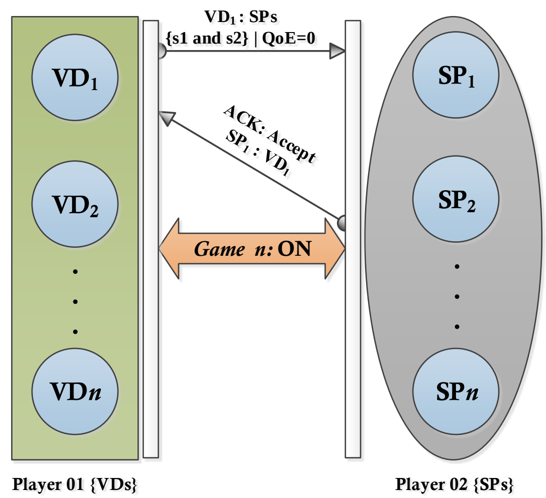


Figure 3: *Game n* approach

Game n allows player 01 (i.e. a driver) to start the game, and they have all available information about player 02 (i.e. a service providers). Similarly, player 02 is given access to all information about player 01. For example, at some point VD_1 seeks services $\{s_1 \; and \; s_2\} \in \mathcal{S}$ from service providers, without any conditions such as latency or privacy. The service providers accept or decline a request based on the information about VD_1 and the nature of the request. The details of a driver's request (e.g. time, type) play a role in the decision to accept or decline the request; if the service provider accepts it the game begins between them.

The outcomes of *Game n* always favour player 02. Even if the players have common knowledge about each other and expectations of utilities and latency, player 02 can select in their best interest before approving a driver's request. Thus, this model does not guarantee that player 02 decisions are mutually beneficial. In addition, player 01 has no control over their data, nor any guarantees about how the personal information will be used (i.e. absence of QoE). Moreover, the lack of QoE awareness between drivers and service providers means service providers can play in their best of interest only. The drivers have no information or knowledge about service providers' quality of service (e.g. service latency, service cost), and there is no vehicular services feedback from prior drivers regarding the requested services. Nonetheless, service providers tend to offer their best service in order to protect their reputation.

Table 1: Notations used in the proposed model

Notation	*Description*
$a_1, \dots a_i, b_1, \dots b_i$	Possible game outcomes
A, R	Game decision (Accept / Reject)
D	Delay measured in time units
I	Privacy measured in revealed information units
P	Price measured in currency units
QoE, VD_i, SP_j, TTP_n	Quality of Experience, Vehicle Driver *i*, Service Provider *j*, Trusted Third Party *n*.
$\mathcal{S}, s_i$	Set of services and service *i*
i	Interaction level of vehicle drivers,
j	Interaction level of service providers,
n	Interaction level of trusted third parties,
α, β, γ	Quality of Experience coefficients factors

B) MMIGS model

The Multiagent/Multiobjective Interaction Game System (MMIGS) has two potential levels (i.e. *i* and *j*) of interaction between drivers (player 01), trusted third parties (player 02) and service providers (player 03). Both the QoE-based framework and the theoretic game approach are adopted (i.e. the Nash Equilibrium) to provide players' experience throughout the game, and to introduce multi-objective services among multiple agents.

Four main games (*i_1, i_2, i(j_1)* and *i(j_2)*) can be applied during the game. The participants' strategy is to play their best response between each other during the game. Put simply, player 01 (drivers) aim to get the best services from trusted third parties and service providers, while players 02 and 03 want adequate return when handling or providing services. Three main service objectives (i.e. latency, cost and privacy) are managed during the game, and are the building blocks of our QoE-based framework.

1. MMIGS game i

Game (*i_1*) begins when a driver initiates a service request to a specific trusted third party, and indicates their preferences about the requested service. This means that drivers must provide their best play options, since they know that the QoE-based framework will select the player with the best available services, according to the preferences. The drivers' QoE-based model offers the option to review the trusted third parties and decide which to consider, based on the player's current interest. The MMIGS model implies that drivers and service providers will give the trusted third party their preference values (i.e. *{D, P, I}*) for each requested service, as stated in (1).

Once the trusted third party has a driver's requests, they run the game on the driver's behalf. The trusted third party has access to the driver's preferences, and plays its part of the game without disclosing any of the drivers' information or interests. Trusted third parties have more QoE knowledge about service providers than individual drivers. The second part of the game (*i_2*) is initiated by the trusted third party, who provides the driver's request to the service providers that can match them. Each service provider knows that this game has more than two parties and more than one service provider, which motivates them to play their best choices, not only the winning choice as in *Game n*. Service providers' responses are rated after the services have been delivered to the driver, and the ratings could have a positive or negative impact on a provider's overall QoE reputation. The trusted third party receives the service providers' best offer (i.e. SP_j $\{D_j, P_j, I_j\}$) for the driver's requested services. The trusted third party then constructs a matrix of the service providers' responses (SP_j) to the driver's original request.

The trusted third party then examines the offers and compares them to the driver's request, after which the trusted third party accepts the best offer and notifies all parties accordingly. The choice is based on the trusted third party acting in the best interest of all parties, not only for itself. Thus, the trusted third party's best strategy is to find the best match for the driver's request, select it, add their fee, and notify all parties of the outcome.

The trusted third party's duty is to find drivers the best services that match their preferences, and this is not necessarily straightforward. It becomes more complicated if none of the service providers have extended an offer that matches the driver's request, which means more interactions between the multiagents is required during the game.

2. MMIGS game i(j)

MMIGS game i should be more resilient against unexpected situations, which requires more negotiation between game participants about available choices. More interaction between the parties ensures that all possible options are available to all players, to help them reach a more optimal game model. Though more communications typically leads to additional delays, reasonable extra delays can sometimes have a positive effect on the overall outcome of the game. *MMIGS game i(j)* uses the *game i* level, with an extension to provide more negotiation on the available choices.

MMIGS game i(j) can only be activated if drivers and service providers are open to negotiations, re-visiting and amending the terms of their offers, and the trusted third party feels there is a good chance to start negotiations.

The extension *game i(j)* of *game i* can be only possible if the $SP_j(\mathcal{S}) = \sum_{j=1}^{n} \{(D_j^s, P_j^s, I_j^s)\}$ matrix and $VD_i(\mathcal{S}) = \sum_{i=1}^{n} \{(D_i^s, P_i^s, I_i^s)\}$ are not considered a suitable match by the trusted third party, they are very close to each other, and none of the terms compromise others. For example, given that a driver is willing to tolerate some extra delay, and has more privacy information or less to pay, the trusted third party runs the closest options from the generated matrix on the driver. The driver studies the offers and decides to either accept one, or propose a new request with the amended values of the new offers. If the driver accepts one of the closest offers there is no need to notify the service providers, since one of the objectives is to reduce the latency. However, if the driver proposes a new game request (i.e. *game i(j_1)*) with valid enhancements of the initial preference values, the appointed trusted third party continues the game and passes this new request (i.e. *game i(j_2)*) to the group of service providers involved. Participants can interact with each other to help make the negotiations successful, and it is assumed that they will agree that any new proposed offers must have more persuasive compromise values than before.

At this point, the trusted third party has received the amended offers that satisfy the driver's new proposed offer from the service providers. Finally, the trusted third party passes the amended offers from the group of service providers to the vehicle driver. If the driver accepts them, an acknowledgment message is sent to the chosen service provider permitting delivery of the service.

At the end of the game, and once the driver has received the service(s), all participants can rate both the services and the game. Drivers typically rate the service they received based on their level of satisfaction, while trusted third parties rate the drivers and the service providers, based on the interactions and the level of the promises made between them. Service providers can also rate their interaction with the trusted third parties during the game.

3. MMIGS game i(j) scenario

Figure 4 illustrates *game i* and *game i(j)* in detail. At the start, VD_1 is seeking services $\{s_1 \in \mathcal{S}\}$, and selects TTP_1 to play the game on their behalf. VD_1 choses TTP_1 because it is the best match for the service and interests of VD_1. Drivers can select any other available trusted third party, based on their QoE reputation. The QoE for the participants are then announced and are available for all parties on the cloud, which is why each party in our QoE-based framework wants to maintain their QoE reputation. In most cases, selecting the corresponding party in the QoE framework is based on the QoE reputation about a particular service.

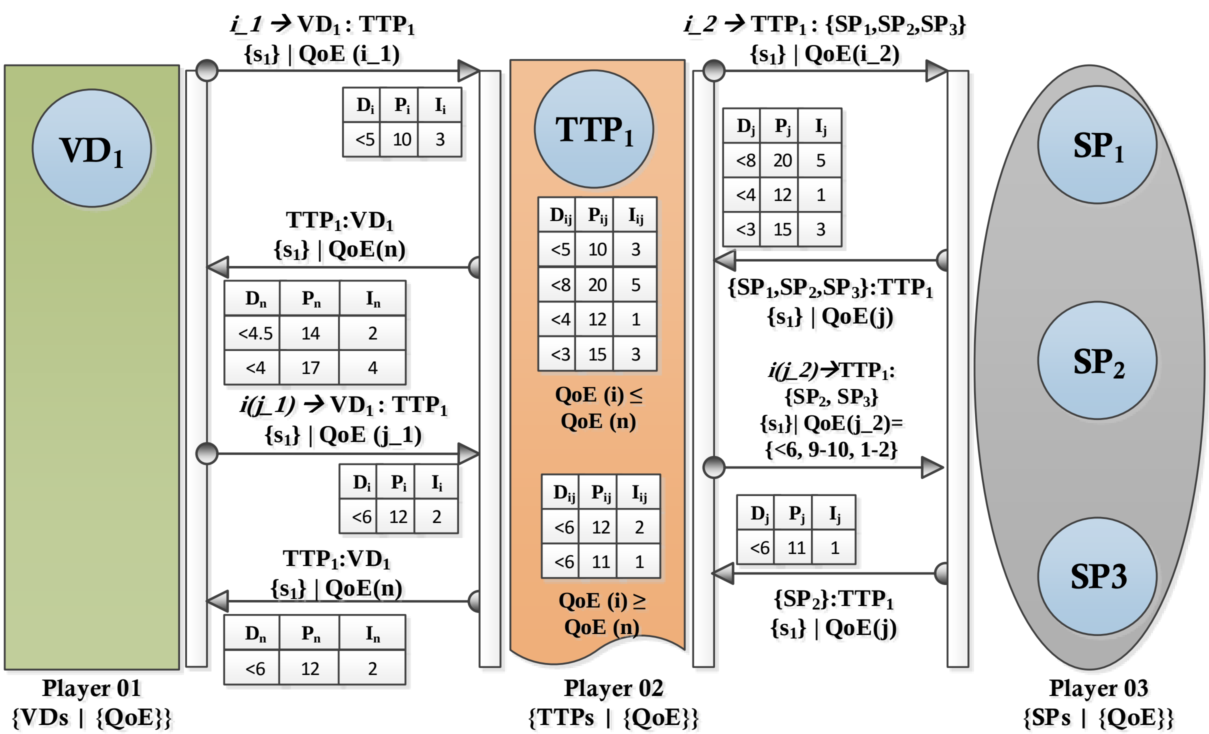


Figure 4: An example scenario of the MMIGS game approach

A one-to-one game (*i_1*) starts when TTP_1 receives the VD_1 request and all the related request information:

$$QoE\ (VD_i) = \{D_i, P_i, I_i\} = \{<5, 10, 3\} \quad (2)$$

TTP_1 keeps client (e.g. VD_1) information protected, and applies its previously found knowledge and experience to find the most suitable and available service providers (e.g. SP_1, SP_2, SP_3) to contact about the VD_1 service request. A one-to-many game (*i_2*) is initiated by a TTP_1 request to the service providers with the appropriate QoE reputation to provide the services. The intention of TTP_1 at this stage of the game is to release only the service type $\{s_1\}$ to the service providers, and hide the driver service preferences (e.g. {<5, 10, 3}). At this point, TTP_1 has no information about offers from service providers for the service, so the best strategy is not to disclose the driver preferences to the service providers.

The service providers know that there are other service providers in the game, so they will respond with their best offer. This keeps them in the game, and gives them a significantly better chance of winning than playing for their own benefit and being excluded from the game later. Thus, as in Figure 4, the three service providers have responded with the following offers:

$$QoE\ (SP_j) = \{D_j, P_j, I_j\} = \{ \{<8, 20, 5\}, \{<4,12,1\}, \{<3,15,3\} \} \quad (3)$$

Once TTP_1 has all the service providers' offers, it selects the most suitable ones and puts them and the VD_1 preferences into a matrix to match and compare them, as shown in Figure 5. If more than one service is requested by the drivers, match/compare matrices are built for each service.

	D_{ij}	P_{ij}	I_{ij}
VD_1	<5	10	3
SP_1	<8	20	5
SP_2	<4	12	1
SP_3	<3	15	3

Figure 5: QoE (i,j) preference comparison

TTP_1 finds that SP_2 and SP_3 are proposing the most appropriate offers. Based on this, TTP_1 determines its best option and responds back to VD_1 with a new matrix, as shown in Figure 6. The matrix is based on the most suitable offers proposed by SP_2 and SP_3 that were amended to make them suitable for TTP_1.

$$QoE\ (TTP_n) = \{D_n, P_n, I_n\} = \{ \{<4.5, 14, 2\}, \{<4,17,4\} \} \quad (4)$$

	D_n	P_n	I_n
1	<4.5	14	2
2	<4	17	4

Figure 6: QoE (n) proposed offer to vehicle drivers'

One objective of trusted third parties is to spend more time and computational effort to protect drivers' personal information, while getting them the best available offers and services from the service providers. Thus, an acceptable offer to the drivers has better, equal or QoE values that meet their requirements. The semi-final proposed game offer from TTP_1 to VD_1 typically has the following priorities:

$$\{D_n, P_n, I_n\} > \{D_i, P_i, I_i\} \rightarrow QoE\ (TTP_n) > QoE\ (VD_i) \quad (5)$$

A typical game offer that can be considered by the vehicle drivers should meet the following:

$$QoE = QoE\ (VD_i) - QoE\ (TTP_n) \geq 0 \quad (6)$$

In this example, the QoE final offer shown in Figure 6, is not equal or less than what VD_1 is expecting. However, it is close, and persuasive enough to be re-considered for negotiation. At this point, VD_1 is not fully satisfied with the two offers because they cost more, even though they have less delay than specified, so, now the driver's best strategy is to re-negotiate the offers that have just been received. A new game (*i(j_1)*) with an amended offer is initiated by VD_1 to TTP_1, stating that the driver is willing to pay slightly more (10 to 12) and experience slightly higher delay (<5 to <6) to get better privacy (3 to 2) for the personal information revealed.

TTP_1 receives the new VD_1 preferences, checks to make sure that VD_1 has made reasonable amendments to the extended proposal, informs SP_2 and SP_3 that a new amended proposal has been made due to driver dissatisfaction, starts a new game session (*i(j_2)*) with SP_2 and SP_3, and passes the extended proposal directly to them. Thus far, TTP_1 has proposed two main games (i.e. *Game (i_2)* and *i(j_2)*), as shown in Figure 4. The games are not similar, since they are fundamentally different in terms of strategy. As explained earlier, since TTP_1 is not certain what it is negotiating against, its best approach for the first game *(i_2)* is to not disclose its driver's preferences to the service providers. However, in the second game (*i(j_2)*), TTP_1 reveals more of the driver's preferences, to show the service providers that the driver is determined to get this service. Another reason for revealing more is to give the service providers additional background about what they should expect. Moreover, at game (*i(j_2)*), the drivers' preferences are adjusted slightly, then passed to a small subset of the original service providers who have already responded with reasonable offers (SP_2 and SP_3). In our scenario, TTP_1 shares its client's preferences with only SP_2 and SP_3, excluding SP_1 since its offer was not reasonable. TTP_1 then adjusts VD_1's preferences, and introduces them to SP_2 and SP_3 as follows.

$$QoE\ (VD_{i\_2}) = \{D_{i\_2}, P_{i\_2}, I_{i\_2}\} = \{ <6, 9\text{-}10, 1\text{-}2 \} \quad (7)$$

SP_2 and SP_3 receive TTP_1's adjusted preferences, examine them, and then play their best strategies. Service providers can quit the negotiations for any reason, although it could affect their QoE reputation, depending on how often they quit games. In this example, SP_2 is the most likely candidate since its choices are very close to VD_1's adjusted preferences, so its best play is to propose a new offer that fits the VD_1 adjusted preferences. Accordingly, SP_2 proposes a new offer ({<6, 11, 1}) to TTP_1, as shown in Figure 4. TTP_1 receives the offer, then plays its best game option ({<6, 12, 2}) and matches its driver's needs at the same time. The final offer is delivered to VD_1 which is found to be a perfect fit, and is accepted.

$$QoE = QoE\ (VD_i) - QoE\ (TTP_n) = 0 \quad (8)$$

C) *"Game a"* model

Game a is a blind game between drivers and trusted third parties. Service providers are not involved, and there is no QoE awareness between the players. *Game a* begins when a driver requests to be bound to an available trusted third party; it is the driver's responsibility to include any further information in the request. If a trusted third party accepts the request, the driver informs them of the service(s) they want. A blind request with no information about the service type always favours the driver, for two reasons: the driver can refuse the trusted third parties offer, or they can choose to quit the game at any time if they receive an offer from one trusted third party while another is still proposing. However, this could affect the willingness of the trusted third parties to accept blind requests. If a trusted third party chooses to accept, then the game is played between them and the driver, as shown in Figure 7. Trusted third parties are supposed to guarantee basic QoS for their drivers, such as low latency and optimal privacy. However, it is a blind game, since the trusted third parties have no idea of the service type or cost. Another drawback of this game is if a trusted third party receives offers from service providers about a requested service, proposes them to the driver and the driver does not accept them. Thus, both players have no knowledge of the outcome. A scenario of this approach is illustrated in Figure 7.

VD_1 sends a blind request to trusted third parties to inform to start a game. TTP_1 and TTP_2 accept the request, which triggers VD_1 to send them the service type $\{\mathcal{S}_x\}$. TTP_1 and TTP_2 contact the service providers to get their offers for the service $\{\mathcal{S}_x\}$. Two service providers can provide the service, and they make their offers to TTP_2. Meanwhile, another provider (SP_3) also makes an offer to TTP_1. TTP_2 selects the best of the two offers received, adds their service fees, and proposes the final offer to VD_1. If VD_1 choses to accept the offer, they inform TPP_2 and quit the game with TTP_1. The driver can also wait to see the possible final offer from TTP_1, compare it with the TTP_2 offer, and select their preference. This scenario demonstrates that trusted third parties are more vulnerable in this game than drivers and service providers.

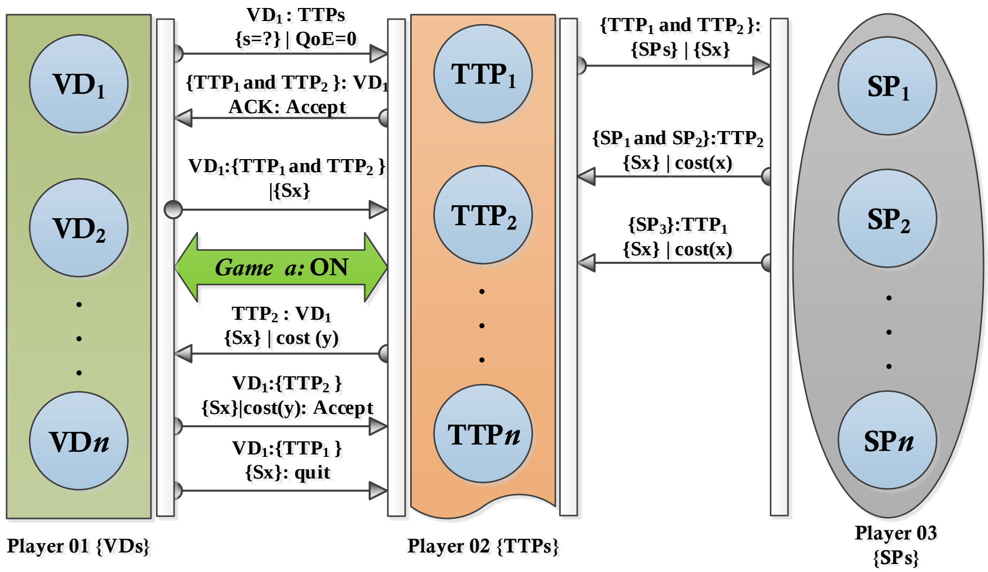


Figure 7: *Game a* approach

VI. Analysis of Outcomes Under MMIGS

In order to understand the mutliagent/multiobjective interaction game system, the types and roles of the players must be defined, as well as the possible interactions between them. In our proposed game system, we consider three main players $\{VD_i,\ TTP_n,\ and\ SP_j\}$, each of which is independent and has preferences that represent their best interests. The expected outcomes can be defined by the following set:

$$\Omega_{outcomes} = \{\, QoE_{VD}, QoE_{TTP}, QoE_{SP}\} \tag{9}$$

A set is made up of all possible outcomes of the game, and each outcome involves three different preferences (objectives) for each player. The set of these preferences is then defined (the preferences refer to the QoE factors in the QoE framework).

$$\Omega_{\text{preferences}} = \{D, P, I\} \tag{10}$$

Every player in the game has their own QoE, as shown in the outcomes set (9), and each wants to keep their QoE in good standing (the higher the QoE value the better). Thus, the system experience preferences function can be defined as follows:

$$QoE\colon \Omega_{\text{outcomes}}\left(\Omega_{preferences}\right) \to \mathbb{R} \tag{11}$$

Our system has more than one possible outcome at a time for each preference. For example, if a and b are possible outcomes (e.g. *a* for delay, *b* for price) for QoE_{vd1}, and $QoE_{vd1}(a) \geq QoE_{vd1}(b)$, then VD_1 prefers outcome *a* over outcome *b*. Based on this, we can introduce a more general concept: if the possible outcomes for a player's preference are *a*, *b* and *c*, and given $a \geq b$ and $b \geq c$, then,

$$QoE(a) \geq \text{QoE}(b)\ and\ QoE(b) \geq \text{QoE}(c), \Rightarrow QoE(a) \geq \text{QoE}(c) \tag{12}$$

With this concept of player preferences, we can show the interactions between our players for specific or multiple outcomes. A player in the game has to make a decision (action), and the outcome results from this action. The final result of all interactions between the players is the final outcome of the game result. More simply, we examine the beginning of a game (i_1) that two players start to achieve a possible outcome (a), and each player has only two possible actions to consider {A, R}, where A stands for *accept* and *R* stands for *reject*. Given that the set of actions for this outcome is $QoE(a) = \{\mathrm{A}, \mathrm{R}\}$, then the final outcome can be determined with the following formula:

$$QoE = QoE_{VD}(a) \times QoE_{TTP}(a) \times QoE_{SP}(a) \rightarrow \Omega_{outcomes} \quad (13)$$

To present the game more clearly, we show different actions in *game i* for one possible outcome (a), as formulated in Eq. 14:

$$QoE(a) = QoE_{VD}(a) \times QoE_{TTP}(a) \quad (14)$$

Thus, four possible outcomes can occur for different combinations of players' actions, as in the following:

$$QoE_{VD|TTP}(A,A) = a_1 \text{ , } QoE_{VD|TTP}(A,R) = a_2 \text{ ,}$$

$$QoE_{VD|TTP}(R,A) = a_3 \text{ , } QoE_{VD|TTP}(R,R) = a_4, \quad (15)$$

The game can also be mapped onto the same outcome, as follows. Such an environment is unlikely in our system, since the outcome will remain the same regardless of the players' actions.

$$QoE_{VD|TTP}(A,A) = a_1, QoE_{VD|TTP}(A,R) = a_1 \text{ ,}$$

$$QoE_{VD|TTP}(R,A) = a_1 \text{ , } QoE_{VD|TTP}(R,R) = a_1 \text{ ,} \quad (16)$$

We can also consider a more sensitive environment, where the outcomes could be affected by the action of one of the players as in the following:

$$QoE_{VD|TTP}(A,A) = a_1 \text{ , } QoE_{VD|TTP}(A,R) = a_2 \text{ ,}$$

$$QoE_{VD|TTP}(R,A) = a_1 \text{ , } QoE_{VD|TTP}(R,R) = a_2 \text{ ,} \quad (17)$$

In this environment, it does not matter what the vehicle driver's action is, since the outcome depends only on the action of the trusted third party. If a trusted third party choses to reject, as shown in Eq. 17, an a_2 outcome will result, while if the trusted third party chooses to accept an a_1 outcome will result. Our QoE game assumes that all players have influence in the game, thus all player selections affect the outcome. It becomes more interesting when we combine players' preferences with their actions. If we pick the most generic environment, where players' actions produce different outcomes as shown previously, and map it onto the players' preferences, we can predict the best possible outcomes of the game based on the players' selections, according to Example 1:

$$QoE_{VD}(a_1) = 2 \text{ , } QoE_{VD}(a_2) = 2 \text{ , } QoE_{VD}(a_3) = 1 \text{ ,}$$
$$QoE_{VD}(a_4) = 1 \text{ , } QoE_{TTP}(a_1) = 2 \text{ , } QoE_{TTP}(a_2) = 1 \text{ ,}$$
$$QoE_{TTP}(a_3) = 2 \text{ , } QoE_{TTP}(a_4) = 1 \text{ ,}$$

Since we know that each possible outcome is mapped onto a different action:

$$QoE_{VD}(A,A) = 2 \text{ , } QoE_{VD}(A,R) = 2 \text{ , } QoE_{VD}(R,A) = 1 \text{ ,}$$
$$QoE_{VD}(R,R) = 1 \text{ , } QoE_{TTP}(A,A) = 2 \text{ , } QoE_{TTP}(A,R) = 1 \text{ ,}$$
$$QoE_{TTP}(R,A) = 2 \text{ , } QoE_{TTP}(R,R) = 1 \text{ ,}$$

It is clear that the driver and the trusted third party action in this example means acceptance. The preference description is as the follows:

$$QoE_{VD}(A,A) \geq QoE_{VD}(A,R) \geq QoE_{VD}(R,A) \geq QoE_{VD}(R,R)$$

$$QoE_{TTP}(A,A) \geq QoE_{TTP}(R,A) \geq QoE_{TTP}(A,R) \geq QoE_{TTP}(R,R)$$

Examining the different possible actions available to the driver and the trusted third party, raises the question: Which action should both chose to ensure best outcome? As explained earlier, the driver's best strategy to achieve the best possible outcome would be to *accept*. The trusted third party's best outcomes (i.e. a_1 and a_3) will be if vehicle driver *accepts* and they also accept, or if the driver rejects and they accept. However, the trusted third party preference description above means they accept over all other possible actions. Thus, in this example, it would be best if both players (VD and TTP) act rationally and chose the action that is mutually beneficial.

To prove the concept of using game models, we construct a different Example 2 with new player preferences as follows:

$$QoE_{VD}(A,A) = 2 \text{ , } QoE_{VD}(A,R) = 1 \text{ , } QoE_{VD}(R,A) = 2 \text{ ,}$$
$$QoE_{VD}(R,R) = 1 \text{ ,}$$

$$QoE_{TTP}(A,A) = 1 \text{ , } QoE_{TTP}(A,R) = 1 \text{ , } QoE_{TTP}(R,A) = 2 \text{ ,}$$
$$QoE_{TTP}(R,R) = 3 \text{ ,}$$

In Example 2, the trusted third party's best outcome is to reject if the driver rejects, and the driver's best outcome is to accept and reject if the trusted third party always accepts. However, the trusted third party's second best strategy in this game is to accept if the driver rejects. In this selection of (*R*, *A*), both players get benefits and better outcomes.

VII. PERFORMANCE EVALUATION

A) Simulation settings

The simulations for performance evaluation of the proposed schemes were performed using NS-2 [41]. The communication platform employs the Destination-Sequenced Distance-Vector Routing (DSDV) protocol, on IEEE 802.11.p communication stack with 1024 byte/packets. In the next set of simulations, each was repeated 10 times with a range of 5 to 50 vehicles. For the QoE-awareness equation coefficient factors, the α, β *and* γ parameters are initially evaluated when equally weighted. In order to investigate the impact of the weighting on performance, we simulated random combinations against the game models, and these values can be adjusted based on the driver's preferences. With the simulations, we intend to: 1) study all possible parameters of the game model with different approaches, 2) study the impact of employing the concept of QoE-awareness with gaming, 3) satisfy our proposed objectives for service provisioning in a

Table 2: Simulation scenarios and corresponding settings

Scenarios	*Vehicles*	*TTPs*	*SPs*	**a, β and γ in normal mode**	**a, β and γ in *Driver's Comfort* mode enforcement**
1	5	3	4	0.33, 0.33, 0.34	_
2	10	4	7	0.33, 0.33, 0.34	$\beta = 20\%, a\ and\ \gamma = random$
3	15	6	8	0.33, 0.33, 0.34	$\beta = 40\%, a\ and\ \gamma = random$
4	20	9	10	0.33, 0.33, 0.34	$\beta = 60\%, a\ and\ \gamma = random$
5	25	10	14	0.33, 0.33, 0.34	$\beta = 80\%, a\ and\ \gamma = random$
6	50	12	21	0.33, 0.33, 0.34	$\beta = 100\%, a\ and\ \gamma = random$

vehicular cloud, 4) compare game theory-based and auction-based service provisioning approaches in vehicular clouds, and 5) evaluate the performance of game theoretic service provisioning approaches and determine the method that best fits the vehicular cloud environment. To illustrate this, we simulated multiple scenarios with a random number of game participants, in order to assess the behaviour of the proposed approaches in different situations.

To evaluate the impact of the QoE-awareness coefficient factors $(\alpha, \beta, and\ \gamma)$ on the average savings for the MMIGS-WN model, we ran another set of simulations in which we diversified the weights of these factors (as shown in Table 2), and monitored the behaviour of the system. We studied the effect of the factors under these settings, while gradually increasing the network density from 10 to 50 vehicles in steps of five vehicles. In each step, the coefficient factor of the price (β) is increased equally by 20%, and $\alpha\ and\ \gamma$ are randomly set in intervals of $[0, 1-\beta]$. We also introduced a new mode we call the *Driver's Comfort* mode, in which the MMIGS-WN game is played to provide services that match the drivers' preferences. Thus, we evaluate the difference between user cost and privacy savings when the MMIGS-WN game is played with and without user preferences, denoting the former by *cost* and *privacy* and the latter by *cost-comfort*. The driver's comfort in this mode is represented by the driver's preferences at the beginning of each game. Table 2 presents these scenarios.

B) Simulation results

We have evaluated the different proposed approaches in terms of the following metrics:

1. *Delay* is the end-to-end time before a driver receives the requested service from the service provider. This metric is used to compare the delay generated by game models and other conventional models.
2. *Price* is the total that drivers are charged based on their usage, applied by the trusted third party and the service provider. A *saving* price parameter is evaluated with this metric, to represent how much drivers will save if they adopt one approach over another.
3. *Privacy* is the amount of information revealed to the service provider. It represents the actual personal information a driver must provide to the service provider through the trusted third party to receive the service. The information required will vary for different services.
4. *MMIGS equilibrium* is the average number of negotiation phases it takes the *MMIGS i(j)* approach to reach equilibrium among all participants. It is important to know the number of phases, as it is impractical for participants to engage in endless negotiations for a service.

We categorized the proposed models by two groups, namely the QoE unaware (i.e. *Game n*, *Game a* and *Neutral mode*) method and the QoE aware (i.e. MMIGS and auction-based) method, and conducted three types of evaluations and comparisons based on these methods. First, we analyzed how the proposed *Game n* and *Game a* models behave under the first three metrics (i.e. delay, price, and privacy), and compared them to the *Neutral mode* solution presented in [14]. *Neutral mode* is a simple model in which participants connect to the first available service provider without any QoE aspects. Secondly, another set of simulations was performed to explore the differences between the proposed game approaches MMIGS with no negotiation (MMIGS-NN) and MMIGS with negotiation (MMIGS-WN) under the same metrics. These models were also compared to the auction-based model solution in [14]. The auction-based QoE service provisioning model uses QoE-awareness, and manages a competition between trusted third parties and service providers to select auction participants that maximize their profit. And third, the last set of simulations investigated the impact of the MMIGS-WN in terms of average system savings and game equilibrium.

In the first group, we tested the average delay of the *Game n* and *Game a* models, and compared them to the *Neutral mode* with the delay randomly distributed, as shown in Figure 8. When the vehicles are sparse in the cloud network (i.e. 5 to 15 vehicles), *Game n* and *Game a* have delays similar to those of the neutral mode. As more vehicles enter the game the delay begins to increase, and is at its worst with a group of 50 vehicles. Thus, the delay under *Game a* is expected to be highest, since the worst two stages of communication are among its participants. However, as shown in Figure 9, latency in *Game a* improves the service cost.

Figure 9 compares the average service cost of *Game n*, *Game a* and the *Neutral mode*, distributed over 50 vehicles. The *Neutral mode* technique engages the first available nearby service provider to handle a driver service request. As service provider charges are unpredictable, a driver can find a service provider with lower charges without committing to them. However, *Game n* is a request to play a game while *Game a* is a blind game, which implies that a service provider who can make revenue might accept driver requests. A service provider should present a reasonable offer to the driver if they want to provide the service, otherwise the driver has no reason to play the game. This is the main reason why the total service cost under *Game n* and *Game a* is less than that under the *Neutral mode*.

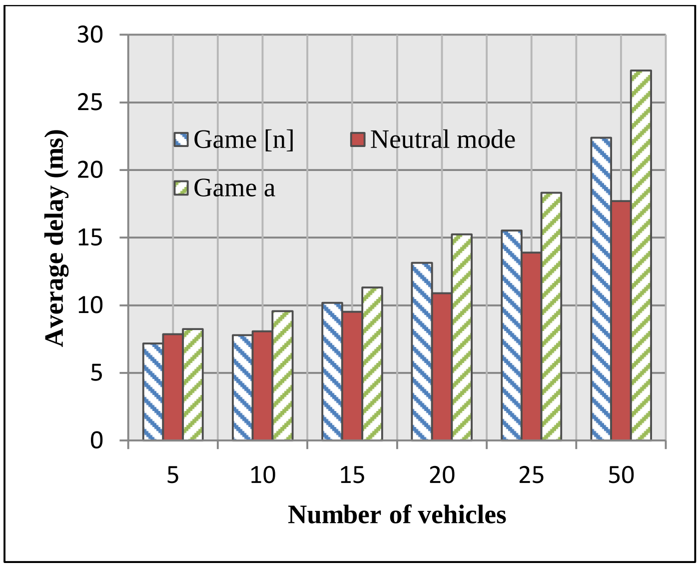


Figure 8: *Game n* delay

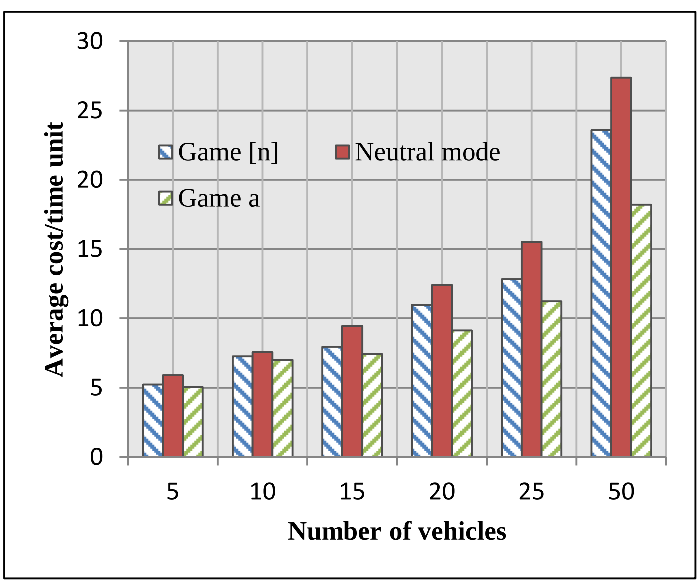


Figure 9: *Game n* service cost

The amount of released information with both modes is similar under a sparsely deployed vehicular network. As the vehicular network becomes denser the amount of revealed information increases, which makes the *Neutral mode* more beneficial than the game-based models, as shown in Figure 10. This is because the game models have more communication overhead than the *Neutral mode*, which has more information. Clearly, there is no reason for a driver to adopt the *Game a* or *Game n* model, since either could encumber them with additional delay and insignificant cost savings. Plus, there is no privacy guarantee due to the lack of QoE-awareness in these models.

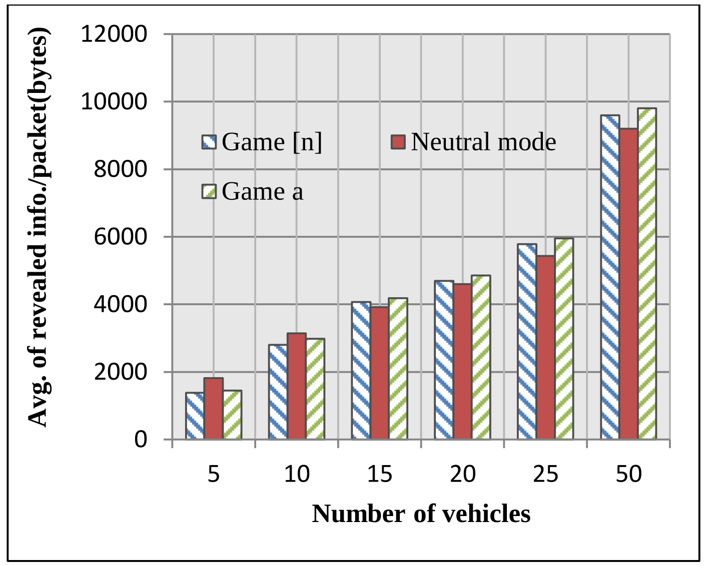


Figure 10: Game n privacy

Figure 11 illustrates the total impact of QoE-awareness on average delay in every group of vehicles when it is integrated with different models. We observed that, under auction-based provisioning (i.e. AQoEP), there are lower average delays until the vehicular network has 50 vehicles. Due to the number of communications levels, both MMIGS-NN and MMIGS-WN lead to longer delays than AQoEP. MMIGS-NN has two levels of communication (i.e. *i_1* and *i_2*), while MMIGS-WN has a minimum of two levels of communication (i.e. *i_1*, *i_2*, *j_1* and *j_2*). Once the network has 50 vehicles, MMIGS-NN and MMIGS-WN have almost the same delay, and they reduce the delay gap between them and AQoEP from 6.13ms to 3.20ms (48.6%). This can be explained by the fact that MMIGS-WN appears to develop its experience over time, and compromises with a little delay in each group participant experience (~3%). Increasing the average delay also means more negotiations, which indicates that the participants are engaged in the game. Moreover, AQoEP conducts one level of communications while MMIGS conducts at least two levels; this can be considered a significant improvement.

As shown in Figure 12, MMIGS-WN outperforms both the other models with respect to service cost. The main reason for this is the circumstances of the negotiations among the game participants, which is not relevant in the case of AQoEP.

The average service cost difference between the proposed MMIGS-WN and AQoEP is in the range of 50% in the first five scenarios, and approximately 65% in the last scenario. MMIGS-WN is also less costly than MMIGS-NN; up to 15% in a sparse vehicular network, and approximately 23% in a denser network. This means that the proposed game models achieve savings on the provision of services of up to 50%. Figure 13 shows the impact on the amount of revealed information when QoE-awareness is adopted with the game theory concept. MMIGS-WN again outperforms the other two models. AQoEP seems to be vulnerable with respect to driver privacy, so MMIGS-WN is a promising alternative when drivers are concerned about revealing their information. It improves driver privacy up to 47% compared to AQoEP, and 19% compared to MMIGS-NN. These improvements in service cost and driver privacy are due to the following: 1) using game theory approaches among vehicular participants, 2) adopting QoE-awareness with games, and 3) testing the feasibility of integrating a negotiation stage between game participants.

The service cost savings with or without applying the *Driver's Comfort* mode in the MMIGS-WN game are illustrated in Figure 14, where the average savings under the MMIGS-WN model are compared to when the MMIGS-WN game is played with prior knowledge of the driver's comfort preferences. As the weight of β increases, the average savings increase and the privacy savings decrease. With the *Driver's Comfort* mode savings, there is always a gap in the 20% to 40% range and the 80% to 100% range. The best average cost/privacy savings are achieved with service weight costs of 60%. Under this weight setting, the average difference in savings between the MMIGS-WN model and the MMIGS-WN model with *Driver's Comfort Mode* is less than 5% of the total *Driver's Comfort* savings.

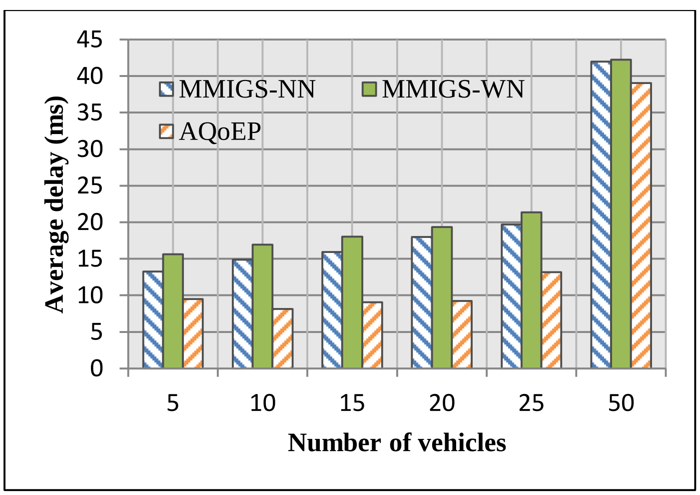


Figure 11: The impact of the QoE-aware models on service delay

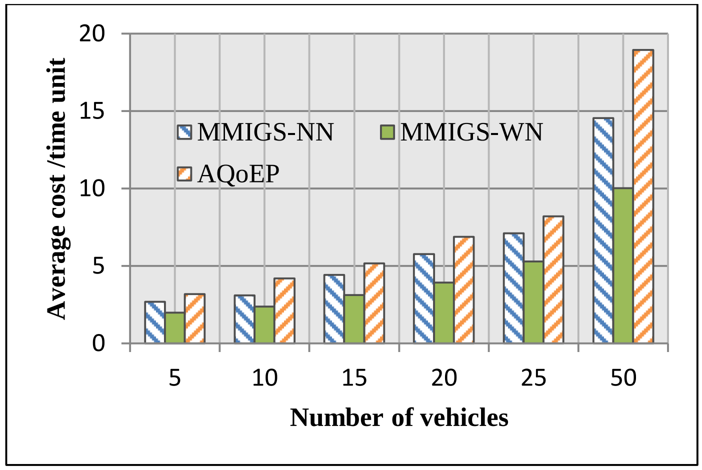


Figure 12: The impact of QoE-aware models on service cost

In the final simulation set, we tested the average number of equilibrium stages required for the MMIGS-WN model to become stable. We wanted answers for two questions, namely 'How many stages are required for a game to reach equilibrium in the proposed scenarios?' and 'Does the number of participants have an impact on the number of stages?' Figure 15 illustrates the equilibrium stages against the number of vehicles, and shows that the number of the vehicles does not affect the number of equilibrium stages, since the system can have the same number of stages (i.e. 3) with 50 vehicles or 20 vehicles.

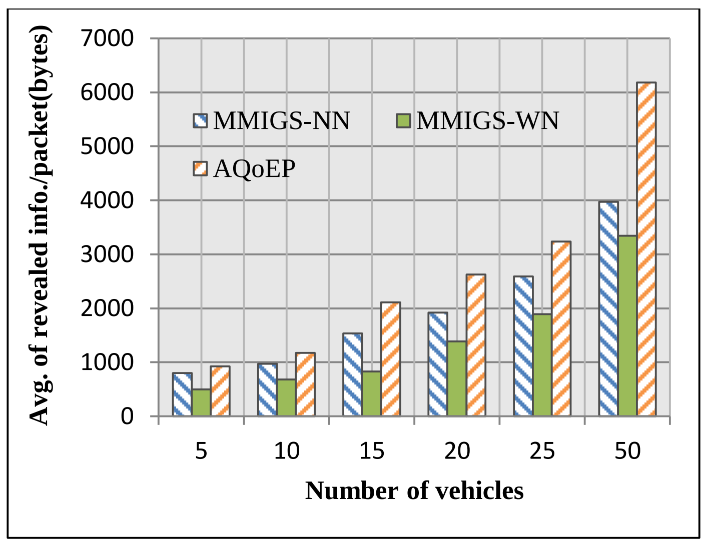


Figure 13: The impact of the QoE-aware models on privacy

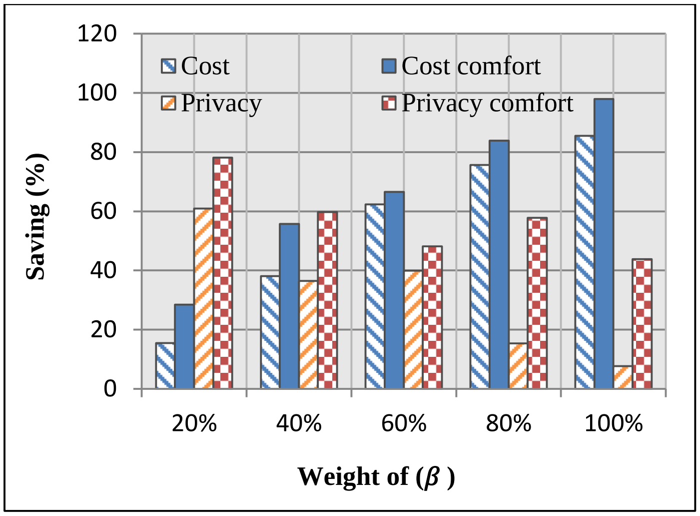


Figure 14: MMIGS-WN average percentage saving

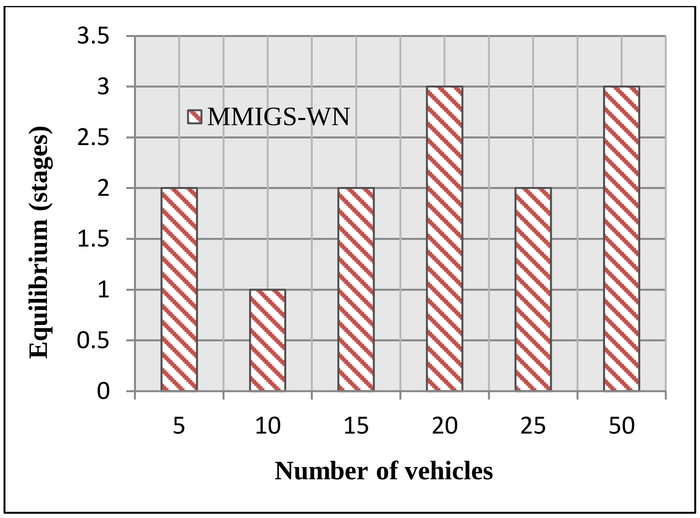


Figure 15: MMIGS-WN equilibrium

VIII. Conclusion And Future Directions

In this paper, we proposed a multiagent/multiobjective interaction game system (MMIGS) for service provisioning in a vehicular cloud, based on a game theoretic approach and a Quality of Experience (QoE) framework. MMIGS balances the overall game, while enhancing drivers' service costs and preserving their privacy. The proposed game system differs from other conventional models, as it allows drivers to prioritize their preferences. It also takes QoE-awareness into account, which enables drivers to negotiate the terms of their preferences. Our extensive simulations show that the proposed game model with negotiations (i.e. MMIGS-WN), incorporated with QoE awareness and a trusted third party (TTP), efficiently mitigates communication latency by a bounded percentage of 3%. In addition, MMIGS-WN with QoE-awareness and TTP involvement achieves reduced service costs of 65%, and preserves driver privacy (i.e. information revealed) by 47%. We also analyzed the performance of this game model in scenarios where the number of vehicles and the weighting factors varied, and the results showed that significant savings can be achieved under various weighted combinations of driver preferences. Finally, we calculated the total number of stages required for the game to reach equilibrium, and determined that the number of vehicles does not affect the number of equilibrium stages.

We are currently extending the proposed game model for use with mobile vehicles, as this paper assumed a network of fixed/parked vehicles. Furthermore, we will incorporate "sensing as a service" with the vehicular cloud, and introduce trustworthiness into the proposed framework as suggested in related work [42]. Finally, we will apply other metrics to quantify driver privacy, and integrate additional methods with the proposed framework to hide sensitive data such as drivers' mobility patterns. We will also prevent service providers learning driver identities, by cloaking regions to avoid revealing location information.

References

[1] H. T. Mouftah and B. Kantarci, *Communication Infrastructures for Cloud Computing: Design and Applications*. IGI Global.

[2] Z. Sanaei, S. Abolfazli, A. Gani, and R. Buyya, "Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 369–392, 2014.

[3] A. R. Khan, M. Othman, S. A. Madani, and S. U. Khan, "A Survey of Mobile Cloud Computing Application Models," *IEEE Communications Surveys Tutorials*, vol. 16, no. 1, pp. 393–413, 2014.

[4] K. Dar, M. Bakhouya, J. Gaber, M. Wack, and P. Lorenz, "Wireless communication technologies for ITS applications," *IEEE Communications Magazine*, vol. 48, no. 5, pp. 156–162, May 2010.

[5] M. Valera and S. A. Velastin, "Intelligent distributed surveillance systems: a review," *IEE Proceedings - Vision, Image and Signal Processing*, vol. 152, no. 2, pp. 192–204, Apr. 2005.

[6] M. Whaiduzzaman, M. Sookhak, A. Gani, and R. Buyya, "A Survey on Vehicular Cloud Computing," *Journal of Network and Computer Applications*, vol. 40, pp. 325–344, Apr. 2014.

[7] M. Aloqaily, B. Kantarci, and H. T. Mouftah, "Vehicular clouds: State of the art, challenges and future directions," *2015 IEEE Jordan Conference on Applied Electrical Engineering and Computing Technologies (AEECT)*, pp. 1–6, Nov. 2015.

[8] M. A. Razzaque, A. S. S., and S. M. Cheraghi, "Wireless Networks and Security: Issues, Challenges and Research Trends, Security and Privacy in Vehicular Ad-Hoc Networks: Survey and the Road Ahead," S. Khan and A.-S. Khan Pathan, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 107–132.

[9] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on {VANET} security challenges and possible cryptographic solutions," *Journal of Vehicular Communications*, vol. 1, no. 2, pp. 53–66, 2014.

[10] S. Pearson and A. Benameur, "Privacy, Security and Trust Issues Arising from Cloud Computing," *2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, pp. 693–702, Nov. 2010.

[11] R. S. Schwartz, R. R. R. Barbosa, N. Meratnia, G. Heijenk, and H. Scholten, "A directional data dissemination protocol for vehicular environments," *Journal of Computer Communications*, vol. 34, no. 17, pp. 2057–2071, 2011.

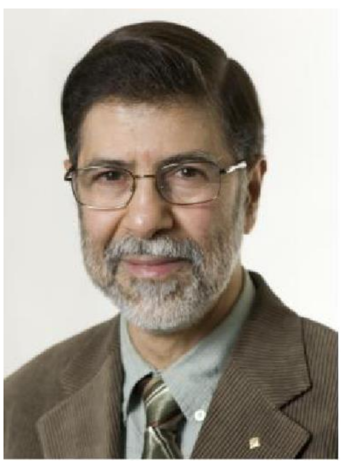
[12] J. Zhao, C. Wu, and Z. Li, "Cost Minimization in Multiple IaaS Clouds: A Double Auction Approach," *Journal arXiv preprint arXiv:1308.0841*, vol. abs/1308.0841, 2013.

[13] W. Chen, R. K. Guha, T. J. Kwon, J. Lee, and Y.-Y. Hsu, "A survey and challenges in routing and data dissemination in vehicular ad hoc networks," *Journal of Wireless Communications and Mobile Computing*, vol. 11, no. 7, pp. 787–795, 2011.

[14] M. Aloqaily, B. Kantarci, and H. T. Mouftah, “An Auction-driven Multi-objective Provisioning Framework in a Vehicular Cloud,” *IEEE GLOBECOM Workshop on Cloud Computing Systems, Networks and Applications*, pp. 1–6, 2015.
[15] M. Mun, S. Hao, N. Mishra, K. Shilton, J. Burke, D. Estrin, M. Hansen, and R. Govindan, “Personal Data Vaults: A Locus of Control for Personal Data Streams,” in *The 6th International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, 2010, pp. 17:1–17:12.
[16] J. Suomalainen and J. Julku, “Enhancing Privacy of Information Brokering in Smart Districts by Adaptive Pseudonymization,” *IEEE Access Journal*, vol. 4, pp. 914–927, 2016.
[17] E. Fonseca, A. Festag, R. Baldessari, and R. L. Aguiar, “Support of Anonymity in VANETs - Putting Pseudonymity into Practice,” in *IEEE Wireless Communications and Networking Conference (WCNC)*, 2007, pp. 3400–3405.
[18] R. Hussain, S. Kim, and H. Oh, *Towards Privacy Aware Pseudonymless Strategy for Avoiding Profile Generation in VANET*, vol. 5932. Information Security Applications, 2009, pp. 268–280.
[19] K. Plobl and H. Federrath, “A privacy aware and efficient security infrastructure for vehicular ad hoc networks,” *Journal of Computer Standards and Interfaces, State of standards in the information systems security area*, vol. 30, no. 6, pp. 390–397, 2008.
[20] D. F., F. K, and H. Lohr, “PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET),” in *IEEE Vehicular Networking Conference (VNC)*, 2014, pp. 25–32.
[21] A. Lazarevic, L. Ertöz, V. Kumar, A. Ozgur, and J. Srivastava, “A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection.,” in *Proceedings of the SIAM International Conference on Data Mining*, 2003, pp. 25–36.
[22] G. Androulidakis, V. Chatzigiannakis, and S. Papavassiliou, “Network anomaly detection and classification via opportunistic sampling,” *IEEE Network*, vol. 23, no. 1, pp. 6–12, Jan. 2009.
[23] P. Xu, H. Jin, Q. Wu, and W. Wang, “Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack,” *IEEE Transactions on Computers,*, vol. 62, no. 11, pp. 2266–2277, Nov. 2013.
[24] R. Chen, Y. Mu, G. Yang, F. Guo, and X. Wang, “Dual-Server Public-Key Encryption With Keyword Search for Secure Cloud Storage,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 789–798, Apr. 2016.
[25] F. Kargl, P. Papadimitratos, L. Buttyan, M. Mter, E. Schoch, B. Wiedersheim, T. V. Thong, G. Calandriello, A. Held, A. Kung, and J. P. Hubaux, “Secure vehicular communication systems: implementation, performance, and research challenges,” *IEEE Communications Magazine*, vol. 46, no. 11, pp. 110–118, Nov. 2008.
[26] S. Ren and M. van der Schaar, “Dynamic Scheduling and Pricing in Wireless Cloud Computing,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2283–2292, Oct. 2014.
[27] Y. Kim, J. Kwak, and S. Chong, “Dual-side dynamic controls for cost minimization in mobile cloud computing systems,” in *13th International Symposium on Modeling and Optimization in Mobile Ad Hoc, and Wireless Networks (WiOpt),*, 2015, pp. 443–450.
[28] I. Menache, A. Ozdaglar, and N. Shimkin, “Socially Optimal Pricing of Cloud Computing Resources,” in *Proceedings of the 5th International ICST Conference on Performance Evaluation Methodologies and Tools*, 2011, pp. 322–331.
[29] M. Mihailescu and Y. M. Teo, “Dynamic Resource Pricing on Federated Clouds,” in *10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid),*, 2010, pp. 513–517.
[30] C. Liu and C. Chigan, “RPB-MD: Providing robust message dissemination for vehicular ad hoc networks,” *Journal of Ad Hoc Networks*, vol. 10, no. 3, pp. 497–511, 2012.
[31] H. Yoo and D. Kim, “Repetition-based cooperative broadcasting for vehicular ad-hoc networks,” *Journal of Computer Communications*, vol. 34, no. 15, pp. 1870–1882, 2011.
[32] M. Torrent-Moreno, F. Schmidt-Eisenlohr, H. Fussler, and H. Hartenstein, “Effects of a realistic channel model on packet forwarding in vehicular ad hoc networks,” in *IEEE Wireless Communications and Networking Conference (WCNC),*, 2006, vol. 1, pp. 385–391.
[33] ITU-T, “Definition of Quality of Experience (QoE).” ITU-T, May-2007.
[34] M. Varela, L. Skorin-Kapov, and T. Ebrahimi, “Quality of Experience: Advanced Concepts, Applications and Methods,” Springer International Publishing, 2014, pp. 85–96.
[35] M. Aloqaily, B. Kantarci, and H. T. Mouftah, “A Generalized Framework for Quality of Experience (QoE)-based Provisioning in a Vehicular Cloud,” in *IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB),*, 2015.
[36] M. Aloqaily, B. Kantarci, and H. T. Mouftah, “On the impact of quality of experience (QoE) in a vehicular cloud with various providers,” in *11th IEEE conference on High-capacity Optical Networks and Emerging/Enabling Technologies (HONET),*, 2014, pp. 94–98.
[37] N. Yaagoubi and H. T. Mouftah, “User-Aware Game Theoretic Approach for Demand Management,” *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 716–725, Mar. 2015.
[38] W. Saad, Z. Han, A. Hjorungnes, D. Niyato, and E. Hossain, “Coalition Formation Games for Distributed Cooperation Among Roadside Units in Vehicular Networks,” *IEEE Journal of Selected Topics in Communications*, vol. 29, no. 1, pp. 48–60, Jan. 2011.
[39] Y. He, L. V. Sun, W. Yang, and H. Li, “A Game Theory-Based Analysis of Data Privacy in Vehicular Sensor Networks,” *International Journal of Distributed Sensor Networks*, vol. 1, no. 1, p. 14, Jan. 2014.
[40] W. Saad, Z. Han, H. V. Poor, and T. Basar, “Game-Theoretic Methods for the Smart Grid: An Overview of Microgrid Systems, Demand-Side Management, and Smart Grid Communications,” *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 86–105, 2012.
[41] K. Fall and E. Kannan, “The ns Manual (formerly ns Notes and Documentation).” Nov-2011.
[42] M. Pouryazdan, B. Kantarci, T. Soyata, and H. Song, “Anchor-Assisted and Vote-Based Trustworthiness Assurance in Smart City Crowdsensing,” *IEEE Access*, vol. 4, pp. 529–541, 2016.

Moayad Aloqaily received the M.Sc. degree in Electrical and Computer Engineering from Concordia University, Montreal, QC, Canada, in 2012. He was a Teaching Assistant and Laboratory Engineer with the Department of Electrical and Computer Engineering, Concordia University, from 2010 to 2012. He is currently a Research and Teaching Assistant, and pursuing the Ph.D. degree in Electrical and Computer Engineering with the School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Ontario, Canada, with a focus on vehicular cloud and cloud computing, under the supervision of Prof. Hussein T. Mouftah. His current research interests include Wireless Communications/Networks, vehicular cloud computing, cloud computing, autonomic networks, Intelligent Transportation Systems, and policy-based networks management. Mr. Aloqaily is the president of Electrical Engineering Graduate Student Association (EEGSA) at the University of Ottawa since 2014 and the incoming IEEE Photonics Society chair for the upcoming year 2016/2017.

Burak Kantarci is an assistant professor in the Department of Electrical and Computer Engineering at Clarkson University, and the founding director of the next generation communications and computing networks (NEXTCON) research lab at Clarkson. Prior to joining Clarkson, he was a postdoctoral researcher at the School of Electrical Engineering and Computer Science of the University of Ottawa. He received the M.Sc. and Ph.D. degrees in Computer Engineering at Istanbul Technical University in 2005, and 2009, respectively. He received the Siemens Excellence Award in 2005 for his studies in optical burst switching. During his Ph.D. study, he studied as a visiting scholar at UOttawa where he completed the major content of his thesis. Dr. Kantarci has co-authored over one hundred papers in established journals and conferences, and contributed to eleven book chapters. He is the co-editor of the book entitled "Communication Infrastructures for Cloud Computing". Dr. Kantarci has served as the technical program co-chair of seven international conferences/symposia/workshops. He is an editor for IEEE Communications Surveys and Tutorials. Dr. Kantarci also serves as the secretary of IEEE ComSoc Communication Systems Integration and Modelling Technical Committee (CSIM-TC). Dr. Kantarci is a senior member of the IEEE and a member of the ACM.



Hussein Mouftah received the BSc in Electrical Engineering and MSc in Computer Science from the University of Alexandria, Egypt, in 1969 and 1972, respectively, and the PhD in Electrical Engineering from Laval University, Canada, in 1975.
He joined the School of Information Technology and Engineering (now School of Electrical Engineering and Computer Science) of the University of Ottawa in 2002 as a Tier 1 Canada Research Chair Professor, where he became a *Distinguished University Professor* in 2006. He has been with the ECE Dept. at Queen's University (1979-2002), where he was prior to his departure a Full Professor and the Department Associate Head. He has six years of industrial experience mainly at Bell Northern Research of Ottawa (Nortel Networks). He served as Editor-in-Chief of the IEEE Communications Magazine (1995-97) and IEEE ComSoc Director of Magazines (1998-99), Chair of the Awards Committee (2002-03), Director of Education (2006-07), and Member of the Board of Governors (1997-99 and 2006-07). He has been a Distinguished Speaker of the IEEE Communications Society (2000-2007). He is the author or co-author of 10 books, 72 book chapters and more than 1400 technical papers, 14 patents, 6 invention disclosures and 144 industrial reports. He is the joint holder of 20 Best/Outstanding Paper Awards. He has received numerous prestigious awards, such as the 2016 R.A. Fessenden Medal in Telecommunications Engineering of IEEE Canada, the 2015 IEEE Ottawa Section Outstanding Educator Award, the 2014 Engineering Institute of Canada K. Y. Lo Medal, the 2014 Technical Achievement Award of the IEEE Communications Society Technical Committee on Wireless Ad Hoc and Sensor Networks, the 2007 Royal Society of Canada Thomas W. Eadie Medal, the 2007–2008 University of Ottawa Award for Excellence in Research, the 2008 ORION Leadership Award of Merit, the 2006 IEEE Canada McNaughton Gold Medal, the 2006 EIC Julian Smith Medal, the 2004 IEEE ComSoc Edwin Howard Armstrong Achievement Award, the 2004 George S. Glinski Award for Excellence in Research of the University of Ottawa Faculty of Engineering, the 1989 Engineering Medal for Research and Development of the Association of Professional Engineers of Ontario, and the Ontario Distinguished Researcher Award of the Ontario Innovation Trust.
Dr. Mouftah is a Fellow of the IEEE (1990), the Canadian Academy of Engineering (2003), the Engineering Institute of Canada (2005) and the Royal Society of Canada RSC Academy of Science (2008).