Secure Pricing-Based Resource Selection in the Vehicular Cloud

Seemran Mishra

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Secure Pricing-Based Resource Selection in the Vehicular Cloud

Thesis submitted in partial fulfillment

of the requirements for the degree of

Master of Technology

in

Computer Science and Engineering
(*Specialization*: *Information Security*)

by

Seemran Mishra

(Roll Number: 713CS2049)

based on research carried out

under the supervision of

Prof. Bibhudatta Sahoo

May, 2018

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Department of Computer Science and Engineering
National Institute of Technology Rourkela

May 26, 2018

Certificate of Examination

Roll Number: *713CS2049*
Name: *Seemran Mishra*
Title of Thesis: *Secure Pricing-Based Resource Selection in the Vehicular Cloud*

We the below signed, after checking the thesis mentioned above and the official record book (s) of the student, hereby state our approval of the thesis submitted in partial fulfillment of the requirements for the degree of *Master of Technology* in *Computer Science and Engineering* at *National Institute of Technology Rourkela*. We are satisfied with the volume, quality, correctness, and originality of the work.

Prof. Bibhudatta Sahoo
Principal Supervisor

Prof. Debi Prosad Dogra
External Examiner

Prof. Durga Prasad Mohapatra
Head of the Department

Department of Computer Science and Engineering
National Institute of Technology Rourkela

Prof. Bibhudatta Sahoo
Associate Professor

May 26, 2018

Supervisor's Certificate

This is to certify that the work presented in the thesis entitled *Secure Pricing-Based Resource Selection in the Vehicular Cloud* submitted by *Seemran Mishra*, Roll Number 713CS2049, is a record of original research carried out by her under my supervision and guidance in partial fulfillment of the requirements of the degree of *Master of Technology* in *Computer Science and Engineering*. Neither this thesis nor any part of it has been submitted earlier for any degree or diploma to any institute or university in India or abroad.

_____
Prof. Bibhudatta Sahoo

Dedication

To my parents.
Thank you for the endless love, continuous care, unwavering support and patience.
You motivate me in every step to strive forward.
You are the reason of what I am today.

Signature

Declaration of Originality

I, *Seemran Mishra*, Roll Number *713CS2049* hereby declare that this thesis entitled *Secure Pricing-Based Resource Selection in the Vehicular Cloud* presents my original work carried out as a postgraduate student of NIT Rourkela and, to the best of my knowledge, contains no material previously published or written by another person, nor any material presented by me for the award of any degree or diploma of NIT Rourkela or any other institution. Any contribution made to this research by others, with whom I have worked at NIT Rourkela or elsewhere, is explicitly acknowledged in the dissertation. Works of other authors cited in this dissertation have been duly acknowledged under the sections "Reference" or "Bibliography". I have also submitted my original research records to the scrutiny committee for evaluation of my dissertation.

I am fully aware that in case of any non-compliance detected in future, the Senate of NIT Rourkela may withdraw the degree awarded to me on the basis of the present dissertation.

May 26, 2018
NIT Rourkela

Seemran Mishra

Acknowledgment

Foremost, I wish to express my deepest gratitude to the late Prof. Sanjay Kumar Jena for the invaluable counsel and encouragement. I owe an earnest obligation to my supervisor Prof. Bibhudatta Sahoo for his perpetual support. His unparalleled guidance and invaluable suggestions have made this research work feasible. I am eternally indebted to Prof. Abhaya Nayak for introducing me to academic life and incessantly mentoring me in every aspect. I am extremely grateful to Prof. Young Choon Lee for providing me with exceptional opportunities and guidance. I extend a heartfelt regard to Prof. Soumyadev Maity for enlightening me on state-of-the-art research and being an extraordinary mentor. It was a great privilege to have got a chance to learn from such inspiring individuals.

I am highly obligated to all the faculty members of the Department of CSE for educating me in the field of computer science. I am most thankful to all the teachers who have contributed in defining me as an individual. A wholehearted thanks to all my friends for their thoughtful assistance.

I would like to acknowledge the boundless affection of my parents who have been the pillar of my life. My every success and accomplishment can be attributed to my father for being a role model and incorporating within me the fearless attitude of confronting every obstacle in life, my mother for building my foundation and filling me with goodness and simplicity. I find myself lucky and thank the Almighty for surrounding me with such connections. I could not ask for more.

May 26, 2018
NIT Rourkela

Seemran Mishra
Roll Number: 713CS2049

Abstract

Vehicular Cloud, which is constituted by gathering the under-utilized resources called On-Board Units (OBU) of the vehicles, has received considerable attention in the recent years. Since the vehicular nodes are privately owned and might be selfish, proper incentive needs to be provided to the vehicular owners for motivating them to join the Vehicular Cloud. Selecting vehicles to supply resources is a crucial research problem which highly depends on the pricing of the resources. Subsequently, resource pricing is an intricate problem influenced by the market demand and quality of service provided. Widespread and autonomous vehicular network requires reputation as a medium for trusting the supplier vehicles. We model the resource selection problem in the Vehicular Cloud as a utility maximization problem. This utility takes into account all the mentioned factors, specifically resource pricing, quality of services provided, and trustworthiness of the supplier vehicles. Subsequently, three pricing-based resource selection mechanisms, namely second-score sealed bid auction, multi-attribute Vickrey's auction, and first-score sealed bid auction are proposed and modeled to maximize consumer utility. The proposed protocols are compared with standard pricing-based resource selection mechanisms in a comprehensive simulation environment and the results indicate that the first-score sealed bid auction performs better than the rest. While implementing the proposed protocols, we face a varied number of security challenges such as authentication of the participating vehicles, confidentiality of the sealed-bid messages and maintaining the integrity of the messages containing negotiated price and quality. Preserving privacy of the vehicles at all instants is vital for the Vehicular Cloud environment where revealing the actual identity might pose a dire threat to these autonomous vehicles. We propose a lightweight hash chain mechanism Hashcryption built on the top of Identity-Based Cryptography for the authentication purpose. Pseudonymous identities of the vehicles instead of their real identities are employed for conditional privacy preservation. Additionally, the Identity-Based Cryptography techniques along with the Hashcryption scheme is added to the proposed auction protocols. Results illustrated that the Hashcryption scheme was computationally efficient than the existing signature-based encryption scheme. Security analysis of the modified auction protocols demonstrated that they satisfy the necessary security requisites.

***Keywords*: *Vehicular Cloud*; *Resource Selection and Pricing*; *Second-Score Sealed Bid Auction*; *Multi-Attribute Vickrey's Auction*; *First-Score Sealed Bid Auction*; *Utility Maximization*; *Hash Chains*; *Identity-Based Cryptography*.**

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

The ever-increasing vehicular fleet in the present roadways had led to an extensive use of Intelligent Transportation Systems (ITS). This has made the vehicular ad-hoc networks a dominant field in the research community. The vehicles are being equipped with highly potential computation, communication, and sensing resources and can be envisioned as computers on the move. A higher percentage of these vehicular resources remain idle which can be aggregated together to develop a pool of mobile computers. This notion as proposed by Olariu et al. as Autonomous Vehicular Cloud (AVC) [1].

Vehicular Cloud has widespread applications in the field of traffic management, infotainment services, and road safety[2]. It can be used for time synchronization of traffic lights to reduce fuel consumption and efficient route discovery for mitigating traffic congestion [3]. Cheap and fast multi-media download, location-based information provision are some of the infotainment services offered by the Vehicular Cloud [4]. Stationary infrastructures like shopping malls and airports can use the resource units of the parked vehicles to form data center and earn revenue [5]. Localized advertisements by these malls can be propagated through the Vehicular Cloud for boosting their business. Additionally, the vehicular owners can give their resources on rent to earn some extra income.

To fully exploit the concept of the Vehicular Cloud, many research challenges have to be addressed [6]. Determining proper incentives to be offered for encouraging the vehicles to provide resources is a major issue. Selecting the fitting vehicles for resource provision as per consumer needs is another problem to be addressed. Service delay and latency of cloud formation have to be taken care of to fully exploit this concept. Other open issues in the Vehicular Cloud are the development of a standardized architecture, security and privacy preservation of the participating vehicles and sensing and aggregation of vehicular data.

The organization of this chapter is as follows: Section 1.2 defines and details the importance of the Vehicular Cloud. Additionally, a brief description of the potential applications of the Vehicular Cloud is given. In Section 1.3 open issues in the Vehicular Cloud is explained. The problem to be addressed in this research work is elaborated in Section 1.4. The research contributions done in this work is summarized in Section 1.5.

Section 1.6 illustrates an abstract view of the thesis.

1.2 Vehicular Cloud

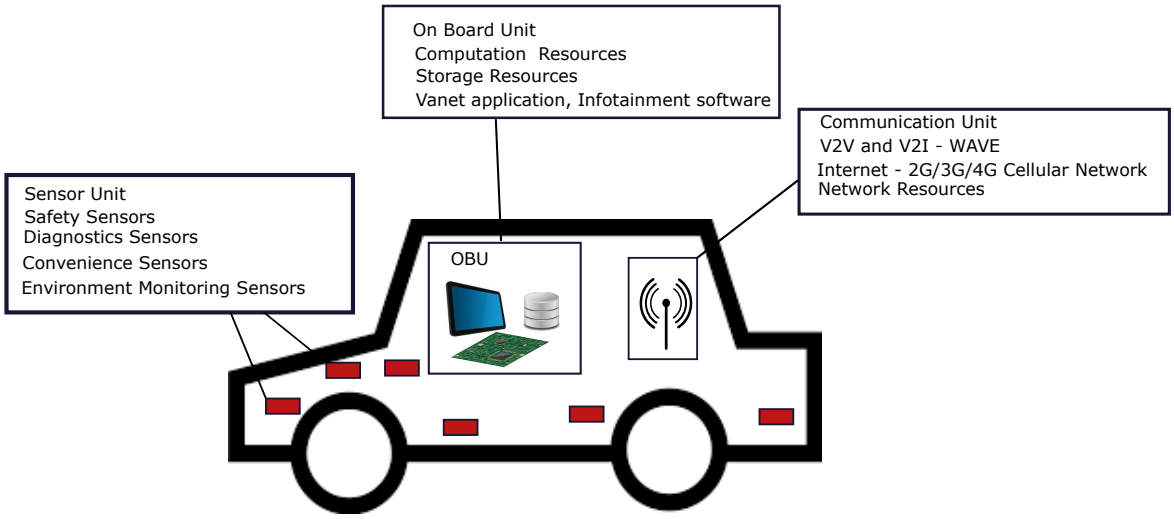

Figure 1.1: Vehicle as a Resource

With the high demand for ITS, the modern day vehicles are equipped with potential On-Board Units (OBU) and can be envisioned as highly mobile computers with substantial computing, networking, and sensing capabilities [6]. Block diagram of a vehicle as a resource node is depicted in Figure 1.1. The sensing unit includes diagnostic sensors essential for monitoring the condition of car machinery like precise control of the fuel and ignition. The safety sensors help in reduction of road accidents and other driving hazards. Environment sensors provide alerts to the drivers on traffic conditions while the convenience sensors provide comfort and entertainment services to the car passengers. The average number of sensors present in the newly manufactured vehicles range from 70-100 [7].

Nowadays the OBUs have abundant computing capabilities to process the applications resulting from the extensive exploration of traffic management, infotainment and other directions of the transportation system. For instance, CPU with quadcore processors as powerful as Intel® Core™ i7-7920HQ with maximum frequency or CPU cycles 4.1 GHz have been embedded in OBUs [8],[9]. Additionally, the computing power is provided by GPU like NVIDIA® GeForce GTX 1050 with frequency 1.8 GHz [10]. External storage units with memory in Terabytes can be connected in addition to the existing storage. These are used as a part of the OBU to meet the requirements.

Vehicles contain a communication unit which supports Wireless Access of Vehicular Environment (WAVE) protocol for vehicular and road-side communication and has cellular network coverage for the Internet access. WAVE is a wireless technology specified for vehicular communications that has been developed based on IEEE 802.11p protocol and Dedicated Short Range Communication (DSRC) [11],[12],[13]. Vehicles use the WAVE

technology to communicate with each other through Vehicle to Vehicle communication (V2V) as well as with the Road Side Unit (RSU) through Vehicle to Infrastructure communication (V2I). Also using the WAVE protocol, the roadside units can send messages to the vehicles in their communication range using Infrastructure to Vehicle communication (I2V) and to each other through Infrastructure to Infrastructure communication (I2I). Communications access for land mobiles (CALM) comprises of wireless communication protocols and air interfaces supporting short, medium and long-range, safety critical communications for applications pertaining to Intelligent Transportation System [14]. Vehicles also use the CALM technology to have the Internet connectivity through 2G/3G cellular communication.

The present-day traffic state has a highly inconsistent nature with unexpected situations like accidents and congestions occurring regularly yet randomly. In many cases, handling such events efficiently goes beyond the power of a single OBU and renting additional resource units seems to be the only feasible solution. Using the services of traditional centralized systems where you have to pre-assign the resources leads to wastage of these resources for a majority time. Also, as the magnitude of these situations increases, the amount of resource to be rented can hardly be pre-determined.

As seen previously, the OBU of vehicles is resource enriched and a huge percentage of moving vehicles occasionally it to the full capacity. Instead, they can rent their idle OBUs to other vehicles deal with such dynamic traffic conditions as described above in exchange for some payment. Such resource units can be pooled together to provide on-demand, proactive and scalable solutions that would otherwise take a conventional cloud unreasonable time. Olariu et al. realized the above notion thereby coining the word Autonomous Vehicular Cloud (AVC) [1]. It is defined as a large group of largely autonomous vehicles whose corporate computing, sensing, communication and physical resources can be coordinated and dynamically allocated to authorized users.

The Vehicular Cloud can be distinguished from the traditional cloud due to its unique property of mobility and autonomy. The localized high-speed communication between the vehicles make AVC a low cost and better alternative for ITS applications than centralized resources. Due to its infrastructure-less nature, AVC can deal with situations where there is no Internet connectivity because of the lack of nearby RSUs, and connection to the conventional cloud seems impossible. Due to the availability of ITS applications in OBUs of other vehicles which would otherwise be required to set up in the conventional cloud, AVC provides efficient and less time-consuming solution for transportation systems. Other benefits of the Vehicular Cloud include:

- Support for pay-as-you-go model with cheap resources.
- Excellent provider of location based services.
- An ideal medium for public sensing purposes.

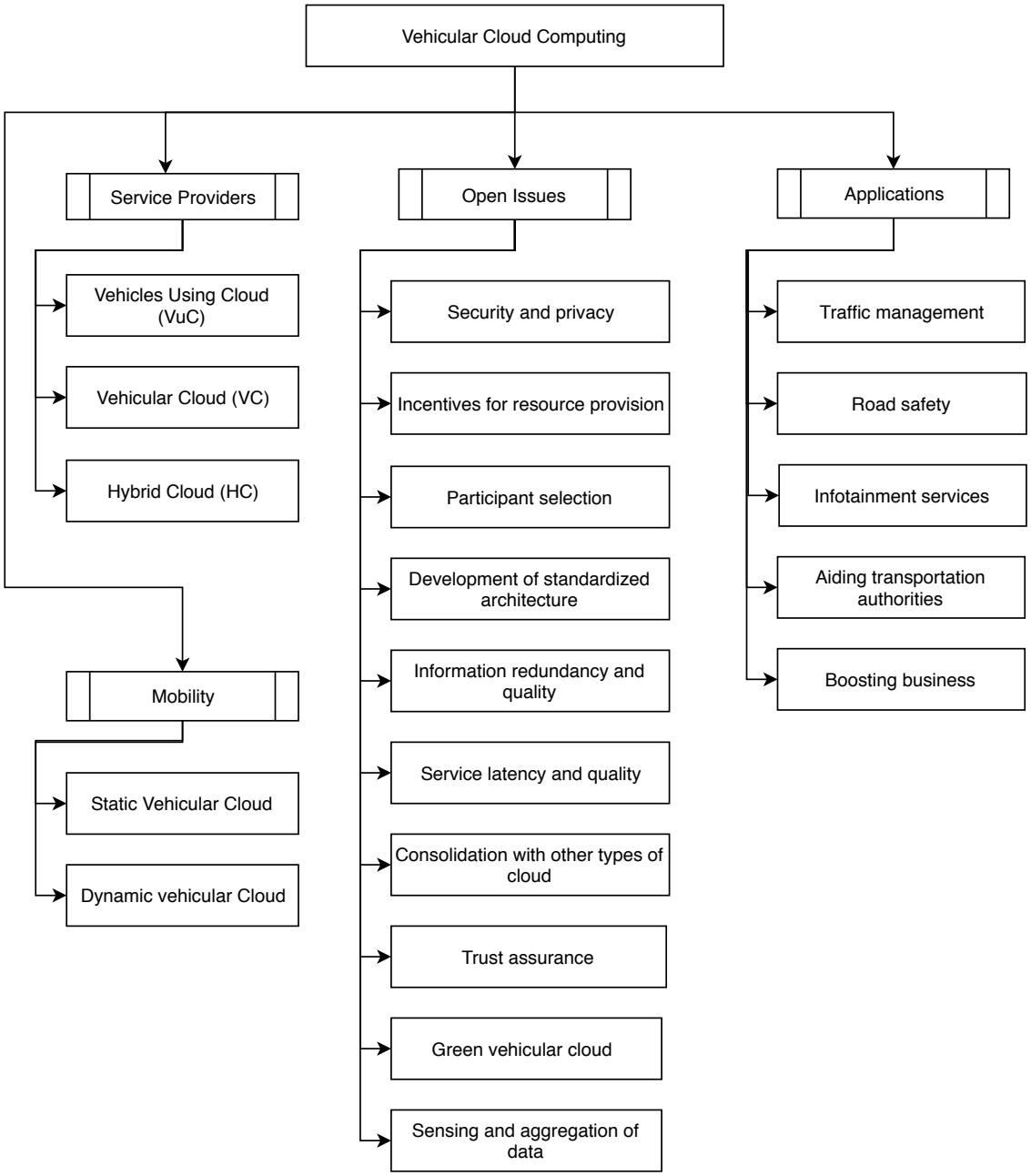

Figure 1.2: Vehicular Cloud Taxonomy

A taxonomy of vehicular cloud computing is presented in Figure 1.2. Depending on the mobility of the Vehicular Cloud, it is subdivided into Static Vehicular Cloud and Dynamic Vehicular Cloud. Based on whether the Vehicular Cloud uses the help of the permanent cloud formed by data centers, it is divided into Vehicles using Cloud, Vehicular Cloud, and Hybrid Cloud. Some applications and research challenges faced by the Vehicular Cloud are also shown in that figure.

1.2.1 Vehicular cloud applications

The application areas of the Vehicular Cloud is illustrated in Figure 1.3. The Vehicular Cloud has potential utilization in the field of traffic management [2]. A huge percentage of cars stay idle in the parking lot of stationary infrastructures like shopping malls, airports, and business offices who resources can be aggregated to form a temporary data center for boosting business with additional income in returned of monetary incentives or discounted offers [5]. They can also be exploited for dynamic management of the parking lots without dependence on external resources [15]. Vehicular Cloud is an apt solution for dealing with the dynamic nature of traffic jams. The scalability feature of the Vehicular Cloud provides the proper amount of resources rather than excessive preallocated resources through the conventional cloud. The vehicles can collectively determine the uniform distribution among all routes for traffic congestion mitigation [3], [16]. Also, they can cooperatively move in clusters to synchronize traffic lights for unnecessary halting to save fuel. The vehicular cloud can perform computation and other data mining services using the location-based data of all vehicles to aid the authorities in traffic management.

Vehicular cloud computing also provides road safety services to the vehicles by accident alerts and predetermining the road-conditions to alert the driver [17]. Even the car manufacturing companies can use the Vehicular Cloud concept for diagnosis of vehicles and eliminate the problems in the future releases. The urban surveillance service to monitor the road traffic conditions using the sensing capabilities of the vehicles can help in improving transport conditions and thereby reducing accident rate [18]. Self-driving autonomous cars is the current trend and they can cooperate by forming a cloud to effectively decide their travel plans, prevent traffic jams and reduce the fuel consumption [19]. Since they have high computational requirements, and in some scenarios their own resources might not be sufficient, they can rent resources from vehicular cloud.

Vehicular Cloud computing also provides infotainment services to the vehicles. They can collectively use the networking resources of neighboring vehicles to ensure fast content download [4]. Additionally, vehicular cloud computing can be exploited to notify the vehicles about attractive offers of the nearby restaurants and shopping centers and any other information they require.

All these applications make the Vehicular Cloud a potential concept that should be fully developed for the betterment of transportation systems.

1.3 Open issues in Vehicular Cloud

The use of the Vehicular Cloud computing is limited since it faces a varied number of challenges. Vehicles are autonomous entities that they require proper incentives to rent their resources for the formation of vehicular cloud. The pricing of these resources has to be determined effectively considering dynamic market demand and quality of service provided

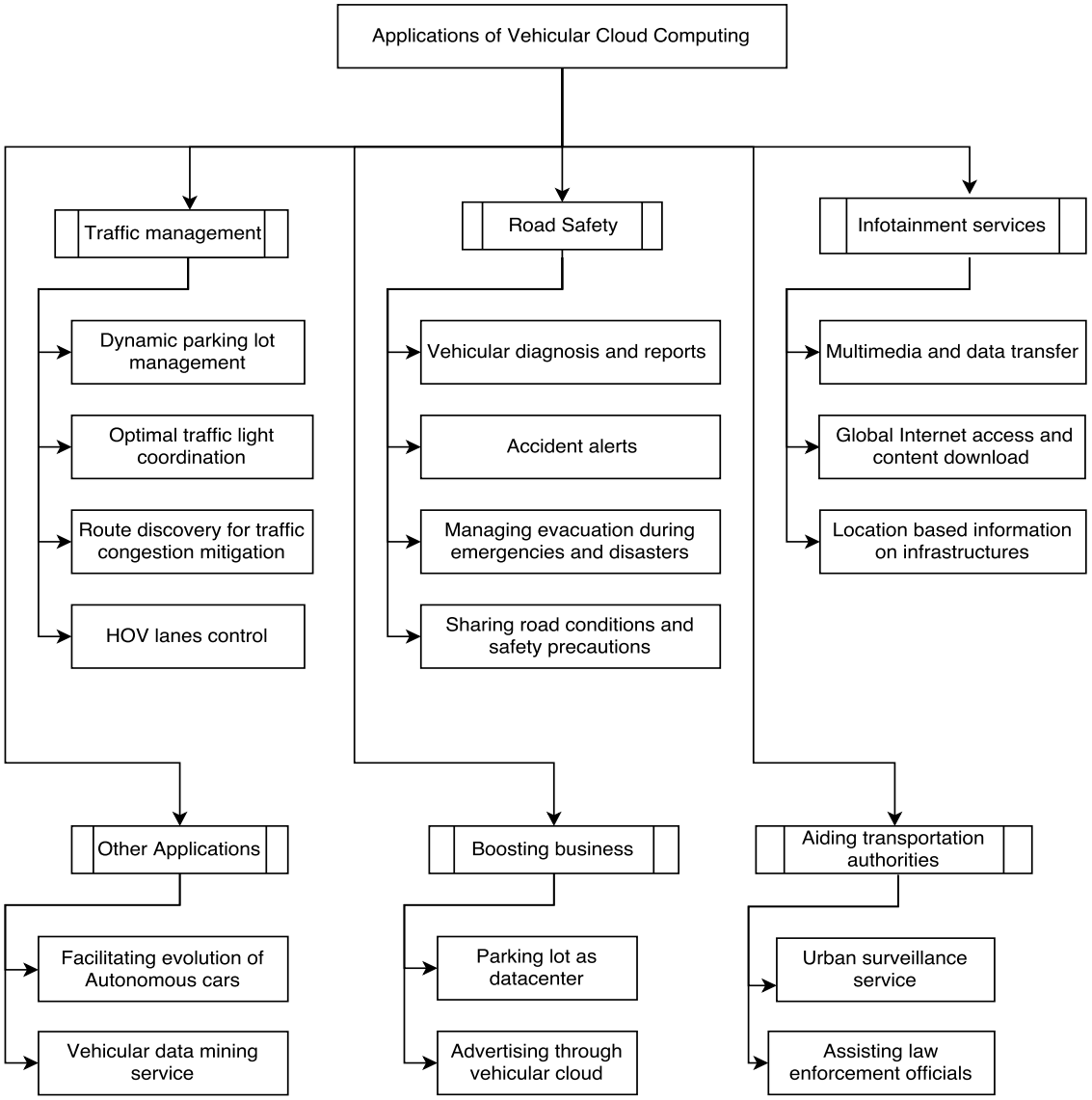

Figure 1.3: Vehicular Cloud Applications

by the vehicles. When incentives in form of monetary payments are provided to supplying vehicles, a large population of vehicles might become interested to become suppliers and an efficient resource selection algorithm has to be designed taking into account the requirements of the consumer vehicle.

There are varied scenarios in which vehicular cloud can be formed. Static vehicular cloud and dynamic vehicular cloud are the two examples when it is classified on the basis of mobility. Determining a standard architecture for the Vehicular Cloud is a research challenge as it depends on the mobility as well as the type of application provided. Research has to be done to ensure that the vehicular cloud formation takes minimum latency and the quality of service provided is desired.

The Vehicular Cloud is built on the top of vehicular networks. The large-scale and autonomous nature of the vehicular networks makes it mandatory to take the security requirements like authentication, non-repudiation, and confidentiality into account. This

is essential for safeguarding the network against the malicious nodes. Revealing the private information like route plans and real identities of vehicles can even cause physical harm to the vehicles and hence privacy preservation is necessary. Trust maintenance in the Vehicular Cloud is another critical issue due to its highly autonomous nature. Other open issues are sensing and aggregating redundant data to ensure high information quality.

1.4 Problem Formulation

For this research work, we aim to address the resource-selection problem in the Vehicular Cloud. As explained previously, it is highly complex due to its dependence on the quality of service provided, trustworthiness and pricing of resources. We aim to consider a performance metric using all of the above factors for evaluation of selection mechanisms to provide maximum utility to the consumer vehicle. Firstly, addressing the resource pricing problem is another crucial challenge which highly depends on the market demand and the quality of service provided. Therefore, our other objective is to determine the optimal quality and pricing value of the resources that the supplier vehicle should declare in order to achieve maximum utility without reducing its chances of winning. Finally, we target to provide the resource selection mechanism with the desired security requirements. The authentication of the participating vehicles has to be done to prevent impersonation attack by the malicious vehicles. Also, the confidentially of certain private messages and it's integrity has to be ensured in the resource selection mechanism. As explained previously, the privacy of the participating vehicles has to be maintained.

Therefore, we aim to design a secure pricing-based resource selection scheme for utility maximization of the participating vehicles.

1.5 Research Contribution

To address the problem formulated in the previous section, we conduct an extensive literature survey. We list the existing works, their objective functions and the mechanisms they have used to address the resource selection problem. Subsequently, we model the resource selection problem by taking into account the pricing of resources, market demand, quality of service provided and trustworthiness of the vehicles in form of utility functions. These utility functions which aim at providing maximum benefit to the vehicular consumers and suppliers are used as performance metrics in the subsequent chapters. We propose three auction-based solution mechanisms namely second-score sealed bid auction, multi-attribute Vickrey's auction and first-score sealed bid auction for solving the resource-selection and pricing in the Vehicular Cloud. Extensive experimentation is performed to compare the proposed auctions with the other standard pricing-based resource selection mechanism. Finally, a lightweight Hashcryption scheme is proposed and is compared with the existing signature-based

encryption techniques. Identity-Based Cryptography schemes along with Hashcryption is added to the proposed auction mechanisms to satisfy the security requirements.

1.6 Thesis Organisation

The present thesis is organized into eight chapters: Chapter 2 gives a detailed analysis of the resource selection problem in the vehicular cloud and its dependence on resource pricing, quality of resource provided, the trustworthiness of suppliers and security requirements. Additionally, the Vehicular Cloud architecture is elaborated. The utility of consumer and supplier vehicles which is the performance metric used in the subsequent chapters is defined. In Chapter 3, a second-score sealed bid auction is proposed for addressing the resource selection problem in the vehicular cloud is designed. The quality of service requirement is relaxed in that chapter. Then three standard resource selection methodologies considering fixed and random pricing of resources are explained and compared with the proposed mechanism using a comprehensive experimental setup. In Chapter 4, a multi-attribute Vickrey's auction which considers the quality of service while resource selection is proposed and is compared with the previous proposed second-score sealed bid auction protocol. In Chapter 5, a first-score sealed bid auction protocol is proposed which considers the market demand factor with topmost priority. A new lightweight Hashcryption scheme built with hash chains on top of Identity-Based Cryptography schemes is proposed in Chapter 6. This scheme along with other cryptography mechanisms are added to the previously proposed pricing-based resource selection protocols to provide to satisfy the security requirements. Chapter 7 concludes the thesis and Chapter 8 provides an insight to the future direction of research work that can be done in this field.

Chapter 2

Resource Selection Problem In the Vehicular Cloud

2.1 Introduction

Due to a substantial increase in the vehicular fleet on the roads, Intelligent Transport System has achieved widespread popularity in the research domain. As discussed in the previous chapter, new vehicles with abundant computing, communication and sensing resources in the form of OBUs have emerged and can be well utilized as modern-day computers. They can tackle highly inconsistent nature of traffic by pooling together and providing on-demand, low cost and high-speed real-time services without dependence on external infrastructures. This gives rise to the concept of Autonomous Vehicular Cloud (AVC) which refers to a large group of largely autonomous vehicles whose corporate computing, sensing, communication and physical resources can be coordinated and dynamically allocated to authorized users.

Understanding the architecture of Vehicular Cloud is important in order to fully exploit its capabilities. Vehicular Cloud computing has many applications in traffic management such as optimal traffic light coordination and route discovery to mitigate congestion. Infotainment services like location-based information and multimedia and data transfer can also be achieved from the Vehicular Cloud. Therefore a lot of research challenges like ensuring service latency and quality, the trustworthiness of participating vehicles and selecting resource providers for the formation of the Vehicular Cloud have to be addressed.

The crux of the concept of AVC is providing proper incentives, most compelling being monetary payments, to the autonomous and selfish vehicular nodes for offering their resources [6]. These monetary payments might instigate a large number of vehicles for resource provision especially in high traffic conditions or fully packed parking lots. This demands a proper selection mechanism to pick out the supplier vehicles best complementing the consumer needs. The dependence of selection mechanism on quality provided as well as the pricing of the resources makes it more complex. Trust has to be established on the supplier vehicles to ensure that malicious vehicles are not selected for service delivery. Again price determination of the service delivered is pivoted on the quality of service and market demand of this service. Many research works have addressed the resource selection

problem but none of them have considered all the issues collectively.

In this chapter, we aim to provide a mathematical formulation of the pricing-based resource selection problem in form of utility functions of consumer and supplier vehicles taking into account all the factors discussed above. We also determine the security challenges which will be confronted which addressing the problem of resource selection and pricing.

The organization of this chapter is as follows: Section 2.2 describes the vehicular cloud architecture and then sub-divides it on the basis of service providers and mobility. Section 2.3 gives a complete insight into the resource selection problem in the vehicular cloud along with the factors it depends on like pricing of resources, quality of service provided, the trustworthiness of the supplier vehicles and some security requirements. Also, a survey of the related work in resource selection domain is presented. In Section 2.4, the utility of consumer and supplier vehicles is designed for modeling the pricing-based resource selection problem as a utility maximization problem and the chapter is summarized in Section 2.5.

2.2 Vehicular Cloud Architecture

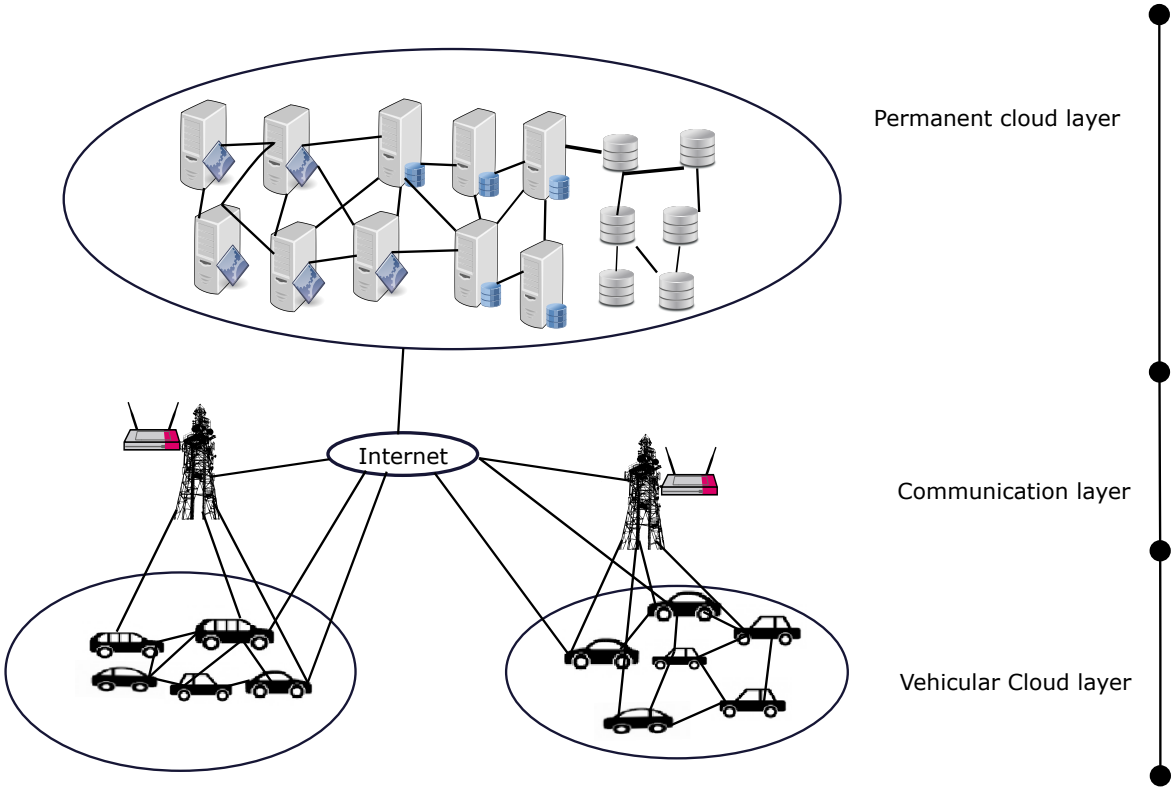

Figure 2.1: Vehicular Cloud Architecture

The enormous fleet of continually moving vehicles with substantial resources as described above can be extensively exploited to form a temporary cloud on the move. They can collaboratively provide processing, analysis, and storage services for localized applications like traffic control and parking lot management more efficiently while reducing

the amount of data transported to the permanent data center cloud.

A multi-tier architecture of vehicular cloud can be visualized by Figure 2.1 where the terminal layer is formed by vehicular nodes grouping together for the creation of a temporary cloud. The vehicular nodes use the communication layer consisting of V2V, V2I, I2V, the Internet connectivity through the cellular network and also through RSUs to provide their services. The final layer is the data center based permanent cloud which can be used by the vehicles for back up and other purposes and is connected through the Internet.

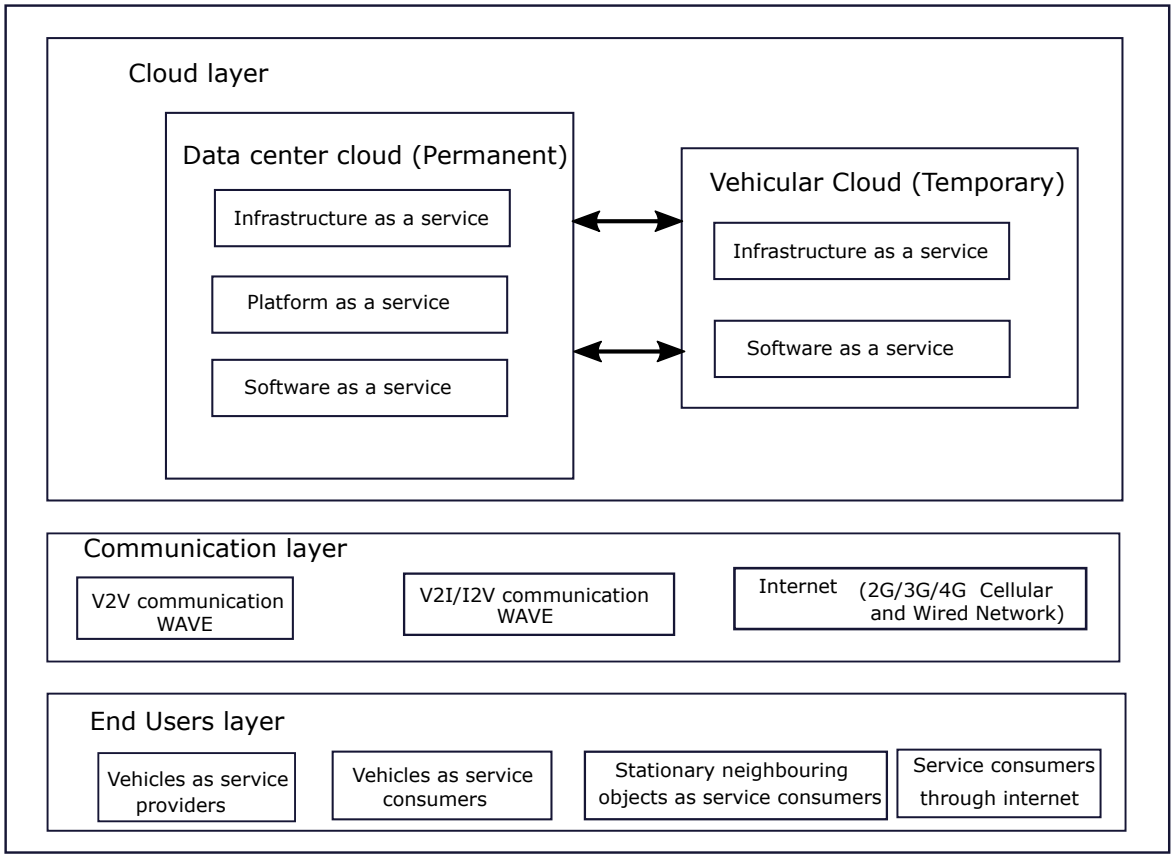

Figure 2.2: Block Diagram of Vehicular Cloud

Vehicular Cloud architecture can be sub-divided into the three abstract layers as shown in Figure 2.2 and is inspired by the VANET-Cloud model in Bitam [20]. The end user layer consists of the vehicular cloud service supplier and consumer entities. The vehicular cloud service suppliers include the vehicular nodes who have abundant resources and are willing to provide their resources to form the vehicular cloud in return for some payment. The service consumers of vehicular clouds may be other vehicles who want to use the resources provided by nearby vehicles while moving. Also, stationary infrastructures like shopping malls or airport authorities may want to use the resources of the vehicles parked in them all day. Even remote users can access the services of vehicular cloud through the Internet.

As it can be seen from Figure 2.3, communication between supplier vehicles and service consumers mostly consisting of neighboring consumer vehicles can occur directly through V2V communication for location-based service provisioning. If the service consumers

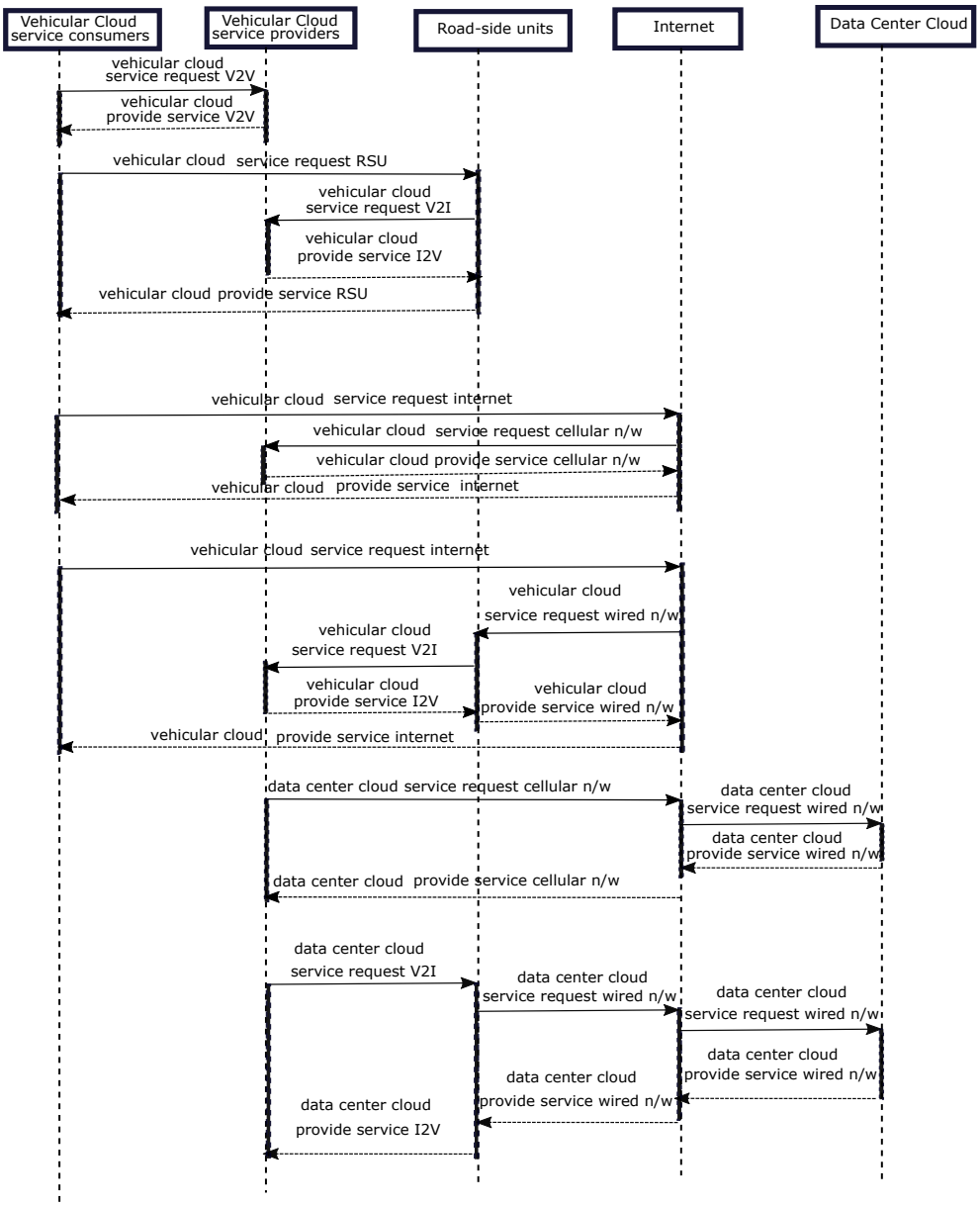

Figure 2.3: Interaction of suppliers and consumers of the Vehicular Cloud

are stationary infrastructures like a parking lot manager or other shopping malls, they can access the vehicular cloud through V2I and I2V communications. Remote vehicular cloud consumers use vehicular cloud through the Internet to which the vehicular supplier nodes can connect directly through the cellular network or through V2I and I2V communications via RSU. Vehicular suppliers can also access the permanent data center cloud for back up purposes or due to heavy resource requirement in addition to their own resources through road-side units or the Internet.

The topmost cloud layer can be further classified into permanent cloud and temporary cloud. The remotely located data centers form the permanent cloud. Pooling of the resources of the supplier vehicles forms the temporary cloud. Similar to the traditional cloud services, the service model of permanent cloud can be classified into the three categories as [21]:

- Software as a service (SaaS): The consumers can use the applications such as email and entertainment running on the supplier's hardware.
- Platform as a service (PaaS): The consumers can deploy consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the supplier onto the cloud infrastructure.
- Infrastructure as a service (IaaS): The supplier provides fundamental computing, storage, and network resources to the consumer.

The service model of temporary vehicular cloud sets itself apart from the traditional cloud by having two layers instead of three. Computing, Storage and networking resources of vehicles can be provided under IaaS. PaaS doesn't seem to be suitable for vehicular cloud framework [22]. SaaS is provided by vehicles when their inbuilt software is accessed by other vehicles for transportation or infotainment purposes.

The cloud computing concerning the vehicular networks can be further subdivided into Vehicles Using Cloud (VuC), Vehicular Cloud(VC) and Hybrid Cloud(HC) based on whether the consumers are using permanent cloud or temporary cloud or both [22].

A) Vehicles Using Cloud

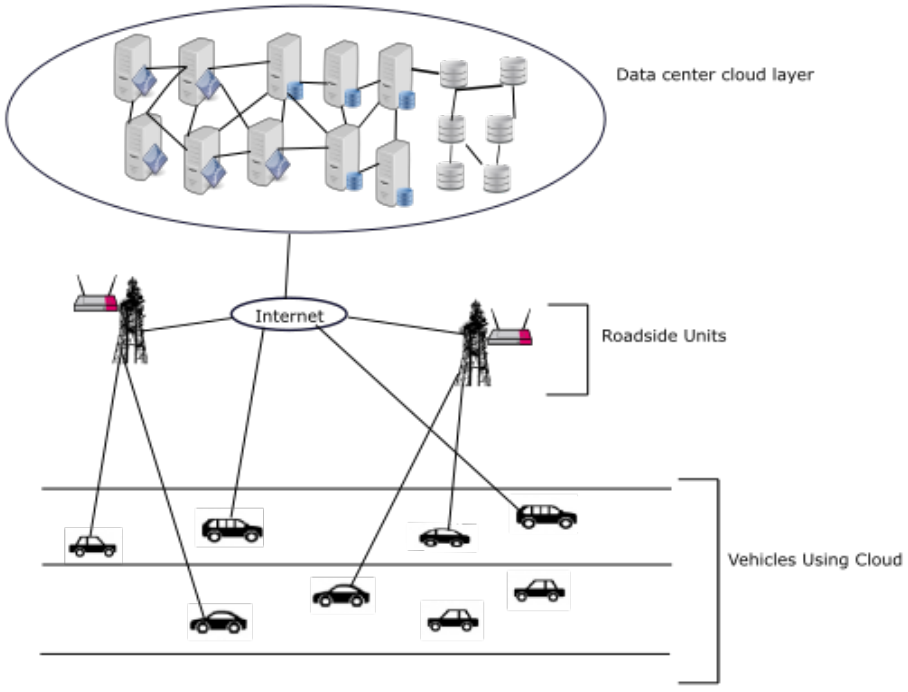

Figure 2.4: Vehicles Using Cloud (VuC)

Figure 2.4 portrays the model of Vehicles Using Cloud (VuC) where the cloud services are only provided by the data center based permanent cloud. The cloud consumers consist of

either vehicles on the road or the parked vehicles and the RSUs form the gateways through which the consumer vehicles access the data center cloud. It is mainly used for storage purposes like data back up while many software services can also be obtained through the Internet using browser and program interface [20].

B) Vehicular Cloud

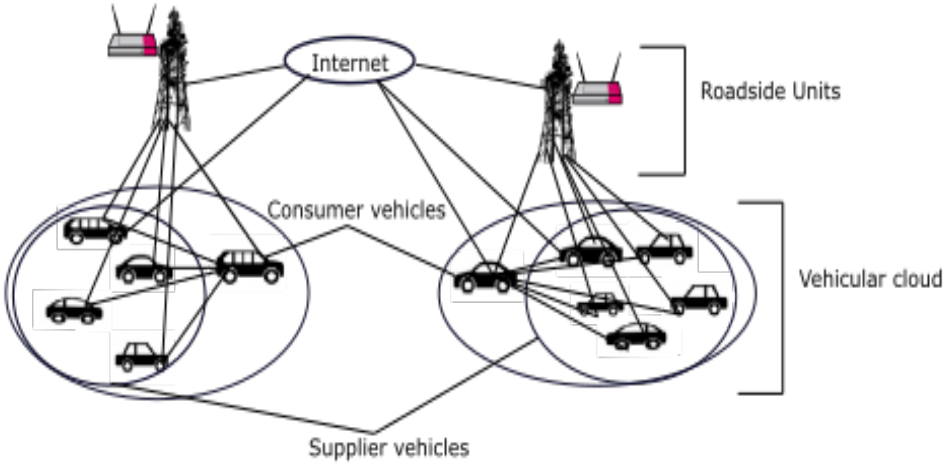

Figure 2.5: Vehicular Cloud (VC)

This work mainly considers Vehicular Cloud (VC) as shown in Figure 2.5. The cloud services are temporary in nature and only provided by the supplier vehicles either on the move or parked ones. The cloud consumers consist of consumer vehicles and location-based stationary road infrastructures like shopping malls, restaurants, etc. Some of its applications as elaborated in the previous chapter include traffic signal optimization, sharing on-road safety messages, urban surveillance and infotainment services like multimedia sharing and shopping mall advertisements.

C) Hybrid Cloud

On combining the previous approaches of VuC and VC, Hybrid Cloud (HC) depicted in Figure 2.6. Here supplier vehicles form the temporary cloud and can also access the data center based permanent cloud through the Internet.
The vehicular cloud can be further sub-divided into Static Vehicular Cloud and Dynamic Vehicular Cloud based on the mobility of the cloud formed by the supplier vehicles [22].

A) Static Vehicular Cloud

As seen in the Figure 2.7, the temporary cloud is stationary and is formed by the parked vehicles. The number and identity of the constituent supplier vehicles may change with

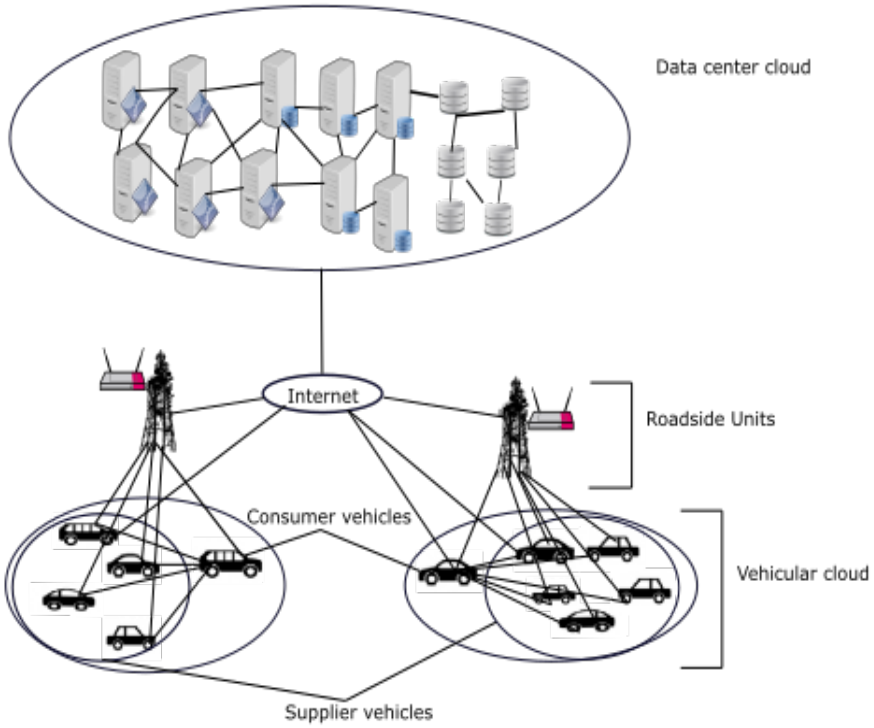

Figure 2.6: Hybrid Cloud (HC)

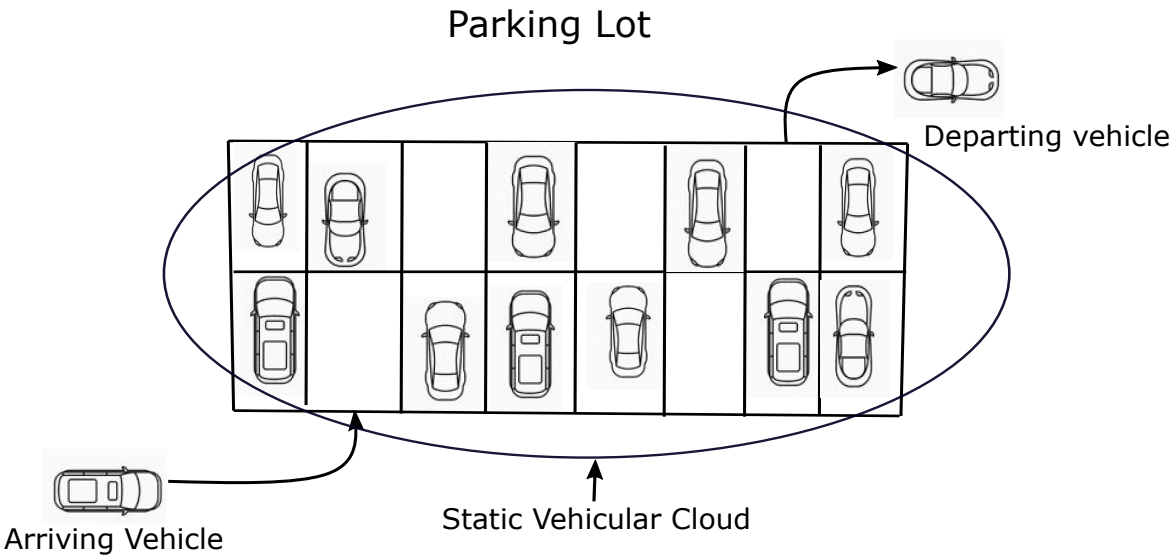

Figure 2.7: Static Vehicular Cloud Example Scenario

respect to time they arrive and depart from the parking lot. A typical application includes dynamic parking lot management.

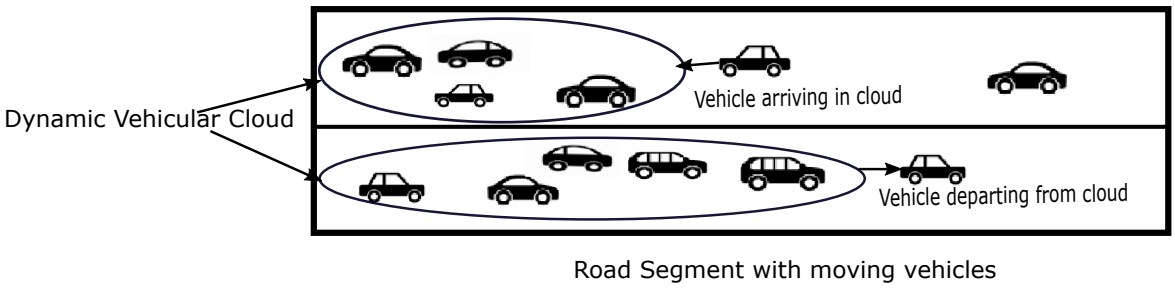

Figure 2.8: Dynamic Vehicular Cloud Example Scenario

B) Dynamic Vehicular Cloud

Here the temporary cloud is on the move as illustrated in Figure 2.8 and similar to the Static Vehicular Cloud, the number and identity of the constituent supplier vehicles changes. They help in traffic light optimization, sharing safety messages, accident alerts, finding optimal routes, providing location-based information and have various other applications.

2.3 Resource selection problem in vehicular cloud

Vehicular cloud sets itself apart from the conventional cloud due to its specialization in ITS applications and this leads to vehicles as the ideal service consumers. Also, due to the high availability of ITS applications in vehicles, they are the ideal service providers in the vehicular cloud as compared to resource enriched permanent cloud. As discussed previously in Section 2.2, the services of vehicular cloud can be either availed locally from the neighboring supplier vehicles or remotely from supplier vehicles through the Internet. Due to low cost and delay of localized vehicular communication and abundant presence of location-based information, we argue that using the services of vehicular cloud locally is better than using it remotely. The only exception lies when there are no neighboring supplier vehicles which is an improbable scenario and forces consumer vehicles to use service remotely. Also, the vehicular cloud can be used as a data center as discussed in the previous chapter. In case of Static Vehicular Cloud, the consumer node is a stationary node and in case of Dynamic Vehicular Cloud, it is a remote user. We argue that using Dynamic Vehicular Cloud as a data center remotely is not economic for the consumer as it can avail cheap resources from the conventional permanent cloud. However, the situation differs in case of Static Vehicular Cloud due to low communication cost.

Encouraging the vehicular nodes for actively providing their resources is vital for the formation of vehicular cloud. Some form of incentive be it monetary or service in return has to be provided [6]. A large number of vehicles might become interested in resource provisioning especially in high traffic conditions or fully packed parking lots due to these incentives. Therefore a proper selection mechanism has to be designed for the consumer vehicle to determine the best supplier vehicles as per its requirements.

In the research works done in this domain, the resource selection process is done by a controller node who can either be a consumer vehicle, leader vehicle or a stationary node (mostly in case of Static Vehicular Cloud) in the shopping center or RSU who lies in the vicinity of the vehicular cloud mostly. A group of supplier vehicles aggregate to form a vehicular cloud, choose a leader based on the performance who controls the vehicular cloud and communicates with the remote user through the Internet. The major difference between the leader vehicle and the consumer vehicle is that the identity of the leader vehicle gets changed after the election. As explained previously in this section, the situations where remote users are required are either improbable or not economic. Therefore, we assume the service consumers to be localized stationary nodes or consumer vehicles making the service consumer to be the controller node.

Consider a generalized scenario where there is one vehicular cloud consumer V_c and n interested supplier vehicles available to provide their resources in return for some incentive. We assume that resources of all supplier vehicles are homogeneous in nature but how much they are being used at the instant varies from vehicle to vehicle. The supplier vehicles put to rent their resources so that it is used to the maximum capacity. Vehicular cloud consumer V_c needs the services of N such supplier nodes. The resource selection problem in the vehicular cloud can be defined as:

Definition 2.1. The process of selecting a set of N vehicular suppliers out of the total n vehicular supplier nodes present by the vehicular consumer V_c.

The first question to address is how to determine the ideal number of resources N of vehicular suppliers which the consumer node requires as per it's service requirements. To solve this, Zheng et al. considered a Stationary Vehicular Cloud of vehicles in a parking lot which he uses as a data center [23]. When a service request arrives at the stationary controller node, it determines whether to process the request locally through Vehicular Cloud or send the request to conventional permanent cloud in case sufficient resources are not present. If it decides to use the local vehicular cloud, it models the problem as a Semi-Markov decision process and determines N. The objective is maximizing reward gained by the system considering revenue gained by task completion and cost of task completion which is energy and time cost for processing it in vehicular Cloud. For processing it in permanent cloud, the task completion cost is communication cost, delay and cost of services of permanent cloud.

Incentives given to the supplier vehicles are most compelling in form of monetary payments [6]. All consumers are assumed to be rational with their major objective being profit maximization which can be done only be selecting resources with low price. The above situation can be seen as a conventional consumer and supplier based market where pricing is the pivot on which the supplier selection is based. So the resource selection problem should depend on the pricing of resources. Determining the pricing of these resources is next challenging problem which has to be solved before dealing with the resource selection problem and is discussed in the next section.

2.3.1 Quality of Service requirements

Quality of Service (QoS) is the description or measurement of the overall performance of a service like availability and delay of service provided by the cloud supplier [24]. It is important for the cloud suppliers who need to determine the right tradeoff between the pricing of resources, quality of service provided and cost of resources. Also, it is important for cloud consumers who expect a flawless service as per the QoS mentioned in Service-level agreement (SLA) paying a higher price for better quality [25]. Aloqaily shows the importance of quality of service in the vehicular cloud by stating that if vehicular consumers are provided with an environment which allows them to have input on decisions regarding the quality required, their feedback will improve the provisioning quality and promote the technology of vehicular cloud itself [26]. Hence resource selection problem should take into account the quality of services required by consumer vehicles and provided by supplier vehicles.

In this work, we consider SaaS and only CaaS and NaaS as the services provided under IaaS. We assume the number of CPU cycles as an evaluation metric for computing services and throughput for networking services. Latency and error rate are the two other performance metrics that ensure a hassle-free communication. Considering the highly mobile nature of vehicles, relative velocity has to be taken into account to prevent the supplier vehicles going outside the transmission range of the consumer vehicle.

2.3.2 Trusting Supplier vehicles

Vehicles are autonomous nodes and trusting a supplier vehicle to provide the resources as per the agreement is definitely a challenge. We have to deal with both selfish and malicious supplier vehicles and ensure that they don't get selected as winners. They can be further categorized into three types:

- Eligible vehicles who get selected as supplier vehicles, escape from the beginning and don't provide any resources at all.
- Eligible vehicles who get selected as supplier vehicles, escape mid-section and don't provide resources till the stipulated time in the contract.
- Eligible vehicles who get selected as supplier vehicles, provide resources till the stipulated time in the contract but don't satisfy the quality of service conditions in the contract.

Many research works in vehicular networks have dealt with the malicious and selfish vehicles by using reputation for trust assurance in the network [27], [28]. The reputation of a supplier vehicle evaluates it on the basis of the service it has provided in the past and is constantly updated by the feedback of the consumer vehicles who use its service. This makes reputation an important factor to be considered in resource selection problem.

2.3.3 Pricing of resources in vehicular cloud

Existing works reveal that incentives that are in form of monetary values come out to be highly motivating for supplier nodes [6]. Aloqaily points out that the service pricing in the vehicular cloud is a critical as well as a complex problem [26]. He states that the resource pricing is challenging as it needs to be dynamic and no proper and efficient service price matching algorithms have been developed to tackle the issue. Also, the privacy of the supplier vehicles has to be ensured during this process. We now define the pricing problem in the vehicular cloud as:

Definition 2.2. The process of determining the monetary value that the vehicular cloud consumer V_c should provide to vehicular cloud supplier in return for utilizing its services.

The question that immediately follows the pricing problem is that "Who will decide the pricing of the resources? Consumer vehicle or supplier vehicle?" Taking any general market scenario into consideration, the seller of the product which is either producer or supplier or the business who owns the product or provides the service sets the price of the product based on the consumer needs [29]. Pricing of resources should depend on:

1. Market demand: The market competition among the resource suppliers highly affects the pricing of resources indicating that the price determination should be dynamic in nature [30], [31]. When there is a low demand yet high availability of resources, an intense competition among the suppliers occurs leading the low pricing since the ulterior motive of the suppliers would be to become winners anyhow. In the contrasting scenario of a high demand for resources by the consumers and low availability, competition occurs among the consumers to possess the scarce resources leading to high resource pricing by the supplier.

2. Quality of service: The cost of services for the suppliers depend on the quality of service provided which heavily affects pricing. Right tradeoff has to be maintained by the supplier node between the resource pricing and quality of service provided to increase its probability of winning. Suppose the supplier node increases the quality of the resource to the optimum level, then the cost of providing the resource will be increased, leading to high pricing if it wants considerable profit. Then the consumer base will be decreased since many consumers will be now aiming for a low priced product will slightly less quality. In the opposite scenario when the quality of the resource is really low leading to low pricing, many genuine customers who want a satisfactory quality resource won't opt for that resource.

Some research works in the vehicular cloud have addressed the pricing issue. In a comparison based selection mechanism called CROWN, pricing of resources is fixed by the supplier vehicles during the registration phase [32]. Consumer vehicles declare the maximum price they are going to provide a resource with a certain quality and the winner is

selected based on a comparison mechanism. This work doesn't consider the dynamic pricing of the resources based on the market demand which is highly essential as discussed above. Lagra et al. also follow the same type of resource pricing as CROWN which is chosen randomly by the supplier node and remains fixed throughout [33].

Kong et al. is the only research work which takes up the dynamic pricing of resources based on the market competition [34]. Considering the optimal strategies of other supplier vehicles, each supplier node decides the amount of resources it will provide which will subsequently determine the pricing of resources and the reward it will receive. This research work doesn't take into account the quality of service parameters provided. Also, the pricing is set by the leader vehicle who consumes the resources and the supplier vehicles don't get a say in it as opposed to a general market case.

None of the previous works have solved the resource pricing problem through the supplier vehicles in vehicular cloud taking into account the market demand and quality of services provided which we consider in our research.

2.3.4 Security challenges for pricing-based resource selection

The security challenges in vehicular networks are more complex than the ones faced by traditional ad-hoc networks due to their high mobility and a large scale nature causing a volatile network where connectivity is one-time and transient in nature [35]. Additionally, this makes tracking down of attackers and other malicious vehicles very difficult. Security challenges encountered during the pricing-based resource selection process are similar to those of vehicular networks. To maintain the trust on supplier vehicles, we have already discussed previously that the use of reputation based on past experience can segregate some malicious nodes from the sincere ones. The security requirements for pricing-based resource selection process are:

1. Privacy preservation of vehicles: All vehicles, namely consumer and supplier vehicle, participating in the pricing and resource selection mechanism are autonomous and unknown to each other. They might not want to reveal sensitive personal information like driver name, license plate, future directions and routes since it jeopardizes their privacy and may also affect their physical security. Conditional privacy preservation must be achieved in a way such that the vehicle must determine the amount of private information it must disclose and still other security requirements like authentication and non-repudiation should be satisfied [36].

2. Traceability of vehicles: Due to the privacy preservation requirement, the vehicular network tilts towards anonymous network where it is difficult to identify and blacklist attackers and other malicious vehicles. We have to ensure that there is a trusted authority present who knows the identity of each and every participating vehicle which

will aid in catching attackers, monetary transfer from consumer to supplier vehicles and also maintenance of reputation of the vehicles.

3. Prevention of impersonation attack: We have to ensure that all vehicles are participating in resource selection and pricing mechanism are authenticated so that only genuine consumer and supplier vehicles form the vehicular cloud. We also have to guarantee that vehicles can not spoof the identity of others. This again becomes difficult due to privacy preservation condition.

4. Ensuring message confidentiality: In the pricing-based resource selection mechanism, the supplier vehicles send messages to the consumer vehicles containing the quality and price of the service which is private information. Since the messages travel through insure channel, any supplier vehicle may eavesdrop and know the strategy of others which will prevent a fair market competition. This requires that these messages should always be encrypted to ensure their confidentiality.

5. Prevention of message tampering: The contract between the consumer and supplier vehicles detailing the quality and pricing of resources is formed through message transfer. Consumer vehicle might tamper with the contract message by increasing the quality and reduce the pricing of the resources for getting higher profit. It will then claim for better quality and provide less price to supplier vehicle on the basis of the new tampered message. Similarly the supplier vehicles can also tamper the message to reduce quality and increase price for their profit maximization. Therefore the integrity of the messages have to be maintained.

6. Authentication and non-repudiation of messages: All transactions between consumer and supplier vehicles occur through message passing. Suppose a malicious vehicle poses as an interested supplier vehicle, takes part in pricing-based resource selection mechanism and wins but then does not provide service. It then claims not to be involved in the process and denies sending any message. To prevent the situations like the one mentioned above, we need to guarantee that all messages come from authenticated source and non-repudiation is achieved so that message senders are accountable for their actions.

7. Prevention of replay attacks: Attacker vehicles can overhear the supplier messages and send them again to consumers to interfere and harm the pricing-based resource selection mechanism. This can be avoided by ensuring that the freshness of the message is maintained.

8. Updating and validating reputation: The reputation should be stored and updated by a trusted authority who can validate and send the reputation of the supplier vehicles whenever required.

2.3.5 Related work

Resource selection problem is highly challenging, as there can be many potential participants in an area of interest and can reach hundreds of vehicles in a congested area[6]. Extensive research has been done to determine the set of vehicles who will provide their resources as shown in Table 2.1. Researchers have used a variety of objective functions, as listed below, based on which selection mechanism is carried out.

- Service Discovery Delay: The time gap between sending the service request packet and receiving the acknowledgment packet that service will be provided.
- Service Consuming Delay: The time gap between sending a service request packet till the first data packet of service delivery is received.
- Service Delivery Ratio: The ratio of number of successful service delivery to the number of times the service is requested.
- Task Completion Time: The time taken to complete a task announced by the vehicular cloud consumer V_c by the vehicular cloud suppliers.
- VM migration overhead: The number of times virtual machines are migrated among the vehicular cloud suppliers over a time frame.
- Reward maximization: Maximizing the profit of the service consumer vehicles.

Mershad and Artail proposed CROWN method which was the first one to address resource selection problem in vehicular cloud [32]. RSU acts as directories which store the information about the supplier vehicles known as STAR. All STARs register at the nearby RSU detailing the type of resource they will provide, attributes of the resource, the price it will charge per resource unit and the time they will be available in VANET for resource provisioning. When a consumer vehicle sends a service request, the RSU searches through it directory for STARs actively present within a coverage area satisfying the resource requirement, quality of service and pricing conditions. The performance evaluation of CROWN framework is done by using service discovery delay and ratio. The main demerit of this method is that STARs have to predetermine the timing it will be present in the network, type of service it will provide and the pricing of resources at least before a week during registration which is highly unrealistic considering that these details are very dynamic in nature.

Arkian et al. mention that long-term pooling of resources is impossible in vehicle cloud which is an important factor that distinguishes it from the conventional cloud [38]. They have formed the vehicular cloud by the clustering mechanism called COHORT and the cluster head which is the controller is selected by using fuzzy logic. The average speed, neighborhood degree, RSU communication link and quality is considered while selecting

Research Work	Objective	Method	Pricing	Service type	Cloud mobility	Reputation	Simulation
Mershad and Artail [32] 2013	Minimising service delay	Comparison based resource selection	Yes	Yes	Mobile	No	SUMO and NS2
Li et al. [37] 2014	Minimization of task completion time	Location based resource selection	No	Yes	Mobile	No	Eclipse Java
Arkian et al. [38] 2015	Minimising service delay	Cluster head by fuzzy logic and helper by MDP	No	Yes	Mobile	No	OMNet++ and SUMO and Veins
Zheng et al. [23] 2015	Determine optimal number of resources required for reward maximization of Vehicular cloud system	SMDP	Yes	No	Stationary	No	MATLAB
Lagraa et al.[33] 2015	Minimising service delay	Comparison based resource selection	Yes	Yes	Mobile	No	OMNet++ and SimuLTE
Sibaï et al. [39] 2015	Maximize service delivery ratio	Comparison based on communication time required	No	Yes	Mobile and Stationary	No	OMNet++ SUMO and Veins
Meneguette et al. [40] 2016	Maximizing service availability	Comparison based resource selection	No	Yes	Mobile	No	OMNet++ and SUMO and Veins
Salahuddin et al. [41] 2016	Minimising VM migration overhead	MDP	No	Yes	Mobile	No	MATLAB
Kong et al. [34] 2016	Optimal task division between supplier vehicles to maximize reward of vehicular cloud system	Stackelberg equilibrium	Yes	No	Mobile	No	NTU-NXP Smart Mobility Testbed
Tamani et al. [42] 2017	Reducing service delay by maximizing link stability	Distance and quality of service comparison based resource selection	Yes	Yes	Mobile	No	OMNet++ and SUMO

Table 2.1: Resource selection approaches in Vehicular Cloud

the cluster head. The cluster head selects the helper or follower vehicles by modeling the problem as a Markov Decision Process (MDP) and solving it by Q-learning algorithm. Average speed of vehicles, bandwidth and total resources present is taken into account while determining the follower vehicles. This mechanism of resource selection is compared with CROWN and the results indicate lower service discovery and consuming delay. They do not consider the pricing of resources and reputation of the vehicles in the selection mechanism. Also, both the cluster head and the follower vehicles are supplier vehicles, which give

resources to the remote user and as elaborated previously, situations where remote users are required are either improbable or uneconomic.

Li et al. proposes a computation offloading mechanism to rent the resources of nearby supplier vehicles [37]. A query packet sent by the consumer vehicle containing the resource requirement is flooded throughout the network. The interested supplier vehicles reply with a confirmation of resource availability mentioning their location, relative speed and quality parameters like computation and communication overhead, latency and hop count. The consumer vehicle determines the longest communication time with each interested supplier vehicle based on their current location and relative velocity. Finally, it calculates the number of tasks that can be offloaded to each supplier vehicle as the amount of task it can perform in unit time multiplied by the longest communication time. It uses a multi-attribute selection mechanism for resource selection based on the number of offloaded tasks, longest communication time, computation and communication overhead. Here the evaluation is done on the basis of the task completion time. The main demerit that lies in the method is that the pricing of resources and the reputation of the supplier vehicles is not considered.

Brik et al. use Long Term Evolution - Advanced (LTE-A) which is a well known mobile standard for vehicular communication [33]. Similar to CROWN each supplier vehicle registers at the Mobile Management Entity (MME) acting as the Trusted Authority mentioning its common attributes like service cost and availability time and it's specific attributes like storage and computation capacity. When a consumer vehicle requires a resource, it sends a request to the MME mentioning the maximum storage or computation requirements, duration of service required and cost of service. MME searches through it's directory and sends a response to consumer vehicle containing the details of all supplier vehicles satisfying the conditions. Finally, the consumer vehicle selects the appropriate supplier based on its requirements like minimum service cost or maximum storage capacity. They evaluate the performance of the method by minimizing the service discovery delay and maximizing service delivery ratio. The major demerit of this system is same as CROWN where the supplier vehicles have to do the registration before where they have to mention at which time they shall be connected to the network making the system unrealistic.

Sibaï et al. proposes that the consumer vehicle is the controller who sends service request consisting of service requirements, current and future location, relative speed and service duration in a multi-hop fashion [39]. On receiving a similar reply from interested supplier vehicles, they use spatio-temporal similarity analysis to calculate the maximum communication time between the consumer and each supplier vehicle. To select the winner supplier vehicle, they maximize communication time, computation or bandwidth provided or combination of all as per the requirement of consumer vehicle. The performance evaluation is done on the basis of the service delivery ratio. The disadvantages are that pricing of resources is not considered and trust assurance on supplier vehicles to get rid of the malicious vehicles is not taken into account.

Menguette et al. propose a peer to peer protocol called SMART based on Gnutella for solving resource selection problem in the vehicular cloud [40]. They determine the supplier vehicles on the basis of their distance from consumer vehicle by using control node and gateway node. The control node is the vehicle farthest from the consumer vehicle in the coverage area traveling in the same direction while the gateway nodes are all eligible vehicles between the consumer vehicle and control node. The consumer vehicle sends service request to each gateway node on the basis of their distance and relative velocity and if it is confirmed, the service is initiated. Else each control node determines it's gateway nodes and subsequent 1-hop control node and searches for resources. This process continues till the service is delivered to the consumer vehicle. The evaluation of this protocol is done in terms of service delivery ratio. Then they propose a scheduling protocol for vehicular cloud called CARESS based on SMART [43]. The drawbacks of this protocol are that pricing of resources and trust assurance of supplier vehicles is not taken into consideration.
Kong et al. try to solve the resource selection problem by the game-theory approach [34]. When a request arrives at the leader vehicle, it hires the follower supplier vehicles in such a manner which will maximize its own utility. The utility of the leader vehicle is defined in terms of profit from task accomplishment and the reward it will provide to each follower vehicle for executing the task. Each supplier vehicle determine the optimal task it should accomplish by using Nash equilibrium strategy by maximizing its utility in terms of cost of resources it provides and the reward received. The leader chooses the supplier vehicles by Stackelberg equilibrium. They evaluate the performance of this protocol on the basis of the utility maximization of consumer and supplier nodes. However, they do not consider the quality of service parameters and use the concept of leader and follower vehicle to provide resources to remote users, which as explained before, form situations which are either improbable or uneconomic.

Minimization of service discovery delay and consuming delay have been the main concern for the majority of the mentioned research works. From this section it is evident that resource selection problem should take into account:

1. Pricing of the resources which inturn depends on the market demand.
2. Quality of service provided by the supplier nodes.
3. The reputation of the supplier nodes
4. Satisfying the security requirements like authentication, non-repudiation and confidentiality while satisfying privacy preservation.

None of the research work take all the above factors into account while solving the resource selection problem which we aim to consider while designing our objective function.

2.4 Modeling the utility of vehicular cloud nodes

In this research work, we aim to resource the resource selection problem based on pricing of resources. We consider a generalized Mobile Vehicular Cloud scenario where the there is only one consumer node V_c and n interested supplier nodes. A vehicular cloud supplier is denoted by V_{sj} where $V_{sj} \in S = \{V_{s1}, V_{s2}, ..., V_{sj}, ..., V_{sn}\}$ and S is the set of all interested supplier vehicles. A utility function for the consumer vehicle is designed considering the reputation of supplier vehicles, quality of service required and pricing of service, whose maximization give the highest profit to the consumer node and will help in determining the best supplier vehicles as per consumer requirement. Also, another utility function for the supplier vehicle is designed which takes into account the market demand and cost of the quality of resources provided. This utility function will help the supplier vehicle to determine the optimal price and the quality of service it should provide so that it's profit is maximized without decreasing its chance of winning.

For defining the utility functions of vehicular cloud consumer node and vehicular cloud supplier node, the following assumptions are taken into consideration:

1. Both the vehicular consumer node V_c and vehicular supplier node V_{sj} are rational and non-cooperative with their ulterior motive being profit(which is termed as utility in this case) maximization.

2. The utility of vehicular consumer node V_c increases with the following quality parameters:

   (a) Increase in the number of CPU cycles. Let q_1 denote the number of CPU cycles.

   (b) Increase in throughput. Let q_2 denote the throughput provided in a proper unit as per requirement.

   (c) Decrease in latency. Let q_3 denote the negation of latency in a proper unit as per requirement.

   (d) Decrease in error rate. Let q_4 denote the negation of error rate percentage.

   (e) Decrease in relative velocity. Let q_5 denote the negation of relative velocity in a proper unit as per requirement.

3. The quality parameters $q_1 - q_5$ are independent of one another.

4. The preferences for the quality parameters are opposed for consumer and supplier nodes. This means that cost of providing resource units by the vehicular supplier nodes V_{sj} increases with increase in quality parameters.

5. The cost of providing service as per requirement by the supplier vehicle does not depend on the reputation of the supplier vehicle.

6. Every supplier vehicle V_{sj} is associated with a cost parameter θ_j, which is the private knowledge of the vehicle.

7. As the quality values increase by a unit, the cost of providing that service increases by a constant value for the supplier vehicle throughout it's quality range.

8. The consumer vehicle has knowledge about how much he prefers each quality parameter and values the reputation of the supplier vehicle.

9. The consumer vehicle V_c already has knowledge of N which is the number of resources it requires.

Due to independence of the quality parameters$\{q_{1j}, q_{2j}..., q_{5j}\}$ as provided by V_{sj}, cost of providing services by a supplier vehicle V_{sj} can be characterized as a weighted additive function. It can safely be concluded that impact of an increase in quality on the cost of providing the service is linearly proportional to private cost value θ_j of the supplier vehicle V_{sj} for all quality parameters. Hence, cost of providing service can be modeled as a cost function C_{sj} where

$$C_{sj}(q_{1j}, ..., q_{5j}, \theta_j) = \theta_j . \left(\sum_{i=1}^{5} b_i . q_{ij} \right) \tag{2.1}$$

The proportion coefficient b_i is assumed to be same for all supplier vehicles for certain quality. With a unit increase in quality parameter q_{ij} provided by the supplier vehicle V_{sj}, the cost of providing that service increases by a constant value $b_i.\theta_j$ for the supplier vehicle throughout its quality range. Let p_j be the price that the supplier vehicle V_{sj} receives on providing its resources.

Definition 2.3. The utility function U_{sj} of the supplier vehicle V_{sj} is defined as the difference of price p_j it receives and cost of service it provides as represented by the cost function and C_{sj}. It can be mathematically expressed as:

$$U_{sj}(p_j, q_{1j}, ..., q_{5j}, \theta_j) = p_j - \theta_j . \left(\sum_{i=1}^{5} b_i . q_{ij} \right) \tag{2.2}$$

Additionally the following assumptions about the vehicular consumer node V_c can be taken into consideration:

1. The consumer vehicle has no knowledge about the private cost value θ_j of each supplying vehicle V_{sj}. It only has information about the distribution of θ_j.

2. Private cost value θ_j of each supplying vehicle V_{sj} is independently and identically distributed between $[\underline{\theta}, \tilde{\theta}]$ with $0 < \underline{\theta} < \tilde{\theta} < \infty$. It has distribution function F and density function f.

3. The utility of the vehicular consumer node increases with the reputation Rep_j of the supplier vehicle V_{sj} since the increase of reputation marks the increase in confidence on V_{sj} about providing a good quality of service from the past experience.

4. The value of reputation Rep_j for the consumer vehicle V_c and the quality of service it receives are independent of one another.

5. The utility of consumer vehicles on increase in quality parameters increases and slowly becomes saturated. This is assumed considering the law of diminishing marginal utility [44]. This law of economics states that if a consumer person increases consumption of a product while keeping consumption of other products constant, there is a decline in the marginal utility that the consumer derives from consuming each additional unit of that product. Marginal utility is derived as the change in utility as an additional unit of the product is consumed.

Since the reputation and quality parameters are independent, the benefit that a consumer node receives from just one vehicular supplier node V_{sj} can be expressed as a weighted additive valuation function. A utility function is quasilinear if it is linear in one argument and strictly concave for others [45]. From the last assumption, we can conclude that the valuation function of the consumer vehicle can be expressed as a quasilinear function which is linear with respect to the reputation and concave with respect to quality parameters. Hence benefit that a consumer node receives from just one vehicular supplier node V_{sj} can be modeled as a valuation function Va_{cj}:

$$Va_{cj}(q_{1j}, ..., q_{5j}, Rep_j) = \left(\sum_{i=1}^{5} D_i . \sqrt{q_{ij}} \right) + \alpha . Rep_j \tag{2.3}$$

The weight Di which represents the measure by which the consumer node values the quality parameter q_i. The benefit that the consumer vehicle derives per unit increase in q_i from supplier vehicle V_{sj} is $D_i . \sqrt{q_{ij}}$. For example, if a consumer does not require the computing resources from the supplier vehicle, it can put D_1 which refers to the number of CPU cycles as 0.

The utility of consumer vehicle V_c from a supplier vehicle V_{sj} is the difference of the valuation it derives from V_{sj} and the price p_j it pays. Suppose the vehicular consumer node selects N winners who will provide their resources, it's overall utility is the summation of the individual utility it receives from each selected supplier vehicle V_{sj}

Definition 2.4. The utility function U_c of the supplier vehicle V_c is the summation of all individual utilities gained from each selected supplier vehicle which is the difference of service valuation it receives and the payment it provides to that selected supplier vehicle. It can be mathematically expressed as:

$$U_c(N, p, q_1, ..., q_5, \alpha, Rep_j) = \sum_{j=1}^{N} \left(\left(\sum_{i=1}^{5} D_i . \sqrt{q_{ij}} \right) + \alpha . Rep_j - p_j \right) \tag{2.4}$$

Initially, each vehicular supplier node V_{sj} can decide the price so as to maximize it's utility U_{sj} keeping in consideration that it has to be a winner. Then the consumer node V_c will determine the selected vehicles based on maximization of U_c. Hence the resource selection and pricing problem in the vehicular cloud can be modeled as a utility maximization problem which is described next.

2.4.1 Pricing based resource selection as a utility maximization problem

Taking into account the assumptions made previously, the supplier vehicle who has knowledge about its cost parameter is confronted with two major challenges, namely determining the quality parameters it is going to provide and the ideal price it should demand for each service request while keeping in consideration that high pricing might prevent it from being selected as winners to supply resources. The problem of determining the optimal price p_j^* can be modeled as maximization of vehicular supplier node V_{sj}'s utility function U_{sj}:

$$[p_j^*, q_{ij}^*] = \underset{p_j, q_{ij}}{\operatorname{argmax}}(U_{sj}(p_j, q_{1j}, q_{2j}..., q_{5j}, \theta_j)) \tag{2.5}$$

After knowing the ideal price p_j^* as done by all the supplier nodes, the consumer vehicle V_c will select those nodes from which he will obtain the maximum utility. Let the set W_c denotes the set of N winner supplier vehicles selected by the consumer vehicle V_c for resource provisioning. The resource selection problem which is the determination of set W_c can be modeled as the maximization of vehicular consumer V_c's utility function U_c:

$$W_c = \underset{j}{\operatorname{argmax}}(U_c(N, p, q_1, ..., q_5, \alpha, Rep_j)) \tag{2.6}$$

2.5 Summary

This chapter gives a detailed analysis of the resource selection and pricing problem in the vehicular cloud. Initially, we describe the vehicular cloud architecture and then sub-divide it on the basis of vehicular mobility and the service providers. Then the importance of the resource selection problem in the vehicular cloud is discussed and is followed by the problem definition. The dependence of resource selection on pricing, quality of service provided and reputation of vehicles is elaborated. The challenges associated with the pricing of resources in the vehicular cloud like market demand and quality of service is also discussed. Also, the security challenges that need to resolved while addressing the pricing-based resource selection problem are described. Related research works on resource selection is presented. The utility of consumer and supplier vehicles is then designed and the pricing-based resource selection problem is modeled as a utility maximization problem.

Chapter 3

Second-Score Sealed Bid Auction for Pricing-Based Resource Selection

3.1 Introduction

Vehicular cloud computing is an innovative concept which aggregates the idle vehicular resources to provide low cost, location based, real time service. It has potential applications including dynamic traffic management, traffic light coordination and infotainment services like multimedia and data transfer. As elaborated in the previous chapter, resource-selection in vehicular cloud is a crucial problem which needs to be addressed for fully exploiting this innovative concept. The problem is highly challenging due to it's dependence on the pricing of resources, trust assurance of suppliers, quality of service provision and the market-demand.

Micro-economic models like auctions are proposed as solution mechanisms for the market structure similar to our system with one consumer and limited number of eligible suppliers. Reverse auction mechanisms have been presented for resource selection and pricing determination problem in cloud computing environments [46], [47]. Second-score sealed bid auction is a type of reverse auction where the auction participants bid their actual valuation and receive the payment as per the second highest bid. This mechanism instigates the participants to reveal their actual preference irrespective of their selfish nature. Therefore, use of this mechanism is highly encouraged for resource-selection, and solution mechanisms have used this concept in cloud computing [48]. In many cases, the consumer vehicles may require to rent the entire resource of vehicular suppliers. In this chapter, we relax the quality of service requirements and propose a second-score sealed bid auction mechanism to address the pricing-based resource selection problem.

The organization of this chapter is as follows: Section 3.2 describes the system model of vehicular cloud along with the utility, cost and valuation functions of the consumer and supplier vehicles where no quality of service parameters are taken into account. In Section 3.3, three standard pricing-based resource selection methodologies, namely Fixed-Price Distance Based Selection ($fixed\_dist$), Random-Pricing Distance Based Selection ($rand\_dist$) and Minimum Random-Pricing Selection ($rand\_low$) were

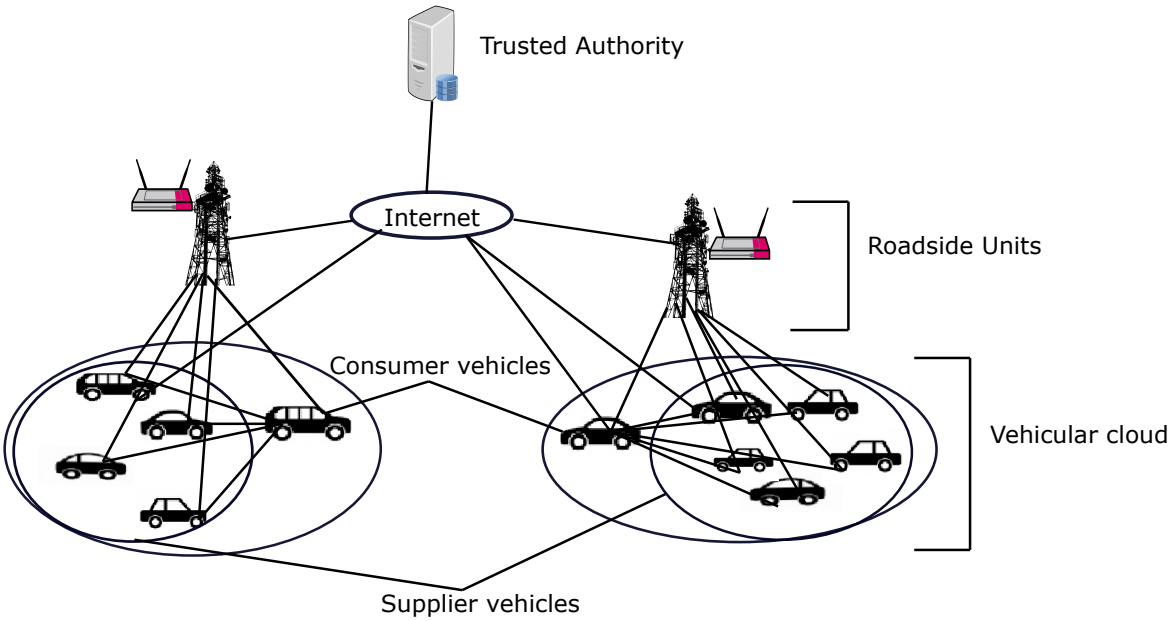

Figure 3.1: A typical Vehicular Cloud scenario with Trusted Authority

elaborated to be used in future for comparison purpose. The second-score sealed bid auction ($2nd\_auc$) mechanism is proposed in Section 3.4 which aims to solve the resource selection problem by utility maximization. Thorough experimentation and analysis of the $2nd\_auc$ with respect to the standard protocols is done in Section 3.5. Finally the chapter is summarized in Section 3.6.

3.2 System Model

The vehicular cloud architecture, as depicted in Figure 3.1, comprises of supplier vehicles acting as cloud service providers. The vehicular cloud consumers can be in the form of vehicles, roadside units or some external user accessing the services via the Internet through vehicles or roadside units. In this work, we represent the vehicular cloud consumers in form of consumer vehicles. V2V communication enables the vehicles to connect with each other while V2I communications link vehicles with roadside units.

The primary concern of the roadside unit is to provide Internet access to all the vehicles in its range although some vehicles might already have Internet access through cellular networks. Hence, in this work we assume that all the vehicles are connected to the Trusted Authority (TA) through the Internet. TA is responsible for the initial registration of the vehicles and maintenance of the identification details like identity, license plate number, reputation, balance and other records of the registered vehicles. It also updates the balances of both consumer and supplier vehicles after the successful completion of a service provision session by transferring the negotiated monetary value from consumer to supplier account. The reputation of supplier vehicles is also incremented and validated whenever necessary by the TA.

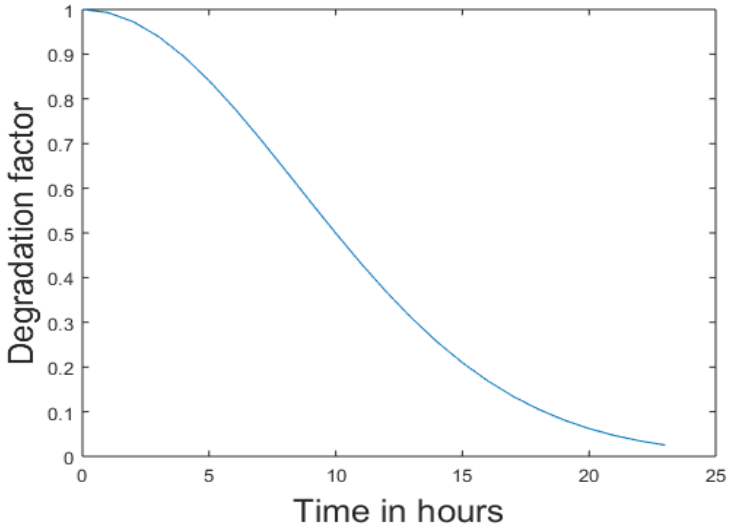

Figure 3.2: Degradation of reputation with time

We consider one consumer vehicle V_c and n interested supplier vehicles for the resource provisioning phase. Similar to Section 2.5 of previous chapter, a vehicular cloud supplier is represented as V_{sj} where $V_{sj} \in S = \{V_{s1}, V_{s2}, ..., V_{sj}, ..., V_{sn}\}$ and S is the set of all interested supplier vehicles. Both consumer and supplier vehicles are assumed to be rationale and non-cooperative with their major objective to maximize their utility. As justified in the previous chapter, vehicles are autonomous bodies and hence trusting a supplier vehicle to provide the resources as per the agreement is a challenge. So reputation based on the previous performance of the vehicle was proposed to be a parameter for evaluating trustworthiness. After a successful task accomplishment, the consumer vehicle can give a feedback about the service quality provided by the supplier vehicle. Service provisioning in vehicular cloud is an one time event. Also the interaction among vehicular consumers V_c and vehicular suppliers V_{sj} lasts for a brief time. Therefore, the reputation provided for one successful service provisioning event reflects the trustworthiness of the supplier vehicle V_{sj} for a short interval. So the reputation value should degrade gradually and get completely exhausted in a day. The current reputation value Rep_j from the previous reputation value Rep_{oldj} can be computed by TA at any time instant when demanded as:

$$Rep_j = R_{oldj}.e^{\left(\frac{\Delta T}{12}\right)^2} \tag{3.1}$$

Here ΔT = current time - time of determination of R_{oldj}. It can be seen from Figure 3.2 that reputation decreases at a slower rate initially since it has high weightage due to freshness. The later part of the curve , due to the staleness of the reputation value, degrades by a steeper rate till it constantly disappears.

In this chapter, we relax the quality of service parameters and assume that the whole resource unit of the supplier vehicle is given in rent. Hence, the cost (C_{sj}) and utility

function (U_{sj}) of supplier vehicle V_{sj} is a slight variation to the ones proposed in Section 2.5. Additionally the valuation function Va_{cj} of the vehicular consumer V_c from supplier vehicle V_{sj} and overall utility of the consumer vehicle U_c have to be modified. All the resource units are assumed to be homogeneous in sense that the utility derived from it is of constant value K to a consumer vehicle irrespective of which supplier vehicle provides it. But the cost of providing the resource unit varies from one supplier vehicle to another. Let, θ_j be the cost of the whole resource unit of V_{sj}. Hence, the cost function C_{sj} of V_{sj} is expressed as:

$$C_{sj}(\theta_j) = \theta_j \tag{3.2}$$

The utility U_{sj} of the supplier vehicle V_{sj} from one successful service provisioning event is the difference of the payment p_j it receives from consumer vehicle V_c and it's cost for providing the entire resource unit. Hence the utility function U_{sj} can be expressed as:

$$U_{sj}(p_j, \theta_j) = p_j - \theta_j \tag{3.3}$$

We assume that the service provisioning always occurs for a fixed time interval as decided by the TA for the whole system and it remains constant irrespective of number and requirement of consumer and supplier vehicles. The utility of the consumer is increased by a constant K on using the whole resource for all supplier vehicles. The valuation of resource provisioning by a supplier vehicle V_{sj} to the consumer vehicle V_c is expressed as:

$$Va_{cj}(Rep_j) = K + \alpha.Rep_j \tag{3.4}$$

The overall utility to the consumer vehicle V_c from a resource provisioning event with N winners is:

$$U_c(p, Rep) = \sum_{j=1}^{N} (K + \alpha.Rep_j - p_j) \tag{3.5}$$

For this chapter, the first part of our research problem is to determine the optimal pricing of the whole resource unit by each supplier vehicle.

$$[p_j^*] = \underset{p_j}{\operatorname{argmax}}(U_{sj}(p_j, \theta_j)) \tag{3.6}$$

The second part of the problem is same as discussed in Section 2.5.1, which is the determination of set W_c of N winner suppliers and is expressed as:

$$W_c = \underset{j}{\operatorname{argmax}}(U_c(N, p, \alpha, Rep_j)) \tag{3.7}$$

3.3 Standard Pricing-Based Selection Protocols

Three standard methodologies namely Fixed-Price Distance Based Selection ($fixed\_dist$), Random-Pricing Distance Based Selection ($rand\_dist$) and Minimum Random-Pricing Selection ($rand\_low$) are discussed below. They do not find the optimal price or set of winners which maximizes the utility function of supplier and consumer vehicles respectively. Only the proposed second-score sealed bid auction ($2nd\_auc$) protocol aims to solve both part of the research problem in equation 3.6 and 3.7.

3.3.1 Fixed-Price Distance Based Selection Protocol

Fixed-Price Distance Based Selection Protocol ($fixed\_dist$) is the most basic resource selection mechanism which relies on the fact that consumer and supplier vehicles with low inter-vehicular distance stay in each other's range for a longer period of time. Hence the service provisioning time will be high and there is less chance of connection error. In this protocol, the resource units of all supplier vehicles is same and equal to a fixed price FP which is continuously determined by the TA. Here we assume that all participating vehicles in the temporary cloud, namely the consumer vehicle and the set S of supplier vehicles are well aware of the value of FP at all time instant. The winner determination in this protocol is done by minimizing the distance of the supplier vehicles from the consumer vehicle. The $fixed\_dist$ protocol is illustrated by Figure 3.3. A detailed description of the protocol is given below:

1. $V_c \rightarrow * : M_1^1$. The consumer vehicle broadcasts the message M_1^1 which is a service request message. It consists of the identity of consumer vehicle (id_{Vc}), the protocol name $fixed\_dist$, the position of the consumer vehicle $\{posx_{Vc}, posy_{Vc}\}$, the current direction dir_{Vc} and speed spd_{Vc} of the consumer vehicle V_c. Hence $M_1^1 =< id_{Vc}, Serv\_Req, fixed\_dist, posx_{Vc}, posy_{Vc}, dir_{Vc}, spd_{Vc} >$

2. $V_{sj} \rightarrow V_c : M_{2sj}^1$ All the interested supplier vehicles whose resource units are available, send service availability message to the consumer vehicle. M_{2sj}^1 consists of the identity id_{Vsj} of the supplier vehicle V_{sj}, the position of the consumer vehicle $\{posx_{Vsj}, posy_{Vsj}\}$ and the current direction dir_{Vc}. So $M_{2sj}^1 =< id_{Vsj}, Serv\_Avl, fixed\_dist, posx_{Vsj}, posy_{Vsj}, dir_{Vsj} >$

3. V_c: fixed_sel$(n, N, msg_lst, posx_{Vc}, posy_{Vc}, dir_{Vc}) \rightarrow win_list$ On receiving the service availability message list $msg\_list =< M_{2s1}^1, M_{2s2}^1, ..., M_{2sj}^1 ..., M_{2sn}^1 >$ from all the supplier vehicles, the consumer vehicle determines the winner by using Algorithm 1. It first segregates the supplier vehicles traveling in it's direction from the interested supplier list, calculates their mutual distance based on their current positions and sorts them on basis of distance. It then selects the required N suppliers with minimum distance as winner supplier vehicles.

4. $V_c \rightarrow * : M_3^1$ The consumer vehicle broadcasts the winner list consisting of the identity of the selected suppliers for service provisioning. $M_3^1 =< id_{Vc}, win\_list >$

5. $V_c \leftrightarrow V_{sj}$: service_provision. Here the service provisioning phase starts and the winner supplier vehicles rent their whole resource to the consumer vehicle. The consumer trusts the winners to stay in it's range for the stipulated service provisioning time by adjusting their speed to the one send in M_1^1. In case of any speed change by the consumer, a beacon message related to the new speed is sent to the service providing vehicles so that they can modify their speed.

6. $V_c \rightarrow$TA: M_4^1 The consumer vehicles send the list of supplier vehicles who prove to be sincere by providing service to the consumer vehicles for the alloted time. It requests the TA to transfer the fixed price FP to these vehicles. Here $M_4^1 =< id_{Vc}, fixed\_dist, serv\_provlst^1 >$ and $serv\_provlst^1 = \{id_{Vs1}, id_{Vs2}, ..., id_{Vsk}, ..., id_{Vsgd}\}$ where V_{sk} and gd are the vehicles and the number of vehicles who provided complete service.

7. TA:transfer_payment: This is the last phase where the TA pays the supplier vehicles in the $serv\_provlst^1$ by reducing the $gd.FP$ amount from the balance of the consumer vehicle.

There are two drawbacks of this protocol. Firstly, the determination of the fixed price FP is a herculean task and overall market condition consisting of all consumers and suppliers has to be considered. Deriving a common fixed price for all market demands with constant updation due to it's dynamic nature is not quite practical. Secondly, the reputation of the supplier vehicles, portraying their trustworthiness is not considered. It assumes all winners will adjusts their speed to stay in it's range to provide service. When a consumer vehicle selects a selfish vehicle which fails to provide resources till the end of the stipulated time, it doesn't receive satisfactory service leading to a decrease in it's utility. Although the selfish vehicles don't receive payment, they can bid the next time subsequently becoming winners and causing harm to other consumer vehicles. This problem is solved by using reputation as a parameter to segregate the selfish ones from the sincere ones.

3.3.2 Random-Pricing Distance Based Selection Protocol

In the Random-Pricing Distance Based Selection protocol ($rand\_dist$), the resource prices are chosen by the supplier vehicles without using any proper pricing mechanism. Similar to the previous $fixed\_dist$ protocol, the selection of winner supplier vehicles is done by minimizing distance from the consumer vehicle. Therefore it selects winners based on the reason that vehicles with low inter-vehicular distance can provide smooth service with less error rate because of remaining in range for longer time. The random-pricing distance based selection protocol as illustrated in Figure 3.4 is described below:

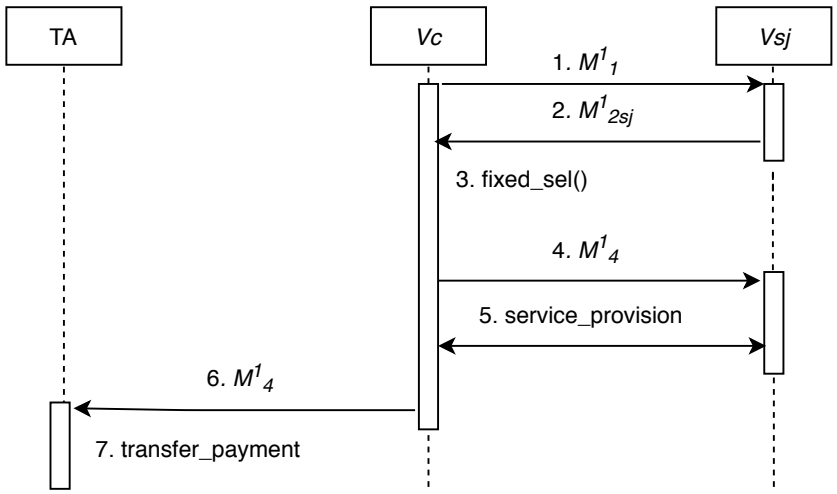

Figure 3.3: Fixed-Price Distance Based Selection Protocol

Algorithm 1 fixed_sel$(n, N, msg_lst, posx_{Vc}, posy_{Vc}, dir_{Vc})$

Input: $n, N, msg\_lst, posx_{Vc}, posy_{Vc}, dir_{Vc}$

Output: win_list containing identity of winners sorted on basis of distance

1: **for** $j = 1$ to n **do**
2: $M^1_{2sj} \leftarrow msg\_list(j)$
3: **if** $dir_{Vc} = M^1_{2sj} < dir_{Vsj} >$ **then**
4: $dist_{sj} \leftarrow \sqrt{(posx_{Vc} - M^1_{2sj} < posx_{Vsj} >)^2 + (posy_{Vc} - M^1_{2sj} < posy_{Vsj} >)^2)}$
5: M^1_{2sj}.**append**$(dist_{sj})$
6: **else**
7: msg_lst.**remove**(M^1_{2sj})
8: **end if**
9: **end for**
10: **Sort** msg_lst in increasing order of $dist_{sj}$
11: $win\_list \leftarrow$ **NULL**
12: **for** $j = 1$ to N **do**
13: win_list.**append**$(msg\_lst(j) < id_{Vsj} >)$
14: **end for**

1. $V_c \rightarrow * : M^2_1$ Similar to the first step of $fixed\_dist$ protocol, the consumer vehicle broadcasts a service availability message consisting of the identity of consumer vehicle, the protocol name rnd_dist, the position of the consumer vehicle, the current direction dir_{Vc} and speed spd_{Vc} of the consumer vehicle V_c. $M^2_1 =< id_{Vc}, Serv\_Req, rnd\_dist, posx_{Vc}, posy_{Vc}, dir_{Vc}, spd_{Vc} >$

2. V_{sj}: rndprice_select() $\rightarrow p_j$: The supplier vehicle V_{sj} determines the price at which it will provide it's resources. Here we assume that the price determination is done in a random basis without using a pricing algorithm considering market demand. The price determination may depend on the cost of resource unit it will provide.

3. $V_{sj} \rightarrow V_c : M^2_{2sj}$The interested supplier vehicles send service availability message

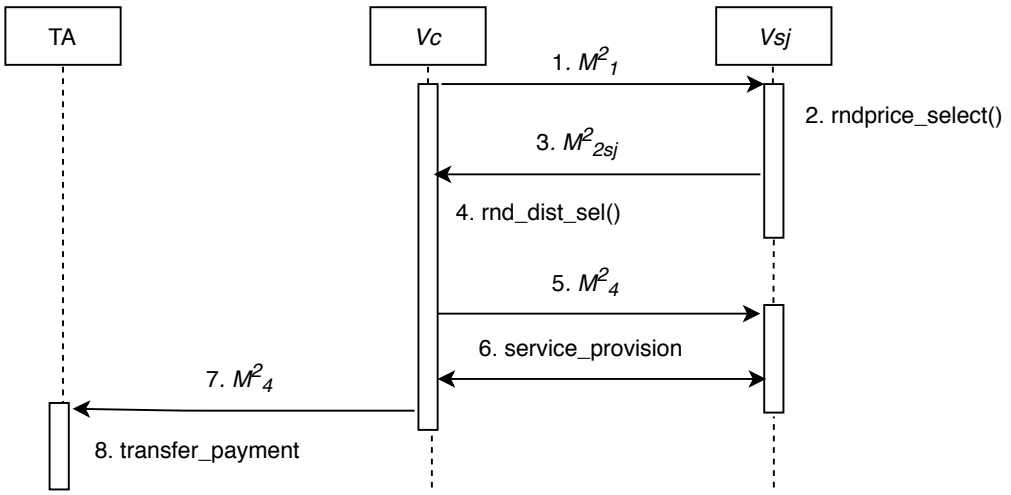

Figure 3.4: Random-Pricing Distance Based Selection Protocol

to the consumer vehicle. M^2_{2sj} consisting of their identity, their current position, their current direction and the price determined in the previous step p_j.So $M^2_{2sj} =< id_{Vsj}, Serv\_Avl, rnd\_dist, posx_{Vsj}, posy_{Vsj}, dir_{Vsj}, p_j >$

4. V_c: rnd_dist_sel$(n, N, msg_lst, posx_{Vc}, posy_{Vc}, dir_{Vc}) \rightarrow win_list$ When the service availability message list $msg\_list =< M^2_{2s1}, M^2_{2s2}, ..., M^2_{2sj}..., M^2_{2sn} >$ is received by the consumer from all interested suppliers, it determines the winner by using Algorithm 2. Similar to the $fixed\_dist$ protocol, it initially shortlist the supplier vehicles moving in it's direction, calculates their mutual distance based on their current positions and determines inter-vehicular distance. Subsequently it determines the winner list by sorting them on basis of distance and selecting top N suppliers.

5. $V_c \rightarrow * : M^2_3$ $M^2_3 =< id_{Vc}, win\_list >$ The consumer vehicle notifies the winner supplier vehicles by broadcasting a winner list consisting of the identity of the selected suppliers and price declared by them for service provision.

6. $V_c \leftrightarrow V_{sj}$: service_provision. In this step the service provisioning starts and the consumer vehicles can use the resources of the winner supplier vehicles. Similar to $fixed\_dist$, the consumer vehicles trust the winner vehicles to stay in their range by adjusting their speed.

7. $V_c \rightarrow$TA: M^2_4:where $M^2_4 =< id_{Vc}, rnd\_dist, serv\_provlst^2 >$ and $serv\_provlst^2 = \{(id_{Vs1}, p_{s1}), (id_{Vs2}, p_{s2}), ..., (id_{Vsk}, p_{sk}), ..., (id_{Vsgd}, p_{sgd})\}$ where V_{sk} and gd are the vehicles and the number of vehicles who provided complete service.

8. TA:transfer_payment. TA transfers the negotiated amount in the $serv\_provlst^2$ from the consumer vehicle to each winner supplier vehicle.

Algorithm 2 rnd_dist_sel($n, N, msg\_lst, posx_{Vc}, posy_{Vc}, dir_{Vc}$)

Input: $n, N, msg\_lst, posx_{Vc}, posy_{Vc}, dir_{Vc}$

Output: win_list containing identity and price for winners sorted on basis of distance

1: **for** $j = 1$ to n **do**
2: $M^2_{2sj} \leftarrow msg\_list(j)$
3: **if** $dir_{Vc} = M^2_{2sj} < dir_{Vsj} >$ **then**
4: $dist_{sj} \leftarrow \sqrt{(posx_{Vc} - M^2_{2sj} < posx_{Vsj} >)^2 + (posy_{Vc} - M^2_{2sj} < posy_{Vsj} >)^2)}$
5: M^2_{2sj}.**append**$(dist_{sj})$
6: **else**
7: msg_lst.**remove**(M^2_{2sj})
8: **end if**
9: **end for**
10: **Sort** msg_lst in increasing order of $dist_{sj}$
11: $win\_list \leftarrow$ **NULL**
12: **for** $j = 1$ to N **do**
13: win_list.**append**$(msg\_lst(j) < id_{Vsj}, p_j >)$
14: **end for**

This protocol also has two major disadvantages. Since the winners are selected on the basis of distance, the supplier vehicles vehicles can choose high pricing values which does not affect their probability of winning. This will lead to a decrease in consumer utility. Similar to the $fixed\_dist$ protocol, it doesn't take into account the trustworthiness of the supplier vehicles by considering their reputation.

3.3.3 Minimum Random-Pricing Selection Protocol

Similar to the $rand\_dist$ protocol, the resource pricing is done by the supplier vehicles without taking into account any pricing mechanism based on market demand. The supplier vehicles declaring minimum pricing values are selected as the winners. The minimum random-pricing selection protocol as depicted in Figure 3.5 is described below:

1. $V_c \rightarrow * : M^3_1$ Initially, the consumer vehicle broadcasts a service availability message consisting of the identity of consumer vehicle, the protocol name rnd_low, the position of the consumer vehicle, the current direction dir_{Vc} and speed spd_{Vc} of the consumer vehicle V_c. So $M^3_1 =< id_{Vc}, Serv\_Req, rnd\_low, dir_{Vc}, spd_{Vc} >$

2. V_{sj}: rndprice_select() $\rightarrow p_j$: In this step the supplier vehicle V_{sj} determines the service provisioning price in a random basis. Similar to the previous rnd_dist protocol, we assume that the supplier doesn't consider market demand or the cost of resource unit it will provide.

3. $V_{sj} \rightarrow V_c : M^3_{2sj}$ Here the service availability message is sent by the suppliers to the consumer vehicle. M^2_{2sj} consisting of their identity, their current position,

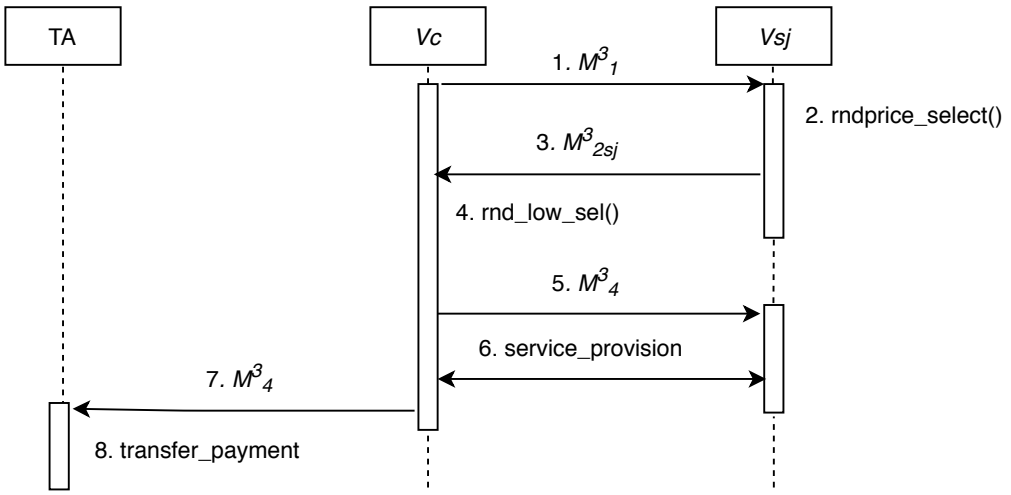

Figure 3.5: Minimum Random-Pricing Selection Protocol

their current direction and the price determined in the previous step p_j.So $M^3_{2sj} =< id_{Vsj}, Serv\_Avl, rnd\_low, dir_{Vsj}, p_j >$

4. V_c: rnd_low_sel$(n, N, msg_lst, dir_{Vc}) \rightarrow win_list$ On receiving the service availability message list, $msg\_list =< M^3_{2s1}, M^3_{2s2}, ..., M^3_{2sj}..., M^3_{2sn} >$, the consumer vehicles initially shortlist the supplier vehicles who are moving in it's directly. It then sorts them in an increasing order of their pricing value and selects the top N winners for service provisioning.

5. $V_c \rightarrow * : M^3_3$ Here the consumer vehicle broadcast the winner list consisting of the identity of the winners and the price they have declared to provide. $M^3_3 =< id_{Vc}, win\_list >$

6. $V_c \leftrightarrow V_{sj}$: service_provision. In this phase the service is provided by the supplier vehicles which are trusted to stay in the range of the consumer vehicles by adjusting their speed.

7. $V_c \rightarrow$TA: M^3_4:where $M^3_4 =< id_{Vc}, rnd\_low, serv\_provlst^2 >$ and $serv\_provlst^2$ is same as in the previous rnd_dist protocol.

8. TA:transfer_payment. The transfer of the negotiated monetary amount is done in a similar way as the rnd_dist protocol.

Since the trustworthiness of the supplier vehicles is not taken into consideration by the use of reputation values, the selfish vehicles are not segregated from the good ones. This indicates that the selfish vehicles can be selected as winner in the subsequent service provisioning sessions leading to a loss of consumer utility. Also the suppliers without having a proper pricing mechanism will declare unusually low pricing of resources to become winner which will often decrease the supplier profit.

Algorithm 3 rnd_low_sel(n, N, msg_lst, dir_{Vc})

Input: n, N, msg_lst, dir_{Vc}

Output: win_list containing identity and price for winners sorted in increasing order of price

1: **for** $j = 1$ to n **do**
2: $M^3_{2sj} \leftarrow msg\_list(j)$
3: **if** $dir_{Vc} \neq M^3_{2sj} < dir_{Vsj} >$ **then**
4: msg_lst.**remove**(M^3_{2sj})
5: **end if**
6: **end for**
7: **Sort** msg_lst in increasing order of p_j
8: $win\_list \leftarrow$ **NULL**
9: **for** $j = 1$ to N **do**
10: win_list.**append**$(msg\_lst(j) < id_{Vsj}, p_j >)$
11: **end for**

3.4 Second Score Auction

In this section, we apply the second score auction to the pricing-based resource selection mechanism. According to a generalized second score auction, all the bidders give their actual valuation of the resource to the auctioneer. The winner is selected by the auctioneer on the basis of a scoring rule and it is provided with a price related to the second highest score.

Considering our system model, the consumer vehicle are substituted as the auctioneer and the supplier vehicles are represented as the participating bidders. The scoring rule as determined by the consumer vehicle is declared as:

$$S_c = \alpha.Rep - p \tag{3.8}$$

The supplier vehicles give their actual valuation in form of the bids. So the price they decide to declare is:

$$p_{sj} = \theta_j \tag{3.9}$$

The consumer vehicle calculates the score of all the bidding supplier vehicles and sorts them in a decreasing order of their score. After selecting the top N vehicles from the list as the winners, it calculates the corresponding price $price_{si}$ provided to the i^{th} winner from the score of the $(i+1)^{th}$ winner by equalizing their score and replacing their bidding price p_{si} with the price $price_{si}$ it will receive. Let S_{si} and S_{si+1} be the score of the i^{th} and the $(i+1)^{th}$ winner respectively.

$$\begin{aligned} & S_{si} = S_{si+1} \\ \Rightarrow\ & \alpha.Rep_{si} - price_{si} = \alpha.Rep_{si+1} - price_{si+1} \\ \Rightarrow\ & price_{si} = price_{si+1} + \alpha(Rep_{si} - Rep_{si+1}) \end{aligned} \tag{3.10}$$

A strategy is dominant if it is always better than any other strategy, for any profile of other players' actions [49]. It can be mathematically defined as:

$$u_i(s_i, s^{'}_{-i}) \geq u_i(s^{'}_i, s^{'}_{-i}) \tag{3.11}$$

where u_i is the utility of the player, s_i is the dominant strategy, $s^{'}_i$ is the alternate strategy and $s^{'}_{-i}$ is the strategy of all other players [50].

Lemma 3.4.1. *Bidding the pricing value as per equation 3.9 is a dominant strategy of the supplier vehicle*

$Proof$: The above lemma means that the dominant strategy of the supplier vehicle is to bid $p_{sj} = \theta_j$ which in turn is bidding a price p_{sj} which is it's actual valuation and makes it's utility in equation 3.3 as 0. We prove this strategy to be dominant by the method of contradiction.

In the first case, we assume that bidding a price $p_{sj} > \theta_j$ gives the supplier a higher utility. On bidding a higher price, the score of the supplier vehicle decreases and hence it's probability of winning decreases. The bidding price p_j does not determine the price $price_j$ it will receive after getting selected as the winner and only depends on the bidding of the next highest scorer. Hence, the utility of the supplier remains same as the case when it bids $p_{sj} = \theta_j$ but the probability of winning decreases. So a contradiction is derived.

In the next case, we assume that bidding a price $p_{sj} < \theta_j$ gives the supplier a higher utility. Since the supplier vehicle is assumed to be rationale and does not want negative utility, a contradiction is derived.

Hence bidding $p_{sj} = \theta_j$ is the dominant strategy of the supplier vehicle V_{sj} in a second score auction. This proves that despite the private information and pure selfish behavior of the supplier vehicles, the second auction mechanism forces them to reveal their actual cost of resources θ_j in form of their dominant strategy. The second-score sealed bid auction as illustrated in Figure 3.6 is described below:

1. $V_c \rightarrow * : M^4_1$ The consumer vehicle broadcasts a service availability message which consists of the protocol name $2nd\_auc$, consumer vehicle, identity, direction, speed and preference weight of the reputation value α. So $M^4_1 =< id_{Vc}, Serv\_Req, 2nd\_auc, \alpha, dir_{Vc}, spd_{Vc} >$

2. $V_{sj} \rightarrow V_c : M^4_{2sj}$ All the interested supplier vehicles send the service availability reply message along with their identity, current direction and private cost value θ_j. Hence $M^4_{2sj} =< id_{Vsj}, Serv\_Avl, 2nd\_auc, dir_{Vsj}, \theta_j >$

3. V_c: dir_check$(n^{'}, msg_lst^{'}, dir_{Vc}) \rightarrow (msg_list, egl_list, n)$ After receiving the service availability message list $msg\_lst^{'} =< M^4_{2s1}, M^4_{2s2}, ..., M^4_{2sj}, ..., M^4_{2sn'} >$ from $n^{'}$ interested suppliers, the consumer vehicle segregates the suppliers moving in it's

direction by using Algorithm 4 to create a new list called egl_list of n eligible supplier vehicles.

4. V_c →TA: M_3^4 The consumer vehicle requests the TA to give the reputation values of the supplier vehicles in egl_list along with it's identity. Here $M_3^4 =< id_{Vc}, Rep\_Req, 2nd\_auc, egl\_list >$

5. TA → V_c : Rep_list The TA replies back to the consumer vehicle giving the reputation of each supplier in the egl_list provided to it in form of $Rep\_list =< (id_{Vs1}, Rep_{Vs1}), (id_{Vs2}, Rep_{Vs2}), ..., (id_{Vsj}, Rep_{Vsj}), ..., (id_{Vsn}, Rep_{Vsn}) > \forall id_{Vsj} \in egl\_list$

6. V_c: second_score_sel$(n, N, \alpha, msg_lst, Rep_list)$ → win_list After getting the reputation values of each eligible supplier node, the consumer vehicle calculates the winner list as per Algorithm 5 and also determines the price that will be provided to each winner after the service provisioning phase.

7. V_c → $*$: M_4^4 The consumer vehicle then broadcasts the winner list consisting the identity of each winner and the price to be provided to them where $M_4^4 =< id_{Vc}, win\_list >$

8. $V_c \leftrightarrow V_{sj}$: service_provision. In this phase the service provisioning occurs between consumer and supplier vehicle and the supplier vehicles adjust their speed according to the consumer vehicles to stay in their range.

9. V_c →TA: M_5^4 The consumer vehicle send to TA the list of supplier vehicles who provided smooth service till the end of stipulated time. Here $M_5^4 =< id_{Vc}, 2nd\_auc, win\_list, serv\_provlst^4 >$
$serv\_provlst^4 = \{(id_{Vs1}, price_{s1}), (id_{Vs2}, price_{s2}), ..., (id_{Vsk}, price_{sk}), ..., (id_{Vsgd}, price_{sgd})\}$
where V_{sk} who provided complete service

10. TA:rep_payment_transfer. After receiving the identity and pricing list of sincere suppliers who provided smooth service, the TA transfers the amount mentioned in the list from consumer vehicle to supplier vehicles. It also updates the reputation value of these suppliers by a constant value RA. For the vehicles in the winner list and not in the service provision list, the reputation is decremented by RA because they don't provide service for the stipulated time.

3.5 Experimentation and Analysis

An extensive experimentation was set up to evaluate the performance of the proposed second-score auction and the results were compared with the standard pricing-based

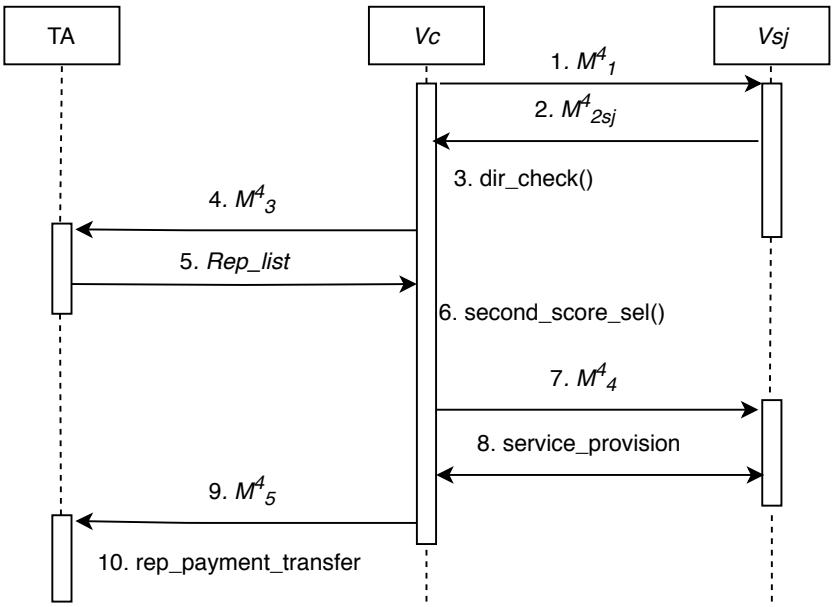

Figure 3.6: Second-Score Sealed Bid Auction for pricing-based resource selection

selection mechanisms. The simulation was conducted using Simulation of Urban MObility (SUMO) platform which is an open-source vehicular network and traffic simulator and tracing the vehicular movements was done with the help of Python programming language [51]. The experimentation was carried out using 10 virtual machines each with 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory using Amazon AWS [52].

We have considered a 15km stretch of NH53 highway in both directions having two lanes each near Paradip Port, India to carry out our experiment Figure 3.7. This was taken using the OpenStreetMap software [53]. The vehicular traffic flow rate, which is the number of vehicles passing through a certain point over unit time, was varied between 1000 vehicles/hour till 6000 vehicles/hour for low and high traffic scenarios respectively. For modeling the traffic flow rate, the following distributions were used: a negative exponential distribution low traffic flow rate, Pearson Type III distribution for intermediate traffic flow rate and normal distribution for high traffic flow rate [54]. The transmission range for vehicular communication is fixed at 400m. The reputation of supplier vehicles is uniformly distributed between 0 and 3. The reputation preference value α of the consumer vehicles was varied between [0,10]. The upper and lower limit of the cost parameter θ_j of the supplier vehicles is fixed at 1 and 100 respectively and is uniformly distributed throughout the range.

The service provision time after the completion of the auction is taken as 60 seconds during which the selected supplier nodes will follow the consumer node while providing their resources. The percentage of the consumers in the simulation scenario is varied between 0.05 till 0.3. Also the maximum number of selected winner vehicles is set at 5. For the highest traffic flow rate with lowest percent of consumers, the maximum number of eligible suppliers can be observed to be 40. Taking into account our objective function maximization, consumer utility per winner is considered as the metric to evaluate the performance of the

Algorithm 4 dir_check($n^{'}, msg\_lst^{'}, dir_{Vc}$)

Input: $n^{'}, msg\_lst^{'}, dir_{Vc}$

Output: msg_list,egl_list and n are message list, identity list and number of eligible vehicles respectively

```
msg_list ← NULL
egl_list ← NULL
n ← 0
for j = 1 to n' do
    M^4_2sj ← msg_lst'
    if dir_Vc = M^4_2sj < dir_Vsj > then
        msg_lst.append(M^4_2sj)
        egl_lst.append(M^4_2sj < id_Vsj >)
        n ← n + 1
    end if
end for
```

second-score auction protocol.

For the Distance-based fixed price selection mechanism ($fixed\_dist$), the fixed price was determined to be the mean of the second-score auction protocol which was 65. For both the random price protocols $rand\_dist$ and $rand\_low$, the price range was determined to be [0,130].

3.5.1 Numerical Analysis

From all the graphs, namely Figure 3.8, 3.9, 3.10, 3.11, it can be seen that $2nd\_auc$ behaves better than $fixed\_dist$, $rand\_dist$ and $rand\_low$. The utility derived from $fixed\_dist$ remains same for all cases of varying number of eligible suppliers, number of winners, percentage of consumers and vehicular flow rate. This is because the price is fixed and only the reputation value is randomly varying giving an overall constant utility when the average is considered. Similarly in case of $rand\_dist$ the utility derived remains same for all cases. This is because the winner selection is done as per distance leading to high pricing by the

Figure 3.7: Cross section of the roadway taken for the experimentation purpose

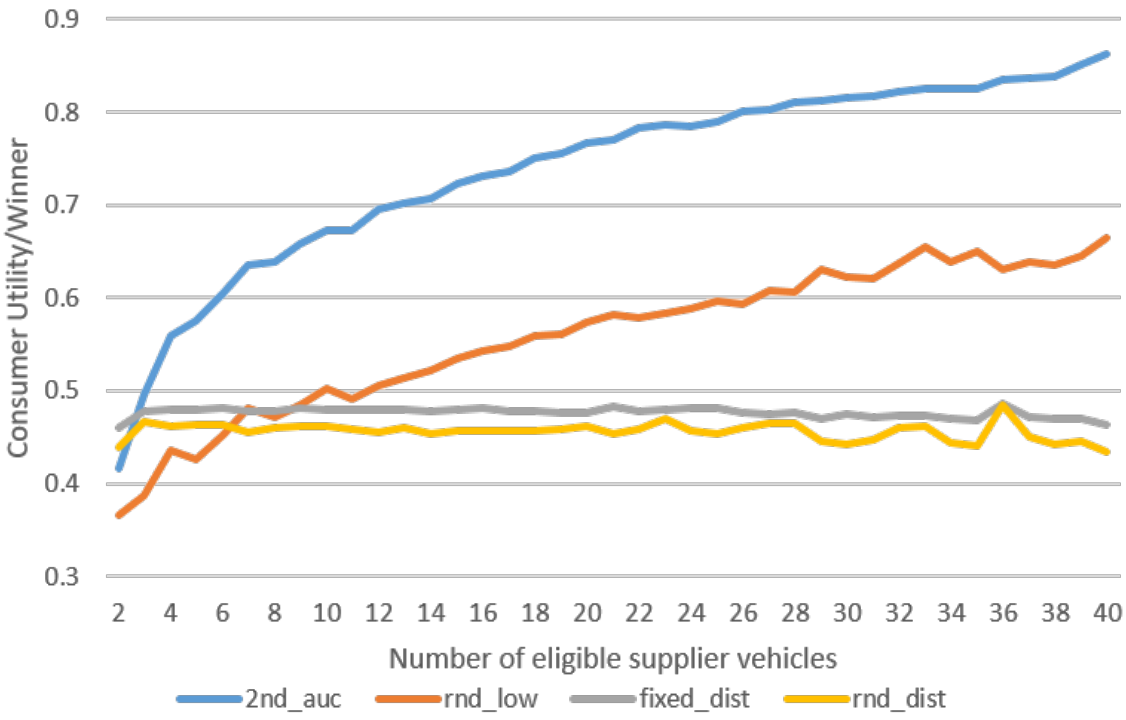

Figure 3.8: Consumer Utility/Winner vs Number of Eligible Suppliers for Second-Score Auction

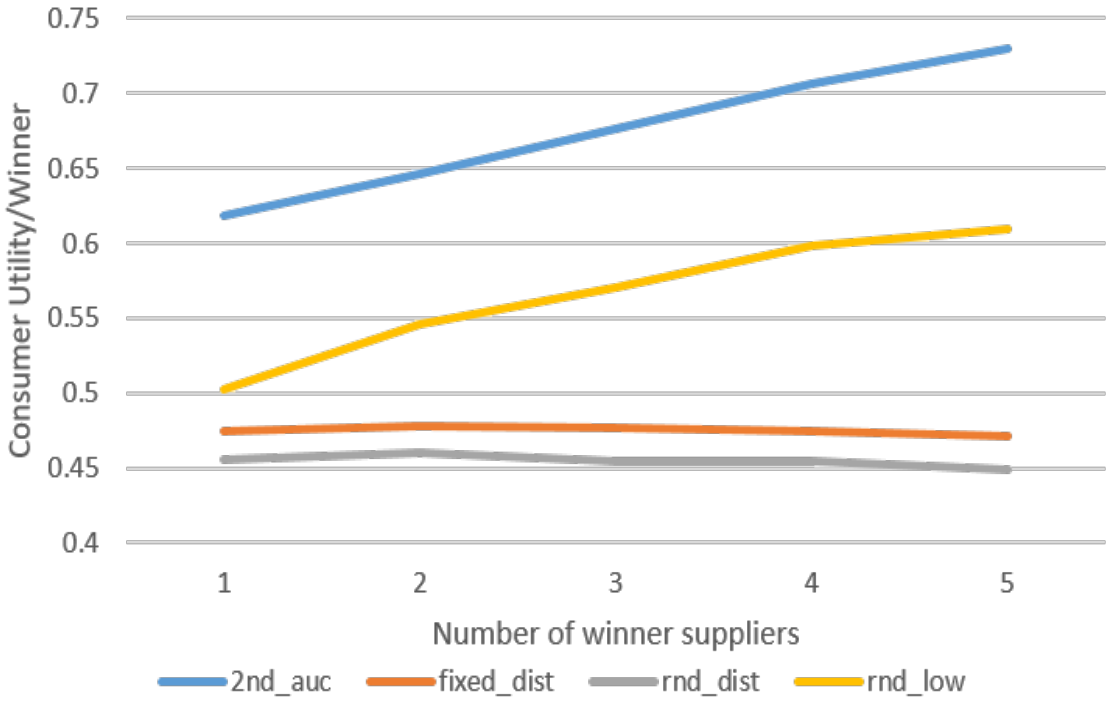

Figure 3.9: Consumer Utility/Winner vs Number of Winner Suppliers for Second-Score Auction

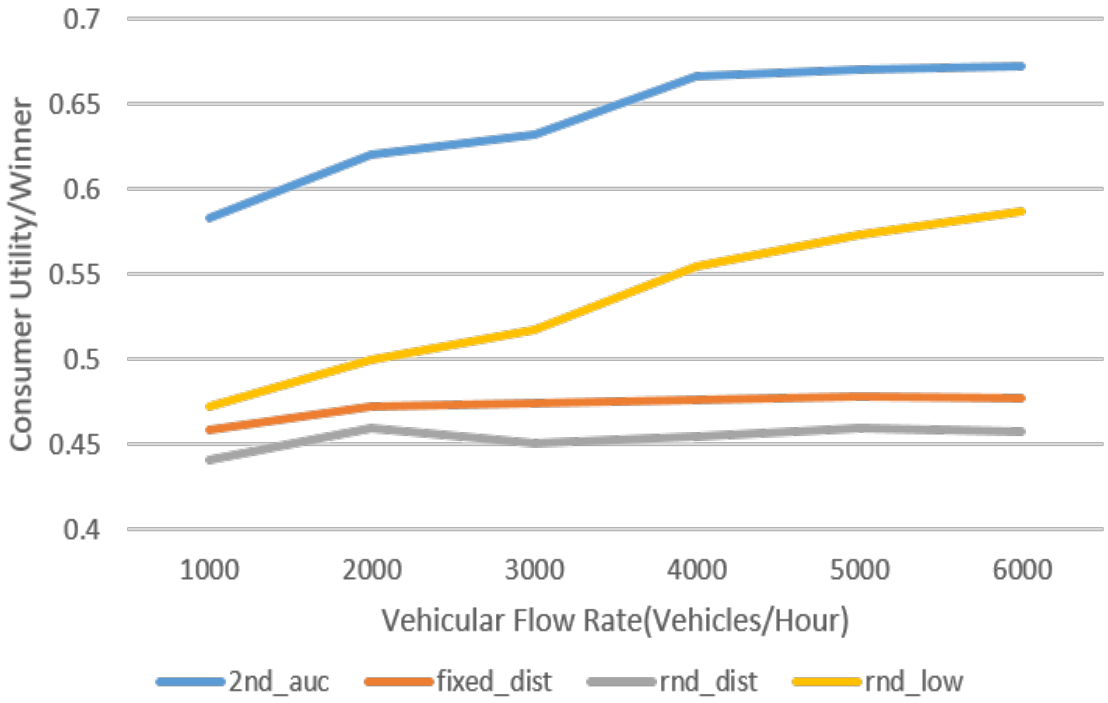

Figure 3.10: Consumer Utility/Winner vs Vehicular Flow Rate for Second-Score Auction

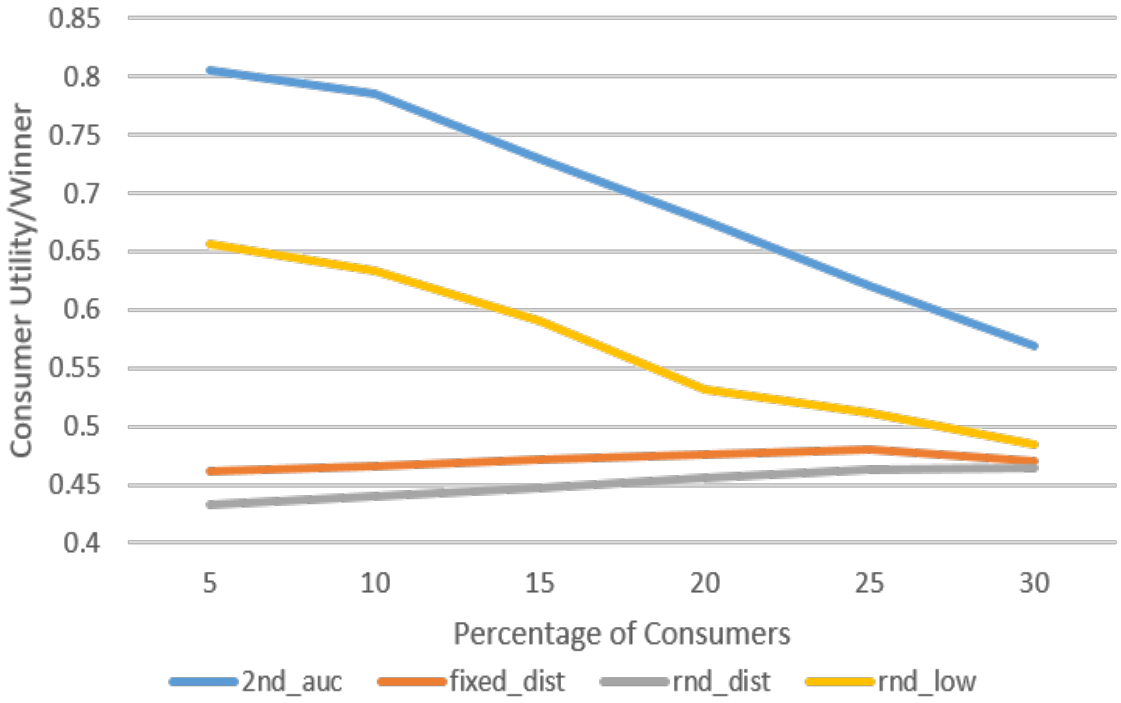

Figure 3.11: Consumer Utility/Winner vs Percentage of Consumers for Second-Score Auction

Algorithm 5 second_score_sel$(n, N, \alpha, msg_lst, Rep_list)$

Input: $n, N, \alpha, msg\_lst, Rep\_list$

Output: win_list containing identity and price for winners on second score basis.

```
score_list ← NULL
for j = 1 to n do
    θ, id ← msg_list(j) < θ_j, id_j >
    Rep ← Rep_list(j) < Rep_Vsj >
    score = α.Rep − θ
    score_list.append(id, score, θ, Rep)
end for
win_list ← NULL
Sort score_list on basis of score
for j = 1 to N do
    price ← score_list(j+1) < θ > +α(score_list(j) < Rep > −score_list(j+1) < Rep >)
    win_list.append(score_list(j) < id, price >
end for
```

vehicles. Since the vehicles are selected without price consideration, utility is derived from random pricing and reputation values giving an overall constant utility when the average is considered. It is less than $fixed\_dist$ due to the unusually high pricing being it's drawback as states in Section 3.3.2.

Since pricing is the main factor considered while determining the consumer utility, both $2nd\_auc$ and $rand\_low$ who select vehicles on basis of price behave better than $fixed\_dist$, $rand\_dist$ where distance is the selection parameter. $2nd\_auc$ considering reputation as a selection criteria behaves better than the $rand\_low$ where trustworthiness is not taken into account leading to loss of consumer utility.

From Figure 3.8, we can observe on increasing number of eligible suppliers, the utility of $2nd\_auc$ gradually increases and then becomes saturated. Since the number of supplier vehicles increase and their cost and reputation is uniformly distributed, we come across high scoring vehicles to choose from, leading to a higher score and hence high consumer utility.

Figure 3.9 illustrates that on increasing the number of selected winner, the consumer utility gradually increases. The score of each subsequent winner is decreases leading to decrease in utility. So as the number of winners increase, the consumer utility/winner average should decrease gradually. But more number of winners imply high number of supplier vehicles and as seen from Figure 3.8, the consumer utility increases with the number of eligible suppliers. Therefore the consumer utility vs number of winners is a balance between the above two factors while dominated by the effect of high number of eligible vehicles leading to it's constant increase.

Figure 3.10 a depict that on increasing the traffic flow in the network, the utility of consumer nodes gradually increase. This is due to the increase in number of eligible suppliers in the network and thereby increasing as explained previously in this section.

From Figure 3.11 we can note that on increasing the number of consumers in the channel, the consumer utility decreases. When number of consumer increase, demand of the resources increase while the availability of resources decrease. This leads to less number of supplier vehicle choices leading to low score and hence decrease in consumer utility.

3.6 Summary

In this chapter, a second-score sealed bid auction is proposed for addressing the resource selection problem in the vehicular cloud. Here, the quality of service parameter is relaxed and the entire resource unit is provided by the supplier vehicle to the consumer vehicle. Initially, we model the utility, cost and valuation functions with respect to the present scenario where no quality of service parameters are taken into account. Then three standard pricing-based resource selection methodologies, namely $fixed\_dist$, $rand\_dist$ and $rand\_low$ were elaborated to be used in future for comparison purpose. Subsequently, the $2nd\_auc$ mechanism was proposed which helps the supplier vehicles to determine the optimal price to bid for obtaining the desirable profit without decreasing it's probability of winning. This bidding price was proved to be a dominant strategy. The winner selection problem for the consumer vehicles was also solved using a scoring function. A comprehensive experimentation was conducted which illustrated that the $2nd\_auc$ behaves better than other standard pricing-based resource selection mechanisms for utility maximization of the consumer vehicles.

Chapter 4

Multi-attribute Vickrey's Auction for Pricing-Based Resource Selection

4.1 Introduction

The concept of vehicular cloud computing proposed by Olariu et al. has widespread applications in ITS like dynamic traffic light scheduling, multimedia transfer and road safety alerts [1]. The problem of resource selection is the major hindrance faced to effective formation of vehicular cloud. Addressing this problem is highly complex due to it's dependence on resource pricing which in turn depends on the market demand. Additionally, the resource selection also depends on the quality of service provided and the trustworthiness in the form of reputation of supplier vehicles.

As explained in the previous chapter, economic models in form of auctions have been extensively used to address the resource selection problem based on pricing. A second-score sealed bid auction was proposed in Chapter 3 which performed better than the standard pricing-based resource selection schemes. But we didn't take into consideration quality of resources which designing the previous second-score protocol. This forces the consumer vehicles to rent the whole resource of supplier vehicles by paying higher price even though they have specific requirements. Also, a smooth service provisioning occurs when distinct quality of service parameters are specified in the contract as the supplier vehicles fulfill it to get full payment and reputation.

Vickrey's auction mechanism has been proposed earlier to address resource selection problem in cloud computing[47]. We propose a multi-attribute Vickrey's auction scheme which aids the supplier vehicles in determining the proper quality values and the corresponding price to bid so as to obtain maximum profit without reducing their winning probability. This auction mechanism also instigates the vehicular supplier to stay truthful and reveal their true valuations irrespective of their selfish nature.

The chapter is organized as follows: In Section 4.2, we elaborate the system model and the utility, cost and valuation functions of consumer and supplier vehicles considering quality of service parameters. The multi-attribute Vickrey's auction mechanism was proposed in Section 4.3 for solving the pricing-based resource selection problem. Subsequently an

extensive experimentation is conducted in Section 4.4 to compare the Vickrey's auction with the previously proposed second-score sealed bid auction ($2nd\_auc$) and other standard pricing-based resource selection mechanisms. The chapter is summarised in Section 4.5.

4.2 System Model

The vehicular cloud architecture used in this chapter is similar to the one described in Section 3.2. As illustrated in Figure 3.1, supplier vehicles act as cloud service providers and consumer vehicles form vehicular cloud consumers. They communicate with each other and to RSUs using V2V communication and V2I communication respectively. All vehicles have the Internet access through cellular networks or through RSUs. They are connected to the TA through the Internet which responsible for the initial registration of the vehicles as well as maintenance and updation of their personal records, balance and reputation. The balance transfer occurs after a successful completion of service provisioning event as per the negotiated amount. Simultaneously the reputation of the supplier vehicle is also incremented as per the feedback received from the consumer vehicle. Whenever a consumer vehicle requests for the reputation Rep_{sj} of supplier vehicle V_{sj}, the TA calculates the current reputation value from the old reputation value Rep_{oldj} as per equation 3.1 formulated in the previous chapter.

We consider one consumer vehicle V_c and n interested supplier vehicles for the resource provisioning phase. The major drawback of the second-score auction (2nd_auc) was that quality of service parameters were not considered. The consumer vehicle have to rent the whole resource unit of the supplier vehicle by paying the full price. For example, if a consumer vehicle is in need of only computing resources, it unnecessarily also pays for the networking resources which decreases it's utility. Also, the maximum latency, error rate and maximum relative velocity requirements can be declared for a smooth service provisioning. Hence, in this chapter, we also include the quality of service requirements of the consumer vehicle V_c which was not included in the previous chapter. The consumer vehicle V_c specifies preference for each quality parameter in terms of a weightage values $\{D_1, D_2, D_3, D_4, D_5\}$.

Every supplier vehicle is associated with a cost value θ_j. The cost function C_{sj} used is formulated in equation 2.1. It shows that with a unit increase in quality parameter q_{ij} provided by the supplier vehicle V_{sj}, the cost of providing that service increases by a constant value $b_i.\theta_j$ for the supplier vehicle throughout its quality range. The utility function U_{sj} of the supplier vehicle considered in this chapter is same as equation 2.2 as the difference between the price p_j it receives and cost of service C_{sj} it provides. The valuation function Va_{cj} used in the subsequent sections of this chapter is formulated by equation 2.3 which describes the benefit that the consumer vehicle obtains from a supplier vehicle V_{sj}. Equation 2.4 formulates the overall utility U_c of the consumer vehicle V_c from N winner supplier vehicles. The research problem considered in this chapter is same as described in Section

2.5.1. The optimal price and quality determination by the supplier vehicles is a maximization function of supplier utility U_{sj} as illustrated by equation 2.5. The objective of consumer vehicles is determining of set of N winner suppliers W_c expressed as the maximization of vehicular consumer utility function U_c in equation 2.6.

4.3 Multi-attribute Vickrey's Auction for Pricing-Based Resource Selection

The multi-attribute Vickrey's auction is an extension of the $second\_score\_auc$ protocol as discussed in the previous chapter which considers the quality parameters instead of providing the whole resource unit for rent. The winner selection in this protocol is done by maximizing the scoring function which is to be declared at the beginning of the auction. The scoring rule is declared as:

$$S_c(p, q_1, ..., q_5, Rep) = \left(\sum_{i=1}^{5} d_i.\sqrt{q_i}\right) + \alpha.Rep - p \tag{4.1}$$

The main problem of the supplier vehicles is to determine the optimal quality parameters and pricing value associated with it that they should bid so maximize their profit without decreasing their chances of winning. After the scoring function S is declared by the consumer vehicle, the valuation of each bid to the consumer vehicle is known by the supplier vehicles. For multi-attribute Vickrey's auction, Che has proposed that unique symmetric equilibrium is one in which each supplier offers bids of each quality attribute as [55]:

$$q_{ij}^*(\theta_j) = \underset{q_{ij}}{\operatorname{argmax}}(Va_{sj} - C_{sj}(\theta_j)) \tag{4.2}$$

Employing the equation 4.1 to our system model and differentiating the given equation with respect to the quality parameter gives us the optimal pricing value:

$$\begin{aligned} &\frac{d(Va_{sj} - C_{sj}(\theta_j))}{dq_{ij}} = 0 \\ \Rightarrow &\frac{d\left(\sum_{i=1}^{5} D_i.\sqrt{q_{ij}}\right) + \alpha.Rep_j - \theta_j.\left(\sum_{i=1}^{5} b_i.q_{ij}\right)}{dq_{ij}} = 0 \\ \Rightarrow &\frac{D_i}{2.\sqrt{q_{ij}^*}} - b_i.\theta_j = 0 \\ \Rightarrow &q_{ij}^*(\theta_j) = \left(\frac{D_i}{2b_i\theta_j}\right)^2 \end{aligned} \tag{4.3}$$

The optimal pricing value that the supplier vehicle should bid in Vickrey's auction is the one which gives it zero utility. Therefore, the pricing value that the supplier vehicle should bid for the optimal quality parameters can be derived as:

$$
\begin{aligned}
& U_{sj} = 0 \\
& \Rightarrow p_j^* - \theta_j . \left(\sum_{i=1}^{5} b_i . q_{ij}^* \right) = 0 \\
& \Rightarrow p_j^* - \theta_j . \left(\sum_{i=1}^{5} b_i . \left(\frac{D_i}{2 b_i \theta_j} \right)^2 \right) = 0 \\
& \Rightarrow p_j^*(\theta_j) = \frac{1}{4\theta_j} \sum_{i=1}^{5} \frac{{D_i}^2}{b_i}
\end{aligned}
\tag{4.4}
$$

The price that should be paid to the winner supplier vehicle is decided as per the score of next highest supplier vehicle after replacing the bidding price with the payment value. The monetary transfer that is to be done after the service provisioning phase is derived as:

$$
\begin{aligned}
& S_{sj} = S_{sj+1} \\
& \Rightarrow \left(\sum_{i=1}^{5} d_i . \sqrt{q_{ij}} \right) + \alpha . Rep_j - price_j^* = \\
& \left(\sum_{i=1}^{5} d_i . \sqrt{q_{ij+1}} \right) + \alpha . Rep_{j+1} - p_{j+1} \\
& \Rightarrow price_j^* = p_{j+1}^* + \sum_{i=1}^{5} D_i (\sqrt{q_{ij}^*} - \sqrt{q_{ij+1}^*}) + \alpha (Rep_j - Rep_{j+1})
\end{aligned}
\tag{4.5}
$$

Lemma 4.3.1. *The optimal price that the supplier vehicles should bid is* $p_j^*(\theta_j) = \frac{1}{4\theta_j} \sum_{i=1}^{5} \frac{{D_i}^2}{b_i}$ *which is a dominant strategy.*

$Proof$: The above lemma means that bidding its actual valuation which gives it zero utility is the dominant strategy of the supplier vehicle. Similar to the previous chapter, we prove this strategy to be dominant by the method of contradiction.

In the first case, we assume that bidding a price $p_{sj} > p_j^*$ gives the supplier a higher utility. On bidding a higher price, the score of the supplier vehicle decreases as seen by equation 4.1 and hence the chances of winning of that supplier vehicle decreases. The bidding price p_j does not determine the price $price_j^*$ it will receive after getting selected as the winner which only depends on the bidding of the next highest scorer.So the utility of the supplier remains same as the case when he bids $p_{sj} = p_j^*$ but the probability of winning decreases. So a contradiction is derived.

In the next case, we assume that bidding a price $p_{sj} < p_j^*$ gives the supplier a higher utility. Since the supplier vehicle is assumed to be rationale and does not want negative utility, a contradiction is derived.

Hence bidding p_j^* is the dominant strategy of the supplier vehicle V_{sj} in the multi-attribute Vickrey's auction.

The multi-attribute Vickrey's auction protocol as illustrated by Figure 4.1 explained as:

1. $V_c \rightarrow * : M_1^5$ The consumer vehicle broadcasts the service request message along with it's identity, current direction, speed, reputation weightage and weightage for each quality parameter as $qual\_req = \{D_1, D_2, D_3, D_4, D_5\}$. Hence the message constituent is: $M_1^5 =< id_{Vc}, Serv\_Req, vik\_qual, \alpha, qual\_req, dir_{Vc}, spd_{Vc} >$

2. V_{sj} :qual_price_calc$(qual_req, \theta_j, cost_coef) \rightarrow (qual_prov, p_j)$ After receiving the service request message, the interested supplier vehicle calculates the optimal quality and the pricing value to bid with the help of Algorithm 6 which uses equation 4.3 and 4.4. It uses the cost coefficient parameters for each quality parameter as $cost\_coef = \{b_1, b_2, b_3, b_4, b_5\}$ which remains constant for all supplier vehicles. The optimal quality parameters are calculated as $qual\_prov = \{q_{1j}^*, q_{2j}^*, q_{3j}^*, q_{4j}^*, q_{5j}^*\}$

3. $V_{sj} \rightarrow V_c : M_{2sj}^5$ The supplier vehicles send the service availability message to the consumer vehicle consisting of it's identity, optimal quality and pricing values and also it's current direction. So $M_{2sj}^5 =< id_{Vsj}, Serv\_Avl, vik\_score\_auc, qual\_prov, p_j, dir_{Vsj} >$

4. V_c: dir_check$(n', msg_lst', dir_{Vc}) \rightarrow (msg_list, egl_list, n)$ The consumer vehicle segregates the suppliers moving in it's direction by using Algorithm 4 to create a new list called egl_list of n eligible supplier vehicles after receiving the service availability message list $msg\_lst' =< M_{2s1}^5, M_{2s2}^5, ..., M_{2sj}^5 ..., M_{2sn'}^5 >$ from the interested vehicles to determine the eligible supplier list.

5. $V_c \rightarrow$TA: M_3^5 The consumer vehicle requests the TA to give the reputation values of the supplier vehicles in egl_list along with it's identity. Here $M_3^5 =< id_{Vc}, Rep\_Req, vik\_qual, egl\_list >$

6. TA $\rightarrow V_c : Rep\_list$ The TA replies back to the consumer vehicle giving the reputation of each supplier in the egl_list provided to it in form of $Rep\_list =< (id_{Vs1}, Rep_{Vs1}), (id_{Vs2}, Rep_{Vs2}), ..., (id_{Vsj}, Rep_{Vsj}), ..., (id_{Vsn}, Rep_{Vsn}) > \forall id_{Vsj} \in egl\_list$

7. V_c: vickrey_auc_sel$(n, N, \alpha, qual_req, msg_lst, Rep_list) \rightarrow win_list$ After getting the reputation values of each eligible supplier node, the consumer vehicle calculates the winner list as per Algorithm 7. It also determines the price that will be provided to each winner after the service provisioning phase using equation 4.5.

8. $V_c \rightarrow * : M_4^5$The consumer vehicle then broadcasts the winner list consisting the identity of each winner and the price to be provided to them where $M_4^5 =< id_{Vc}, win\_list >$

9. $V_c \leftrightarrow V_{sj}$: service_provision. In this phase the service provisioning occurs between consumer and supplier vehicle. Since relative velocity is one of the quality parameters, the supplier vehicles are expected to stay within the maximum relative speed as per their bid failing which their reputation won't be incremented in the next phase.

10. V_c →TA: M_5^5:The consumer vehicle sends to TA two lists of service providers. The $serv\_provlst^5 = \{(id_{Vs1}, price_{s1}), (id_{Vs2}, price_{s2}), ..., (id_{Vsk}, price_{sk}), ..., (id_{Vsav}, price_{sav})\}$ where V_{sk} are the vehicles and av is the number of vehicles who provided service complete time yet did not satisfy the quality requirements they sent during bidding. And $gdserv\_provlst^5 = \{(id_{Vs1}, price_{s1}), (id_{Vs2}, price_{s2}), ..., (id_{Vsk}, price_{sl}), ..., (id_{Vsgd}, price_{sgd})\}$ where V_{sl} are the vehicles and gd is the number of vehicles who provided service complete time and satisfied the quality requirements they sent during bidding. Here $M_5^5 =< id_{Vc}, vik\_qual, gdserv\_provlst^5, serv\_provlst^5 >$

11. TA:rep_payment_transfer. After receiving the identity and pricing list of sincere suppliers $gdserv\_provlst^5$ who provided smooth service throughout the service provisioning phase, the TA transfers the amount mentioned in the list from consumer vehicle to supplier vehicles. It also updates the reputation value of these suppliers by a constant value RA. For the supplier vehicles in $serv\_provlst^5$ who don't provide the service as per the contract but provide service for the entire negotiated time, the payment is transfered and their reputation value is incremented as $\frac{RA}{2}$.

Algorithm 6 qual_price_calc$(qual_req, \theta_j, cost_coef)$

Input: $(qual\_req, \theta_j, cost\_coef)$
Output: $qual\_prov, p_j$ which is the list of quality to be provided and price for the same.

1: $qual\_prov \leftarrow$ **NULL**
2: $p_j \leftarrow 0$
3: **for** $i = 1$ to 5 **do**
4: $\quad q_{ij}^* \leftarrow \left(\frac{qual\_req(i)}{2.cost\_coef(i).\theta_j}\right)^2$
5: $\quad p_j \leftarrow p_j + q_{ij}^*.cost\_coef(i).\theta_j$
6: $\quad qual\_prov$.**append**(q_{ij}^*)
7: **end for**

4.4 Experimentation and Analysis

A comprehensive experiment set up was done for evaluation of proposed Multi-attribute Vickrey's Auction vik_qual and the results were compared with the second score auction protocol $2nd\_auc$ and standard pricing-based selection mechanisms $fixed\_dist$ and

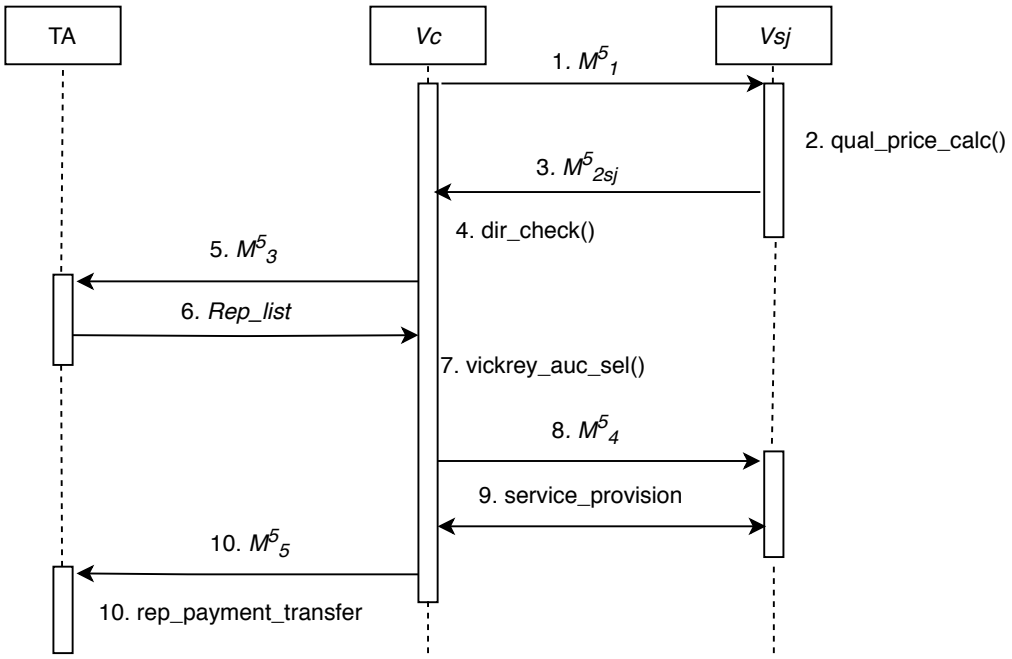

Figure 4.1: Multi-Attribute Vickrey's Auction for pricing-based resource selection

Algorithm 7 vik_score_sel$(n, N, \alpha, qual_req, msg_lst, Rep_list)$

Input: $n, N, \alpha, qual\_req, msg\_lst, Rep\_list$

Output: win_list containing identity and price for winners on Vickrey's auction basis.

$score\_list \leftarrow$ NULL
for $j = 1$ to n **do**
  $\theta, id, qual, p \leftarrow msg\_list(j) < \theta_j, id_j, qual\_prov_j, p_j >$
  $Rep \leftarrow Rep\_list(j) < Rep_{Vsj} >$
  $score \leftarrow \alpha.Rep - p$
  for $i = 1$ to 5 **do**
    $score = score + qual\_req(i)\sqrt{qual(i)}$
  end for
  $score\_list$.**append**$(id, score, p, qual, Rep)$
end for
$win\_list \leftarrow$ **NULL**
Sort $score\_list$ on basis of $score$
for $j = 1$ to N **do**
  $price \leftarrow score\_list(j{+}1) < p > +\alpha(score\_list(j) < Rep > - score\_list(j{+}1) < Rep >)$
  for $i = 1$ to 5 **do**
    $price = price + qual\_req(i)(\sqrt{score\_list(j) < qual(i) >} - \sqrt{score\_list(j+1) < qual(i) >})$
  end for
  win_list.**append**$(score\_list(j) < id, price >$
end for

Parameter	Value
$b_1, b_2...b_5$	Uniform(0,1)
D_3	Normal(μ = 0.9, σ = 0.1)
D_4	Normal(μ = 0.93, σ = 0.07)
D_5	Normal(μ = 0.93, σ = 0.07)
α	Normal(μ = 0.8, σ = 0.2)

Table 4.1: Parameters and their values

Case	D_1	D_2
Computation intensive	Normal(μ = 0.9, σ = 0.1)	Normal(μ = 0.05, σ = 0.1)
Network intensive	Normal(μ = 0, σ = 0.1)	Normal(μ = 0.9, σ = 0.1)
Network and computation intensive	Normal(μ = 0.9, σ = 0.1)	Normal(μ = 0.9, σ = 0.1)
Network and computation random	Uniform(0,1)	Uniform(0,1)

Table 4.2: Service requirement cases

rnd_low. The simulation was conducted using Simulation of Urban MObility (SUMO) platform with the help of Python programming language using 10 virtual machines each with 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory using Amazon Aws [51],[52]. Similar to the previous chapter, a 15km stretch of NH53 highway near Paradip Port, India Figure 3.7 was taken using the OpenStreetMap software [53].

The vehicular traffic flow rate was varied between 1000 vehicles/hour till 6000 vehicles/hour and the following distributions were used for traffic flow: a negative exponential distribution low traffic flow rate, Pearson Type III distribution for intermediate traffic flow rate and normal distribution for high traffic flow rate [54]. Similar to the Section 3.5, the transmission range for vehicular communication is fixed at 400m. The reputation of supplier vehicles is uniformly distributed between 0 and 1. The upper and lower limit of the cost parameter θ_j of the supplier vehicles is fixed at 1 and 100 respectively and is uniformly distributed throughout the range for uniform distribution while in normal distribution case, the mean (μ) is fixed at 50 with a standard deviation (σ) of 10. Table 4.1 gives the list of parameters used and their value.

Four cases of service requirement was taken into consideration as per Table 4.2 The service provision time is taken as 60 seconds and the percentage of the consumers in the simulation scenario is varied between 0.05 till 0.3. Similar to the previous Chapter, the maximum number of selected winner vehicles is set at 5 and the maximum number of eligible suppliers can be observed to be 40. Consumer utility per winner is considered as the metric to evaluate the performance of the multi-attribute Vickrey's auction protocol in comparison to the other protocols. For the second score auction protocol $2nd\_auc$ and standard pricing-based selection mechanisms $fixed\_dist$ and rnd_low, the quality parameters is fixed as the maximum bid done by all the supplier vehicles for each quality

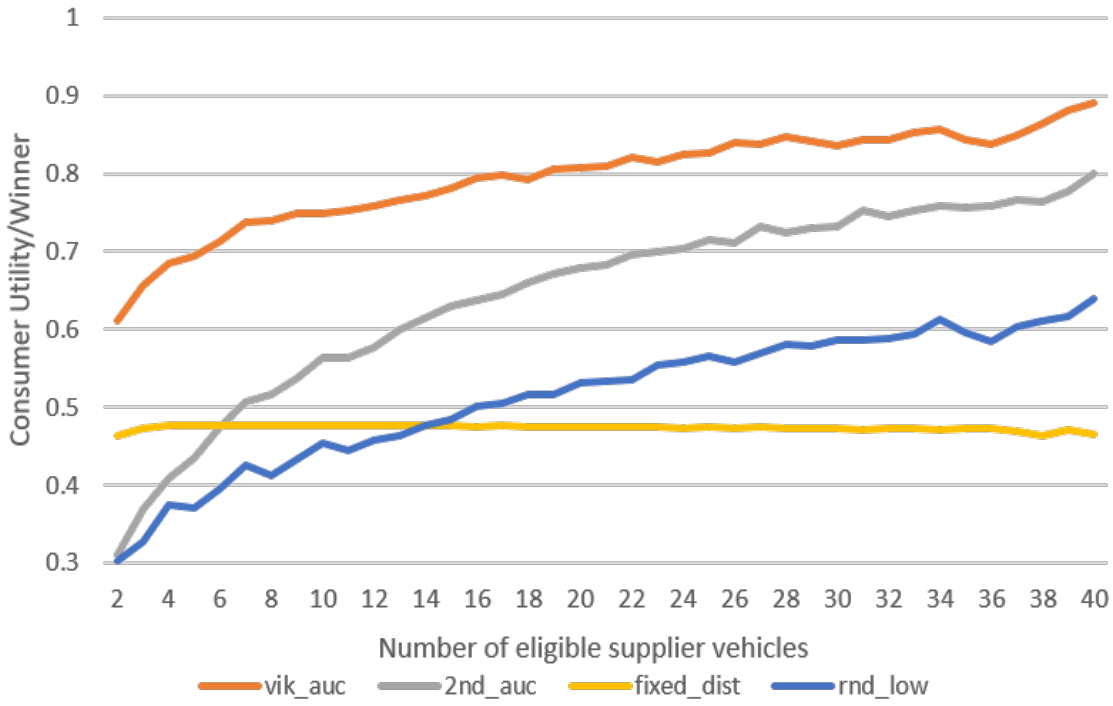

Figure 4.2: Consumer Utility/Winner vs Number of Eligible Suppliers using uniform cost distribution for Vickrey's Auction

parameter.

4.4.1 Numerical Analysis

Multi-attribute Vickrey's auction vik_auc behaves better than $2nd\_auc$ because the consumer vehicle only pays for what it requires instead of paying for the entire resource unit as in case of $2nd\_auc$. Therefore it's utility is higher than that of $2nd\_auc$ for all cases of uniform and normal distribution of cost parameter.

From Figure 4.2 and Figure 4.6, it is seen that on increasing number of eligible suppliers, the slope of the utility curve vik_qual gradually increases and then becomes saturated. This is due to the fact that when the eligible supplier vehicle population increases, since their cost and reputation is uniformly distributed, we come across more high scoring supplier vehicles to choose from. This makes the consumer to select winner supplier having higher score than the normal scenarios which gives it high utility.

Figure 4.3 and Figure 4.7 illustrates that on increasing the number of selected winner, the consumer utility gradually increases. The score of each subsequent winner decreases leading to decrease in overall utility. So as the number of winners increase, the consumer utility/winner average should decrease gradually. But more number of winners imply high number of supplier vehicles and as seen from Figure 4.2, the consumer utility increases with the number of eligible suppliers. Therefore the consumer utility vs number of winners is a balance between the above two factors while dominated by the effect of high number of

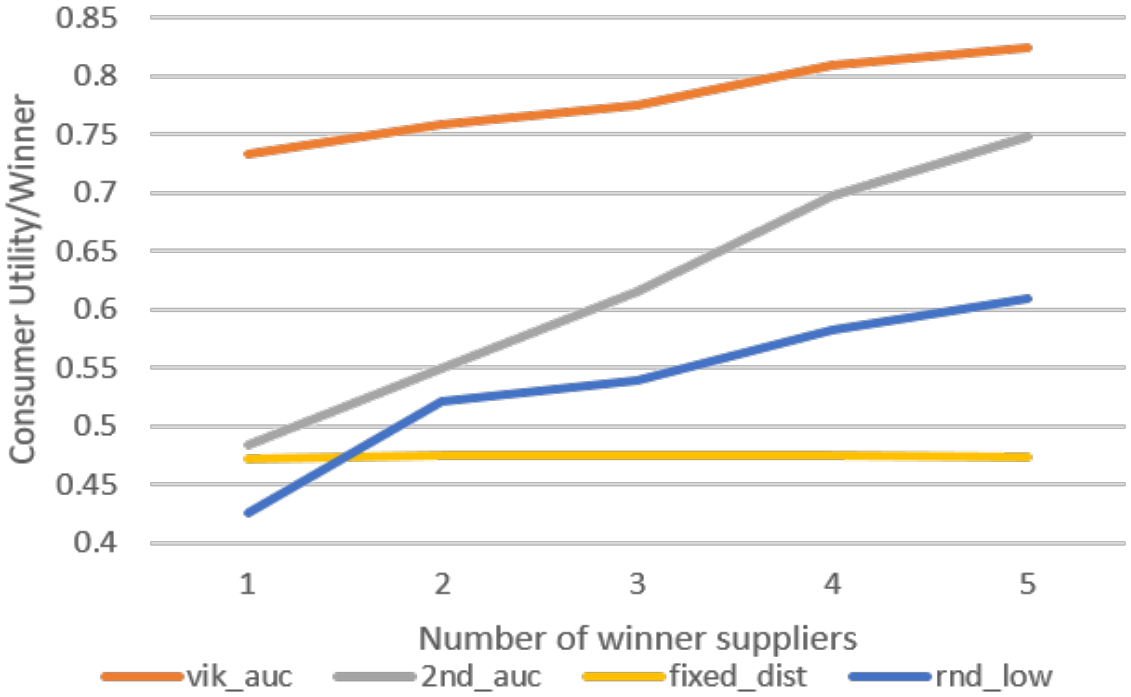

Figure 4.3: Consumer Utility/Winner vs Number of Winner Suppliers using uniform cost distribution for Vickrey's Auction

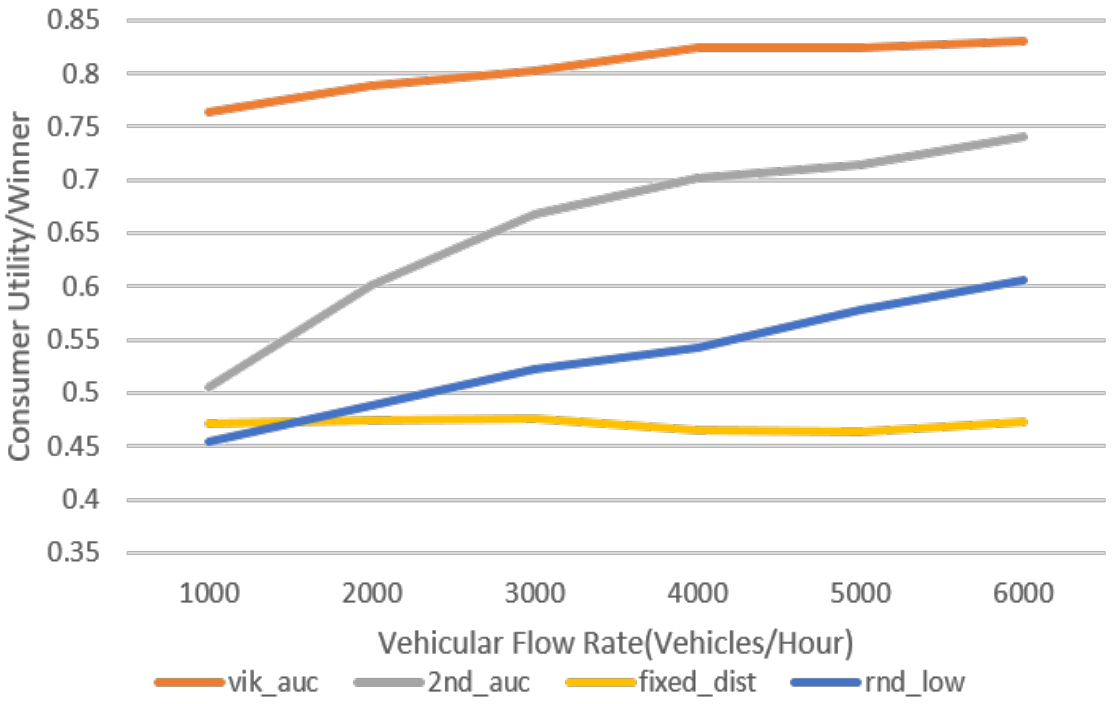

Figure 4.4: Consumer Utility/Winner vs Vehicular Flow Rate in Vehicles/Hour using uniform cost distribution for Vickrey's Auction

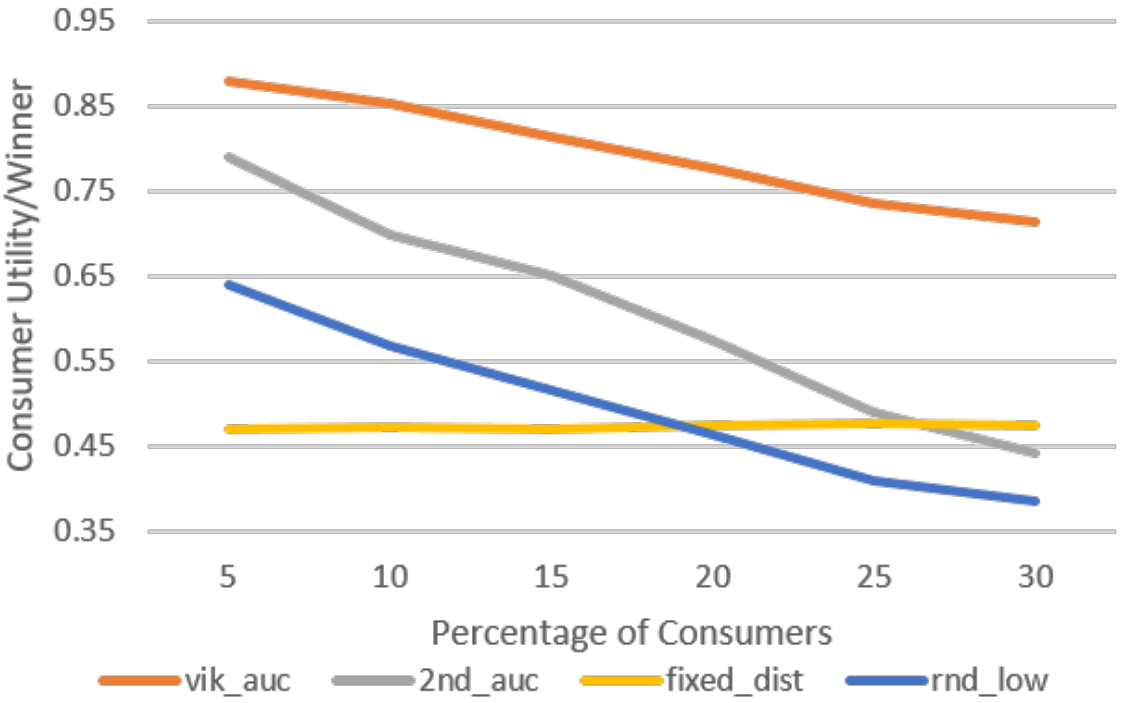

Figure 4.5: Consumer Utility/Winner vs Percentage of Consumers using uniform cost distribution for Vickrey's Auction

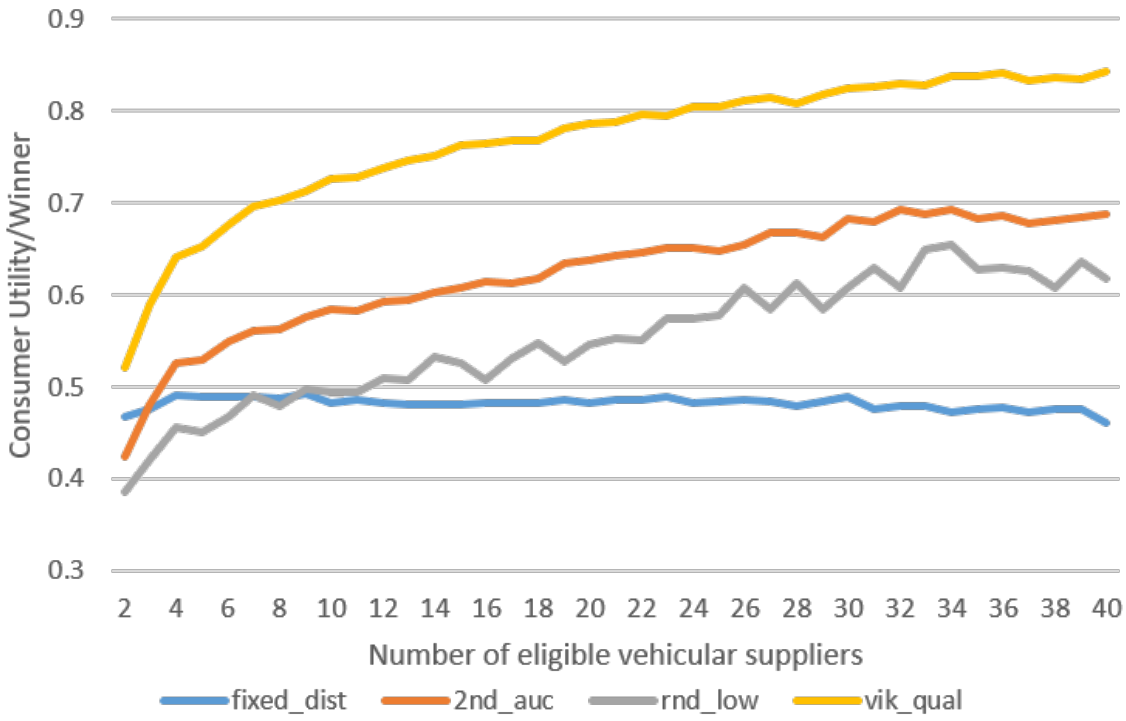

Figure 4.6: Consumer Utility/Winner vs Number of Eligible Suppliers using normal cost distribution for Vickrey's Auction

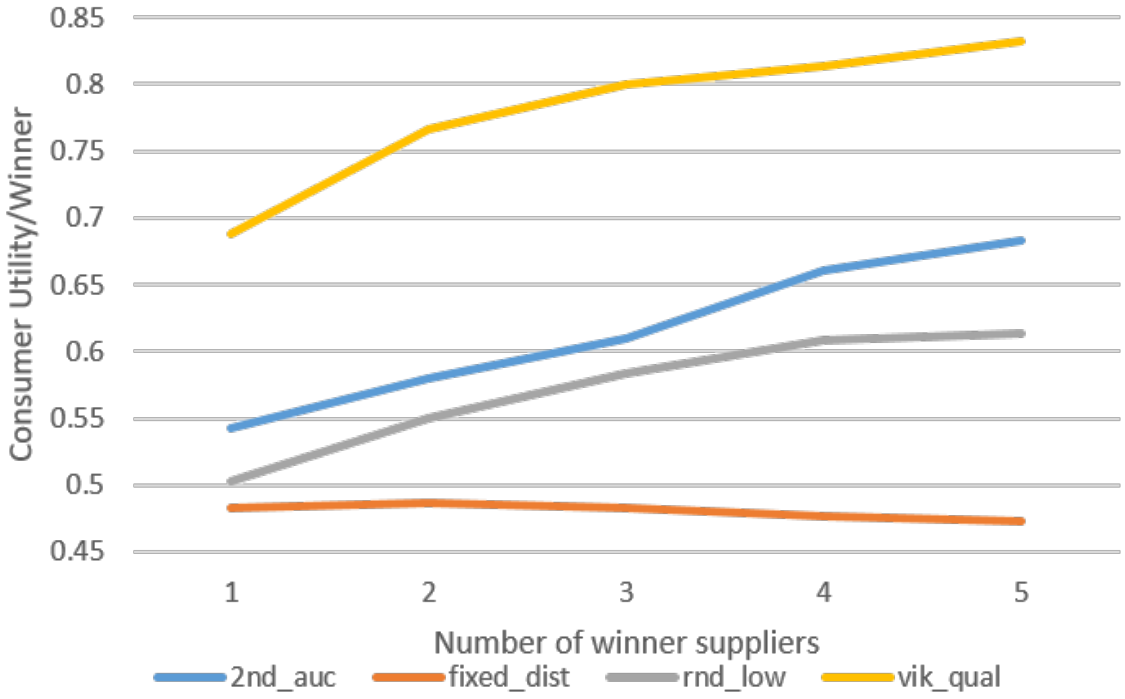

Figure 4.7: Consumer Utility/Winner vs Number of Winner Suppliers using normal cost distribution for Vickrey's Auction

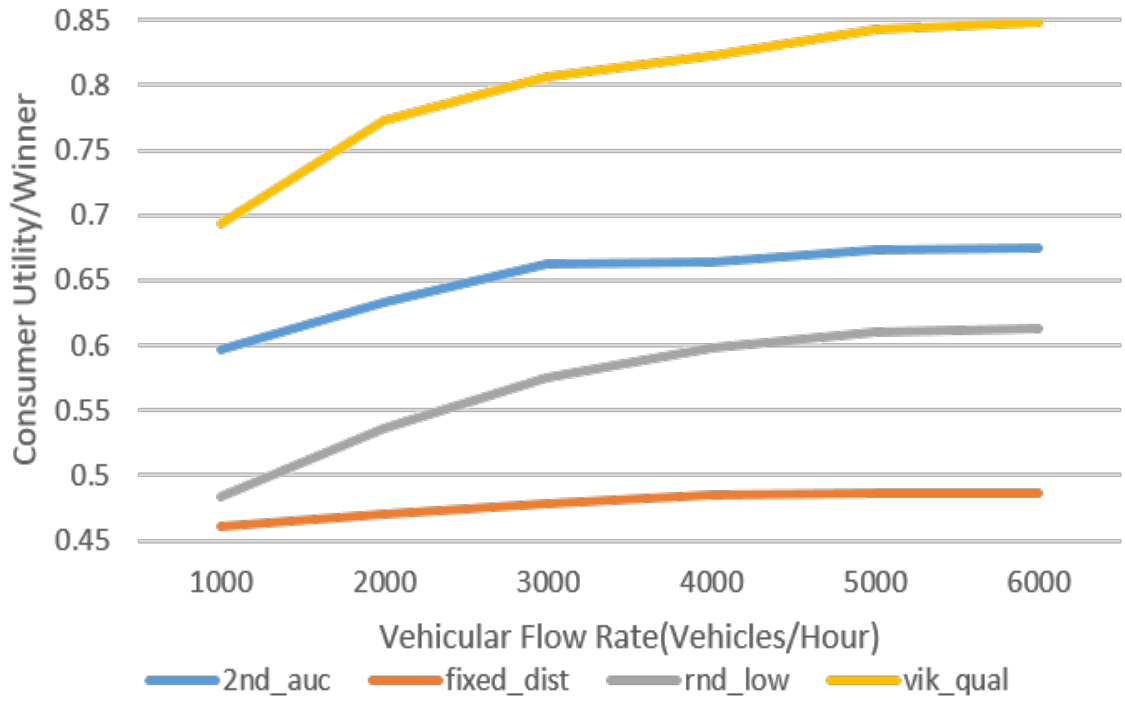

Figure 4.8: Consumer Utility/Winner vs Vehicular Flow Rate in Vehicles/Hour using normal cost distribution for Vickrey's Auction

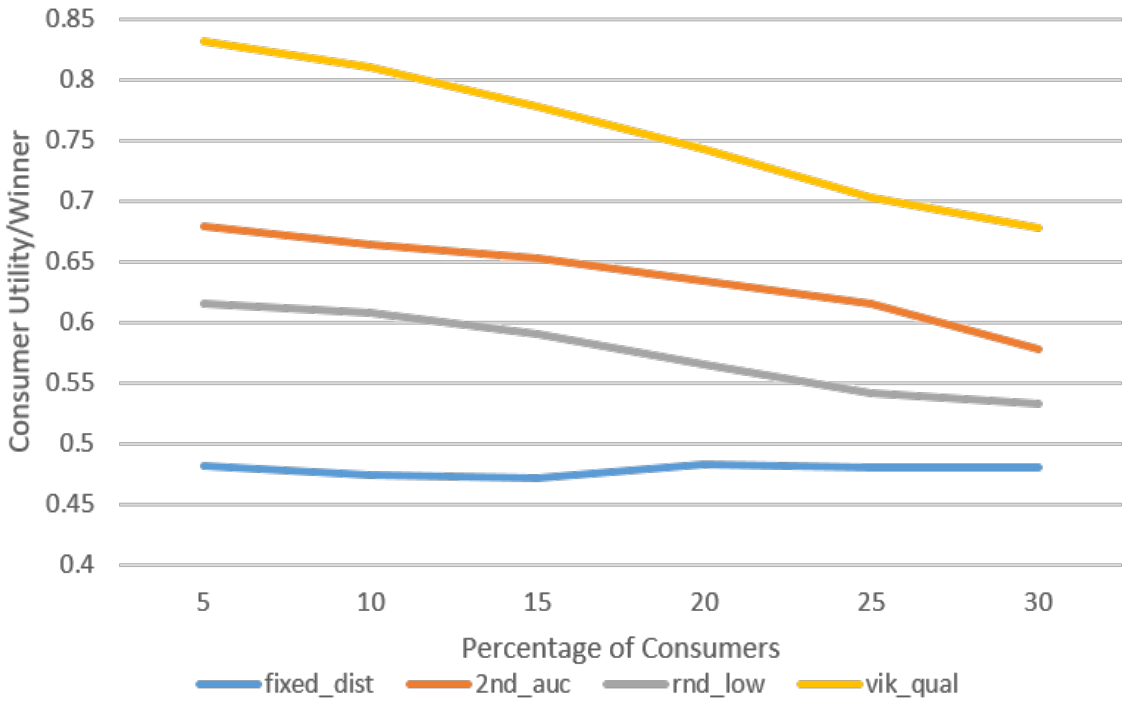

Figure 4.9: Consumer Utility/Winner vs Percentage of Consumers using normal cost distribution for Vickrey's Auction

eligible vehicles leading to it's constant increase.

Figure 4.4 and 4.8 shows that when the traffic flow in the network increases, the utility of consumer nodes gradually increase. This is due to the increase in number of eligible suppliers in the network and thereby increasing as explained previously in this section.

Figure 4.5 and 4.9 can help us conclude that on increasing the number of consumers in the channel, the consumer utility decreases. When number of consumer increase, demand of the resources increase while the availability of resources decrease. This leads to less number of supplier vehicle choices leading to low score and hence decrease in consumer utility.

4.5 Summary

We propose a multi-attribute Vickrey's auction for pricing-based resource selection in vehicular cloud in this chapter. In contrast to the previous chapter, we consider the quality of service requirements while designing the utility, cost and valuation functions of consumer and supplier vehicles. Subsequently, the Vickrey's auction (vic_qual) mechanism was proposed which helps the supplier vehicles to determine the optimal price to bid for obtaining the desirable profit without decreasing it's probability of winning. This bidding price was proved to be a dominant strategy. The winner selection problem for the consumer vehicles was also solved using a scoring function. A extensive experimentation was conducted which illustrated that the vic_qual achieves better utility than the previously proposed second-score

sealed bid auction $2nd\_auc$ and other standard pricing-based resource selection mechanisms.

Chapter 5

First-Score Sealed Bid Auction for Pricing-Based Resource Selection

5.1 Introduction

Autonomous Vehicular Cloud is a state-of-the-art concept refers to a large group of largely autonomous vehicles whose corporate computing, sensing, communication and physical resources can be coordinated and dynamically allocated to authorized users. As discussed previously, the main obstacle to the proper exploitation of this concept is resource selection and it's pricing. Due to the dynamic nature of the vehicular environment, the demand of the resources is ever changing and the pricing of the resources have to be determined in real-time for optimal profit of both consumer and supplier vehicles. Address the resource selection problem is difficult since it depends on a varied number of factors like quality of service provide and trustworthiness of the supplier vehicles apart from the pricing of resources.

Auction theory has been previously used to address the dynamic pricing problem as per the market demand [47],[46] and [47]. Previously in Chapter 3, we proposed a second–score sealed bid auction scheme to address the resource selection problem in vehicular cloud. The quality of service requirements were not considered in that mechanism which was it's major drawback. In the subsequent chapter we proposed a multi-attribute Vickrey's auction for selecting suppliers as well as determining optimal quality and pricing values. It instigates the suppliers to bid their actual valuations by making the consumers pay a higher price which leads to decrease in consumer utility. Here we propose a first-score sealed bid auction which enables the suppliers to bid quality parameters and the pricing values as per the market demand. The consumer provides the suppliers with their bidding price as opposed to a hiked price in case of Vickrey's auction.

The organization of this chapter is as follows: In Section 5.2, a system model is described which is similar to the one in Section 4.2. The optimal quality and price values for the vehicular suppliers to bid is derived for both uniform and normal distribution of cost parameter in Section 5.3. Additionally, the optimal preference values that the consumer vehicles should declare is obtained. A systematic elaboration of the message passing model in the first-score auction is also done. In Section 5.4, a comprehensive experimentation is

conducted for comparison of the first-score sealed bid auction with the previously proposed multi-attribute Vickrey's auction, second-core sealed bid auction and other standard pricing based resource selection mechanisms. The Chapter is summarized in Chapter 5.5.

5.2 System Model

In this chapter, we use the vehicular cloud architecture used as discussed in Section 3.2. The supplier vehicles serve as cloud service providers and consumer vehicles act as vehicular cloud consumers as portrayed in Figure 3.1. Using V2V and V2I mechanisms of IEEE 802.11p, the consumer and supplier vehicles intercommunicate as well as connect to the RSUs in their range. Every vehicle is connected to the Internet either through cellular networks or via RSUs which acts as a gateway. Vehicles are assumed to have all time access to the TA using the Internet connection. As elaborated in the previous chapters, TA does the registration of new vehicles interested in participating in vehicular cloud. Additionally, TA is responsible for the maintenance of private records of vehicles. Payment of the negotiated amount to the supplier vehicles from the consumer vehicle after the service provision phase is carried out by TA. Concurrently, reputation updation of supplier vehicle is carried out according to the consumer vehicle feedback. At any instant, the TA calculates the current reputation of supplier vehicle V_{sj} using it's old reputation Rep_{oldj} as formulated by equation 3.1.

A single consumer vehicle V_c and n interested supplier vehicles are considered designing pricing-based resource selection mechanism. All factors including trustworthiness of supplier vehicles, quality of service requirement by consumer vehicles, pricing of resources based on market demand are taken into consideration in this chapter. This chapter uses the same cost function C_{sj}, supplier utility function U_{sj}, valuation function function Va_{sj} and consumer utility function U_c as elaborated in Section 2.5 and also applied in chapter 4. The cost of resource provisioning by a supplier vehicle V_{sj} is denoted by cost function C_{sj} as formulated in equation 2.1. It uses the cost parameter θ_j of the vehicle which is it's private knowledge. On increasing the quality parameter q_{ij} by one unit, the resource provisioning cost increases by $b_i.\theta_j$ for the supplier vehicle. In this chapter, we use the utility function U_{sj} of the supplier vehicle as given in equation 2.2. The value of the service derived by the consumer vehicle from a supplier vehicle V_{sj} is expressed as a valuation function Va_{cj} as formulated by equation 2.3. The utility function U_c of the consumer vehicle V_c used in this chapter is same as of equation 2.4 which is the benefit it obtains from N winner supplier vehicles.

In this chapter, we aim to find the price and quality parameters that supplier vehicles should declare for gaining maximum utility along with increasing it's chances of becoming the winner. This price and quality determination problem is expressed as maximization of supplier utility U_{sj} as derived in equation 2.5. The problem of finding the set of N winner

supplier vehicles W_c by consumer vehicle V_c, as addressed in this chapter, is described a maximization function of vehicular consumer U_c in equation 2.6.

5.3 First-Score Sealed Bid Auction for Pricing-Based Resource Selection

In a general first score auction protocol, an auctioneer declares the scoring rule which acts as a base for winner selection. All the auction participants calculate and submit their optimal bids according to the scoring rule privately to the auctioneer. The participant with the bid that yields the highest score is announced as the winner. Considering our system model, the consumer vehicle are substituted as the auctioneer and the supplier vehicles can represent the participants. The scoring rule as determined by the consumer vehicle is declared as:

$$S_c(p, q_1, ..., q_5, Rep) = \left(\sum_{i=1}^{5} d_i.\sqrt{q_i}\right) + \alpha.Rep - p \tag{5.1}$$

The optimal quality to bid is derived in the similar manner as the Vickrey's auction protocol as:

$$q_{ij}^*(\theta_j) = \left(\frac{D_i}{2b_i\theta_j}\right)^2 \tag{5.2}$$

Now we aim to determine the optimal pricing value that the supplier vehicle should bid considering the market demand. For an ordinary single valued first score auction, as per Krishna, the symmetric equilibrium strategy is to bid $\beta(x)$ as [56]:

$$\beta(x) = x - \int_0^x \frac{G(y)}{G(x)} dy \tag{5.3}$$

where x is the valuation of the object for the bidder and $\dfrac{G(y)}{G(x)} = \dfrac{F(y)}{F(x)}^{n-1}$ with n number of bidders. Here $F(x)$ is the cumulative distribution function for x. The probability density function for x is denoted by $f(x)$. Che proposes the pricing value for attaining the unique symmetric equilibrium for multi-dimensional sealed bid auction extended from equation 5.3 as [55]:

$$p_j^*(\theta_j) = C_{sj}(q_{ij}^*, \theta_j) + \int_{\theta_j}^{\tilde{\theta}} (C_{sj}^{'}(q_{ij}^*, \theta_t). \left(\frac{1 - F(t)}{1 - F(\theta_j)}\right)^{n-1} dt \tag{5.4}$$

Here $C_{sj}^{'}(q_{ij}^*, \theta_t)$ is the differentiation of the supplier cost function C_{sj} after putting the optimal quality values q_{ij}^* in the equation. Clearly the optimal price of the resources depend on the distribution function of the private cost value θ_j. Initially, we assume that θ_j has uniform distribution. Hence $F(\theta_j) = \dfrac{\theta_j - \underline{\theta}}{\tilde{\theta} - \underline{\theta}}$ and $f(\theta_j) = \dfrac{1}{\tilde{\theta} - \underline{\theta}}$. Since we use the cost function C_{sj} similar to the one used by David et al., the optimal pricing value that the supplier

vehicle should bid is [57]:

$$p_j^*(\theta_j) = \sum_{i=1}^{5} \frac{d_i^2}{4b_i} \left(\frac{1}{\theta_j} + \left(\frac{1}{\tilde{\theta} - \theta_j} \right)^{n-1} \cdot \int_{\theta_j}^{\tilde{\theta}} \frac{(\tilde{\theta} - t)^{n-1}}{t^2} dt \right) \tag{5.5}$$

Now, we consider the distribution of θ_j as normal distribution. Here $F(\theta_j, \mu, \sigma) = \frac{1 + g(\theta_j, \mu, \sigma)}{2}$ where $g(\theta_j, \mu, \sigma) = erf\left(\frac{\theta_j - \mu}{\sigma\sqrt{2}}\right)$ and erf is the error function often used in statistics. The probability distribution function is $f(\theta_j, \mu, \sigma) = \frac{r(\theta_j, \mu, \sigma)}{\sqrt{2\pi\sigma^2}}$ and $r(x, \mu, \sigma) = e^{-\left(\frac{x - \mu^2}{2\sigma^2}\right)}$. The optimal pricing value in case of normal distribution of cost parameter can be derived as:

$$\begin{aligned} p_j^*(\theta_j) &= \sum_{i=1}^{5} b_i.q_{ij}^*.\theta_j + \int_{\theta_j}^{\tilde{\theta}} (\sum_{i=1}^{5} \frac{d(b_i.q_{ij}^*.\theta_j)}{d\theta_j} \left(\frac{1 - g(t, \mu, \sigma)}{1 - g(\theta_j, \mu, \sigma)} \right)^{n-1} dt \\ &= \sum_{i=1}^{5} \frac{d_i^2}{4b_i.\theta_j} + \int_{\theta_j}^{\tilde{\theta}} \sum_{i=1}^{5} \frac{d_i^2}{4b_i.\theta_j} \left(\frac{1 - g(t, \mu, \sigma)}{1 - g(\theta_j, \mu, \sigma)} \right)^{n-1} dt \\ &= \sum_{i=1}^{5} \left(\frac{d_i^2}{4b_i} \left(\frac{1}{\theta_j} + \left(\frac{1}{1 - g(\theta_j, \mu, \sigma)} \right)^{n-1} \cdot \int_{\theta_j}^{\tilde{\theta}} \frac{1 - g(t, \mu, \sigma)^{n-1}}{t^2} dt \right) \right) \end{aligned} \tag{5.6}$$

5.3.1 Determination of Optimal Quality Preference

The supplier vehicles determine their optimal price and quality bids according to the quality preference values $org\_qual\_req = \{D_1, D_2, D_3, D_4, D_5\}$ declared by the consumer vehicle. It is often seen that revealing their actual quality preference by the consumer vehicles does not provide them with maximum utility. So they declare a modified optimal quality preference list $qual\_req = \{d_1, d_2, d_3, d_4, d_5\}$ calculated based on their original quality preference list org_qual_req. David et al. proposed to carry it out by maximizing the expected profit of the auctioneer from the auction with respect to each quality parameter [57]. The utility function U_c of the consumer vehicle, who is the auctioneer is different from the one used in their work and hence we derive the optimal quality preference list both in case of uniform distribution and normal distribution. The expected profit EP by David et al. is expressed as [57]:

$$EP(\underline{\theta}, \tilde{\theta}) = \int_{\underline{\theta}}^{\tilde{\theta}} U_c(p^*(t), q_1^*(t), ..., q_5^*(t), Rep_j)(1 - F(t))^{n-1}.n.f(t)dt \tag{5.7}$$

Now we determine the expected profit EP in case of uniform distribution of cost by replacing the original quality preference values D_i in optimal pricing $p^*(t)$ and $q_{ij}^*(t)$ to the optimal

ones d_i:

$$\begin{aligned} EP(\underline{\theta},\tilde{\theta}) &= \int_{\underline{\theta}}^{\tilde{\theta}} U_c(p^*(t), q_1^*(t), ..., q_5^*(t), Rep_j) \left(\frac{\tilde{\theta}-t}{\tilde{\theta}-\underline{\theta}}\right)^{n-1} .n.\frac{1}{\tilde{\theta}-\underline{\theta}}dt \\ &= \frac{n}{(\tilde{\theta}-\underline{\theta})^n}\sum_{i=1}^{5}\frac{D_i d_i}{2.b_i}\int_{\underline{\theta}}^{\tilde{\theta}}\frac{(\tilde{\theta}-t)^{n-1}}{t}dt + \alpha.Rep\int_{\underline{\theta}}^{\tilde{\theta}}(\tilde{\theta}-t)^{n-1}dt \\ &- \sum_{i=1}^{5}\frac{d_i^2}{4b_i}\left(\int_{\underline{\theta}}^{\tilde{\theta}}\frac{(\tilde{\theta}-t)^{n-1}}{t}dt + \int_{\underline{\theta}}^{\tilde{\theta}}\int_{t}^{\tilde{\theta}}\frac{(\tilde{\theta}-z)^{n-1}}{z^2}dzdt\right) \end{aligned} \tag{5.8}$$

On differentiating the $EP(\underline{\theta},\tilde{\theta})$ with respect to each quality parameter, we obtain the optimal quality preference values as:

$$\begin{aligned} &\frac{d(EP(\underline{\theta},\tilde{\theta}))}{dq_{ij}} = 0 \\ &\Rightarrow d_i(\underline{\theta},\tilde{\theta}) = D_i.\frac{\int_{\underline{\theta}}^{\tilde{\theta}}\frac{(\tilde{\theta}-t)^{n-1}}{t}dt}{\int_{\underline{\theta}}^{\tilde{\theta}}\frac{(\tilde{\theta}-t)^{n-1}}{t}dt + \int_{\underline{\theta}}^{\tilde{\theta}}\int_{t}^{\tilde{\theta}}\frac{(\tilde{\theta}-z)^{n-1}}{z^2}dzdt} \end{aligned} \tag{5.9}$$

Algorithm 8 qual_pref _calc$(dsbn, \underline{\theta}, \tilde{\theta}, org_qual_req, n, \mu, \sigma)$

Input: $(dsbn, \underline{\theta}, \tilde{\theta}, org\_qual\_req, n, \mu, \sigma)$
Output: $qual\_req$ list of quality preference coefficients to be declared.

$qual\_req \leftarrow$ **NULL**
if $dsbn =$UNIFORM **then**
  $int1 \leftarrow \int_{\underline{\theta}}^{\tilde{\theta}}\frac{(\tilde{\theta}-t)^{n-1}}{t}dt$
  $int2 \leftarrow \int_{\underline{\theta}}^{\tilde{\theta}}\int_{t}^{\tilde{\theta}}\frac{(\tilde{\theta}-z)^{n-1}}{z^2}dzdt$
else
  $int1 \leftarrow \int_{\underline{\theta}}^{\tilde{\theta}}\frac{(1-g(t,\mu,\sigma))^{n-1}}{t}r(t,\mu,\sigma)dt$
  $int2 \leftarrow \int_{\underline{\theta}}^{\tilde{\theta}} r(t,\mu,\sigma)\int_{\underline{t}}^{\tilde{\theta}}\frac{(1-g(z,\mu,\sigma))^{n-1}}{z^2}dzdt$
end if
$intv = \frac{int1}{int1+int2}$
for $i = 1$ to 5 **do**
  $d_i \leftarrow org\_qual\_req(i).intv$
  $qual\_req$.**append**(d_i)
end for

Carrying out the above process in case of normal distribution of cost parameter, we

Algorithm 9 qual_firstprice_calc$(dsbn, qual_req, \theta_j, cost_coef, n, \mu, \sigma)$

Input: $(dsbn, qual\_req, \theta_j, cost\_coef, n, \mu, \sigma)$
Output: $qual\_prov, p_j$ list of quality to be provided and price for the same.

$qual\_prov \leftarrow$ **NULL**
$p_j \leftarrow 0$
if $dsbn =$UNIFORM **then**

$$mulv \leftarrow \frac{1}{\theta_j} + \left(\frac{1}{\tilde{\theta} - \theta_j}\right)^{n-1} . \int_{\theta_j}^{\tilde{\theta}} \frac{(\tilde{\theta} - t)^{n-1}}{t^2} dt$$

else

$$mulv \leftarrow \frac{1}{\theta_j} + \left(\frac{1}{1 - g(\theta_j, \mu, \sigma)}\right)^{n-1} . \int_{\theta_j}^{\tilde{\theta}} \frac{1 - g(t, \mu, \sigma)^{n-1}}{t^2} dt$$

end if
for $i = 1$ to 5 **do**

$$q^*_{ij} \leftarrow \left(\frac{qual\_req(i)}{2.cost\_coef(i).\theta_j}\right)^2$$

$p_j \leftarrow p_j + q^*_{ij}.cost\_coef(i).\theta_j^2$
$qual\_prov$.append(q^*_{ij})
end for
$p_j \leftarrow p_j.mulv$

obtain:

$$d_i(\underline{\theta}, \tilde{\theta}) = D_i . \frac{\int_{\underline{\theta}}^{\tilde{\theta}} \frac{(1 - g(t, \mu, \sigma))^{n-1}}{t} r(t, \mu, \sigma) dt}{\int_{\underline{\theta}}^{\tilde{\theta}} \frac{(1 - g(t, \mu, \sigma))^{n-1}}{t} r(t, \mu, \sigma) dt + \int_{\underline{\theta}}^{\tilde{\theta}} r(t, \mu, \sigma) \int_{\underline{t}}^{\tilde{\theta}} \frac{(1 - g(z, \mu, \sigma))^{n-1}}{z^2} dz dt} \tag{5.10}$$

The first-score sealed bid auction protocol as depicted in Figure 5.1 is elaborated below:

1. $V_c \rightarrow * : M_1^6$ Initially the consumer vehicle broadcasts the service availability message along with it's identity, protocol name $first\_score\_auc$, reputation preference weight α along with it's current direction and speed. $M_1^6 =< id_{Vc}, Serv\_Req, first\_score\_auc, \alpha, dir_{Vc}, spd_{Vc} >$

2. $V_{sj} \rightarrow V_c : M_{2sj}^6$ $M_{2sj}^6 =< id_{Vsj}, Serv\_Avl, dir_{Vsj} >$ All the interested supplier vehicles send a service availability message along with their identity and current direction.

3. V_c: dir_check$(n^{'}, msg_lst^{'}, dir_{Vc}) \rightarrow (msg_list, egl_list, n)$ By using Algorithm 4 in Chapter 3, the consumer vehicles segregates the eligible suppliers who are moving in it's direction from all the interested suppliers. Here $msg\_lst^{'} =< M_{2s1}^6, M_{2s2}^6, ..., M_{2sj}^6 ..., M_{2sn'}^6 >$

4. V_c: qual_pref _calc$(dsbn, \underline{\theta}, \tilde{\theta}, org_qual_req, n, \mu, \sigma) \rightarrow qual_req$ Where μ is the mean and σ is the standard deviation. Consumer and suppliers has knowledge of

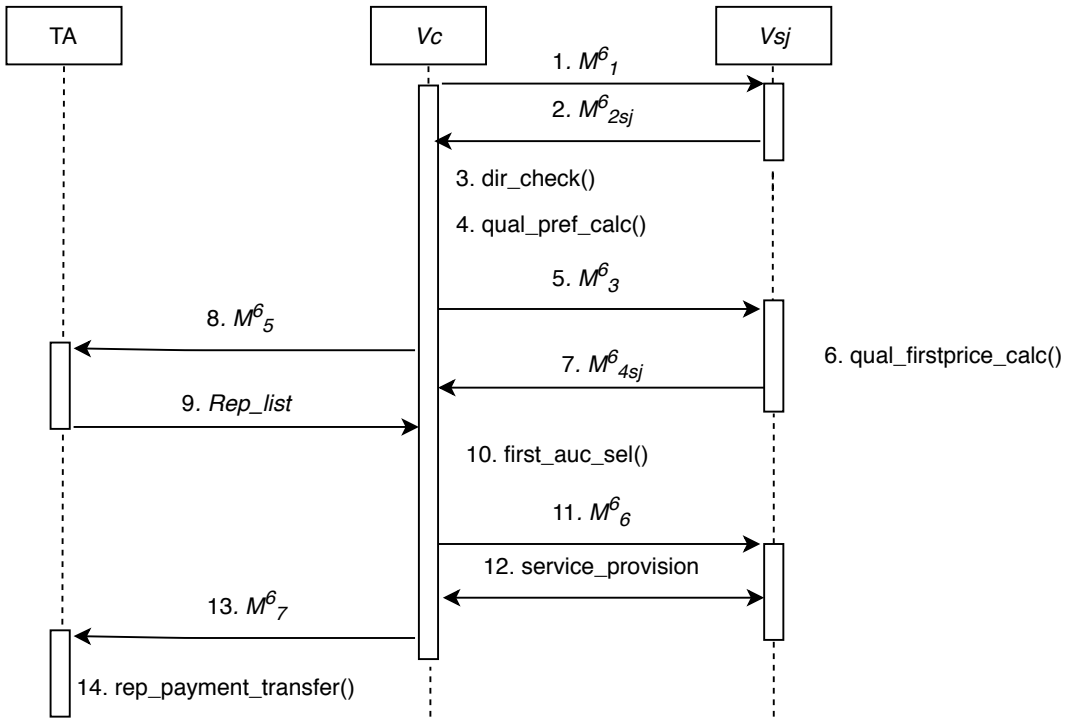

Figure 5.1: First-Score Sealed Bid Auction for pricing-based resource selection

Algorithm 10 first_auc_sel$(n, N, \alpha, qual_req, msg_lst, Rep_list)$

Input: $n, N, \alpha, qual\_req, msg\_lst, Rep\_list$

Output: win_list containing identity and price for winners on second score basis.

1: $score\_list \leftarrow$ NULL
2: **for** $j = 1$ to n **do**
3: $\theta, id, qual, price \leftarrow msg\_list(j) < \theta_j, id_j, qual\_prov_j, p_j >$
4: $Rep \leftarrow Rep\_list(j) < Rep_{Vsj} >$
5: $score \leftarrow \alpha.Rep - price$
6: **for** $i = 1$ to 5 **do**
7: $score = score + qual\_req(i)\sqrt{qual(i)}$
8: **end for**
9: $score\_list$.**append**$(id, score, price)$
10: **end for**
11: $win\_list \leftarrow$ **NULL**
12: **Sort** $score\_list$ on basis of $score$
13: **for** $j = 1$ to N **do**
14: win_list.**append**$(score\_list(j) < id, price >$
15: **end for**

distribution $dsbn$ and μ and σ if it has normal distribution. If it is uniform μ and σ are sent as 0. We assume that functions $g(x, \mu, \sigma)$ and $r(x, \mu, \sigma)$ are already defined in the system. On obtaining the number of eligible suppliers, the consumer vehicle determines the optimal quality preference list to be declared by using Algorithm 8.

5. $V_c \rightarrow * : M_3^6$ The consumer vehicle broadcasts the optimal quality preference list along with the number of eligible suppliers which will be required by the interested supplier vehicles while calculating their bids. Here $M_3^6 =< id_{Vc}, first\_score\_auc, qual\_req, n >$

6. V_{sj} :qual_firstprice_calc$(dsbn, qual_req, \theta_j, cost_coef, n, \mu, \sigma) \rightarrow (qual_prov, p_j)$ The supplier vehicles calculate their optimal pricing and quality values $qual\_prov = \{q_{1j}^*, q_{2j}^*, q_{3j}^*, q_{4j}^*, q_{5j}^*\}$ to bid as per the market demand which consists of quality preference values declared by the consumer and the number of interested supplier vehicles by using Algorithm 9. This also takes into consideration it's cost coefficient list $cost\_coef = \{b_1, b_2, b_3, b_4, b_5\}$.

7. $V_{sj} \rightarrow V_c : M_{4sj}^6$ The interested supplier vehicles send their bids to the consumer vehicle as $M_{4sj}^6 =< id_{Vsj}, qual\_prov, p_j, dir_{Vsj} >$

8. V_c →TA: M_5^6 $M_5^6 =< id_{Vc}, Rep_Req, first_score_auc, egl_list >$While the eligible suppliers calculate and send their bid, the consumer vehicle request the TA to send the reputation values of the eligible suppliers. Here we assume that all supplier vehicles who are in egl_list are going to reply.

9. TA $\rightarrow V_c$: Rep_list The TA sends a reputation list $Rep\_list =< (id_{Vs1}, Rep_{Vs1}), (id_{Vs2}, Rep_{Vs2}), ..., (id_{Vsj}, Rep_{Vsj}), ..., (id_{Vsn}, Rep_{Vsn}) >$ $\forall id_{Vsj} \in egl\_list$ of the interested suppliers to the consumer vehicle.

10. V_c: first_auc_sel$(n, N, \alpha, qual_req, msg_lst, Rep_list) \rightarrow win_list$ After receiving the reputation values of the suppliers and their quality and pricing bids, the consumer vehicle selects the winner suppliers using Algorithm 10.

11. $V_c \rightarrow * : M_6^6$ Here the consumer vehicle broadcasts the winner list along with the pricing values that will be provided to the winning suppliers vehicles after successful service provisioning. $M_6^6 =< id_{Vc}, win\_list >$

12. $V_c \leftrightarrow V_{sj}$: service_provision. In this step the service as per the appropriate quality parameters is provided by the supplier vehicles to the consumer vehicle . Since relative velocity is one of the quality parameters, the supplier vehicles are expected to stay within the maximum relative speed as per their bid failing which their reputation won't be incremented in the next phase.

13. $V_c \rightarrow$TA: M_7^6: where the consumer vehicle sends to TA three lists of service providers. $M_7^6 =< id_{Vc}, first\_score\_auc, gdserv\_provlst^5, serv\_provlst^5, bdveh^6 >$. The consumer vehicle sends to TA three lists of service providers. The $serv\_provlst^5 = \{(id_{Vs1}, price_{s1}), (id_{Vs2}, price_{s2}), ..., (id_{Vsk}, price_{sk}), ..., (id_{Vsav}, price_{sav})\}$ where V_{sk} are the vehicles and av is the number of vehicles who provided service complete time yet did not satisfy the quality requirements they sent during bidding. And $gdserv\_provlst^5 = \{(id_{Vs1}, price_{s1}), (id_{Vs2}, price_{s2}), ..., (id_{Vsk}, price_{sl}), ..., (id_{Vsgd}, price_{sgd})\}$ where V_{sl} are the vehicles and gd is the number of vehicles who provided service complete time and satisfied the quality requirements they sent during bidding. The third list $bdveh^6$ is the list of vehicles V_{sj} who sent who claimed service availability by sending M_{2sj}^6 but didn't bid by sending M_{4sj}^6

14. TA:rep_payment_transfer. When the TA receives the identity and pricing list of sincere suppliers $gdserv\_provlst^5$, the TA transfers the amount mentioned in the list from consumer vehicle to supplier vehicles. It also updates the reputation value of these suppliers by a constant value RA. For the supplier vehicles in $serv\_provlst^5$ who don't provide the service as per the contract but provide service for the entire negotiated time, the payment is transfered and their reputation value is incremented as $\frac{RA}{2}$. In the case of supplier vehicles in $bdveh^6$ list, the reputation is decremented by RA. Thus the selfish and malicious vehicles are segregated from the good ones.

5.4 Experimentation and Analysis

The experimental set up done for evaluation of first-score sealed bid auction $1st\_auc$ was compared with multi-attribute Vickrey's Auction vik_qual , second score auction protocol $2nd\_auc$ and standard pricing-based selection mechanisms $fixed\_dist$ and rnd_low. The simulation was conducted using Simulation of Urban MObility (SUMO) platform with the help of Python programming language using 10 virtual machines each with 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory using Amazon Aws [51], [52]. Similar to the previous chapter, a 15km stretch of NH53 highway near Paradip Port, India Figure 3.7 was taken using the OpenStreetMap software [53].

Similar to the previous chapter, the vehicular traffic flow rate was varied between 1000 vehicles/hour till 6000 vehicles/hour and a negative exponential distribution low traffic flow rate, Pearson Type III distribution for intermediate traffic flow rate and normal distribution for high traffic flow rate was taken into consideration [54]. Similar to the Section 4.4, the transmission range for vehicular communication is fixed at 400m and reputation of supplier vehicles is uniformly distributed between 0 and 1. The upper and lower limit of the cost parameter θ_j of the supplier vehicles is fixed at 1 and 100 respectively and is uniformly distributed throughout the range for uniform distribution while in normal distribution case,

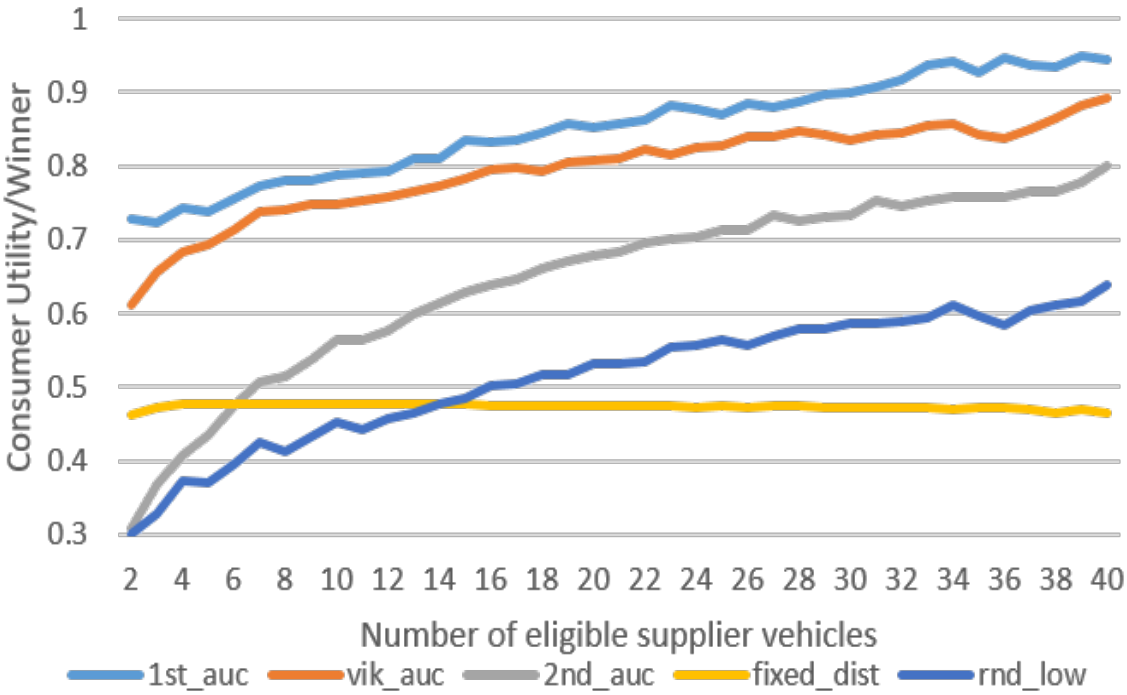

Figure 5.2: Consumer Utility/Winner vs Number of Eligible Suppliers using uniform cost distribution for First-Score Auction

the mean(μ) is fixed at 50 with a standard deviation(σ) of 10. Table 4.1 gives the list of parameters used and their value.

Four cases of service requirement by consumer vehicles was taken into consideration similar to Section 4.4 as given in Table 4.2. The service provision time is considered as 60 seconds while the consumers percentage in the simulation scenario is varied between 0.05 till 0.3. Similar to the previous Chapter 4, the maximum number of selected winner vehicles is set at 5 and the maximum number of eligible suppliers can be observed to be 40. Consumer utility per winner is considered as the metric to evaluate the performance of the first-score sealed bid auction protocol. And similar to Section 4.4, for the second score auction protocol $2nd\_auc$ and standard pricing-based selection mechanisms $fixed\_dist$ and rnd_low, the quality parameters is fixed as the maximum bid done by all the supplier vehicles for each quality parameter as per the first-score sealed bid auction protocol $1st\_auc$.

5.4.1 Numerical Analysis

All the graphs, namely Figure 5.2-5.9 show that the $1st\_auc$ behave better than vik_auc. This is because in vik_auc, the consumer vehicles pay price more than the supplier vehicle's bid to make them stay truthful. In $1st\_auc$, the supplier vehicles bid low price due to market demand which is paid to them thus increasing the consumer utility.

From Figure 5.2 and 5.6, we can observe on increasing number of eligible suppliers, the utility gradually increases and then becomes saturated. As the number of eligible supplier

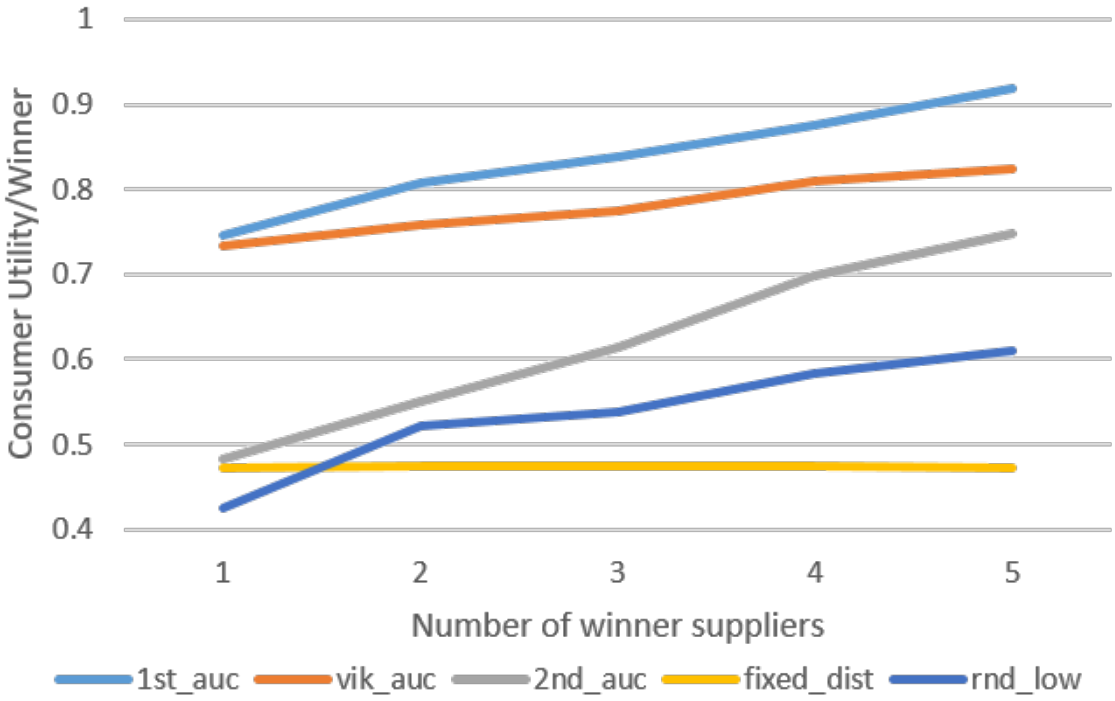

Figure 5.3: Consumer Utility/Winner vs Number of Winner Suppliers using uniform cost distribution for First-Score Auction

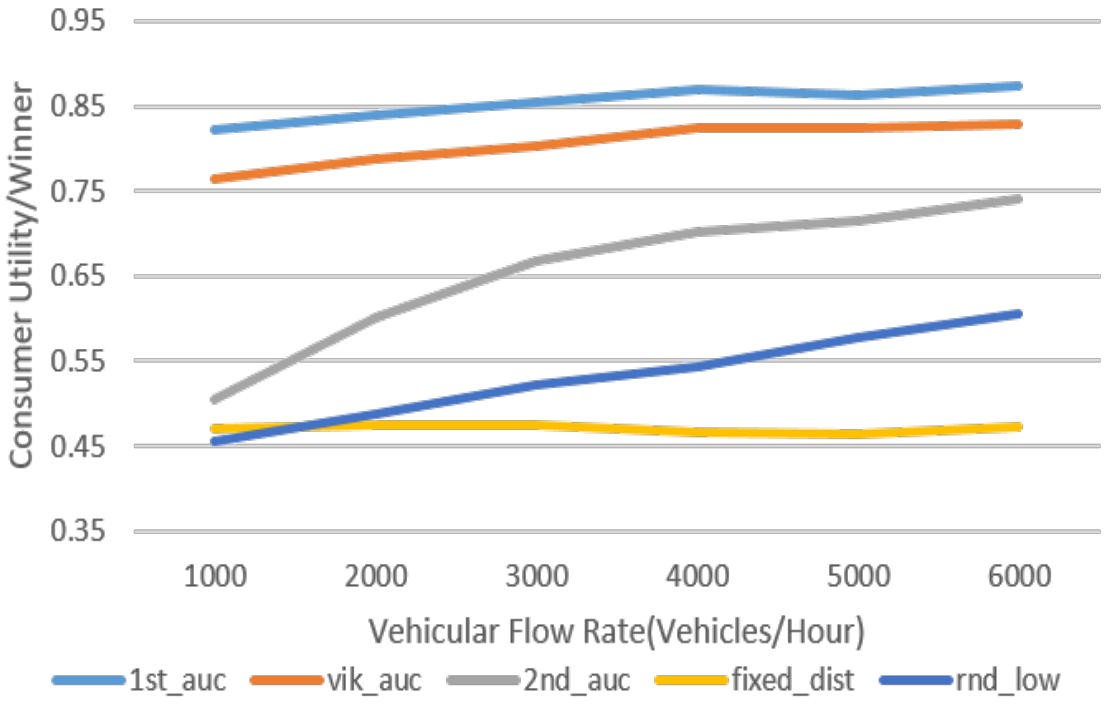

Figure 5.4: Consumer Utility/Winner vs Vehicular Flow Rate in Vehicles/Hour using uniform cost distribution for First-Score Auction

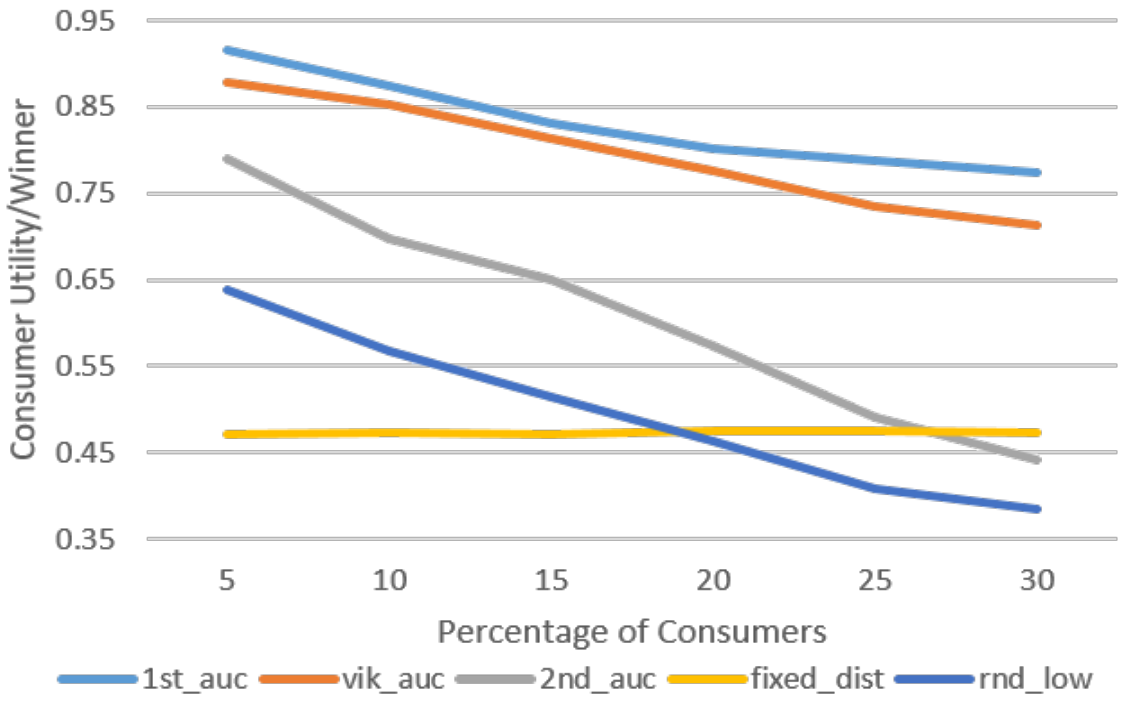

Figure 5.5: Consumer Utility/Winner vs Percentage of Consumers using uniform cost distribution for First-Score Auction

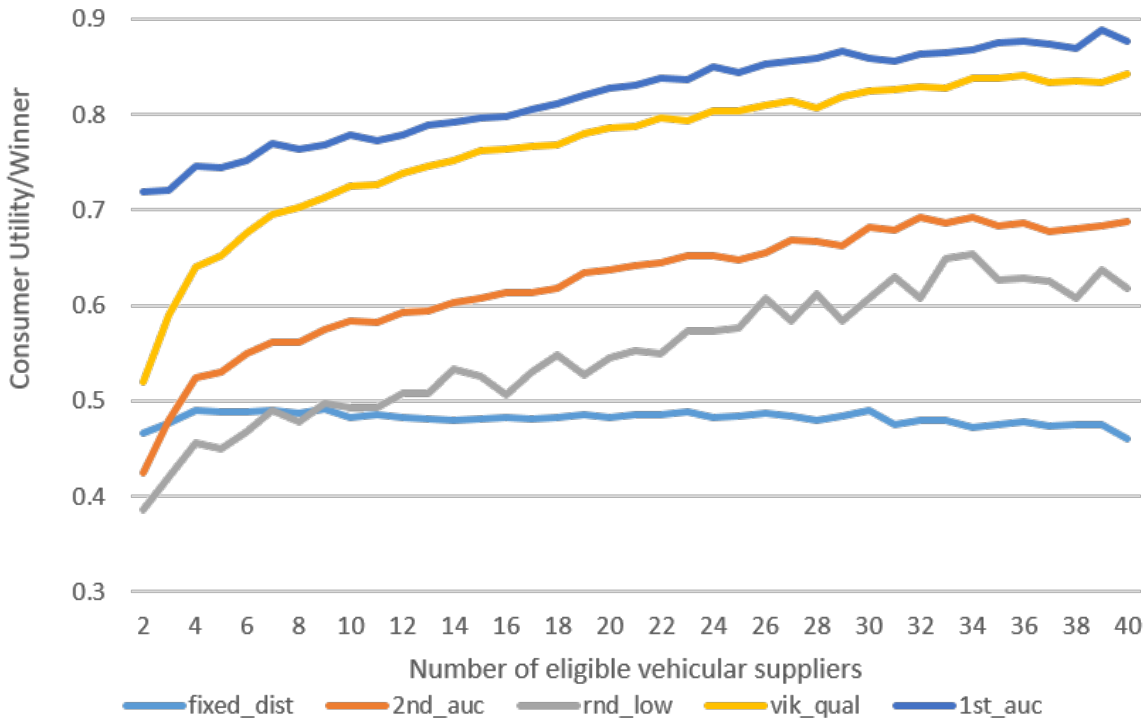

Figure 5.6: Consumer Utility/Winner vs Number of Eligible Suppliers using normal cost distribution for First-Score Auction

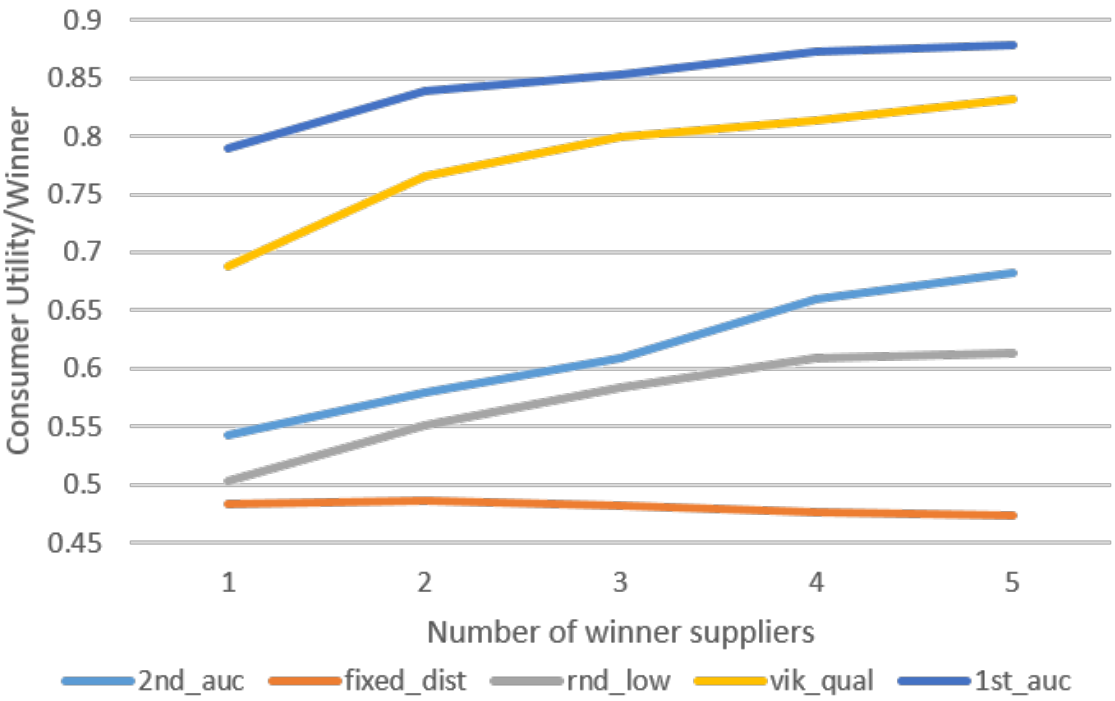

Figure 5.7: Consumer Utility/Winner vs Number of Winner Suppliers using normal cost distribution for First-Score Auction

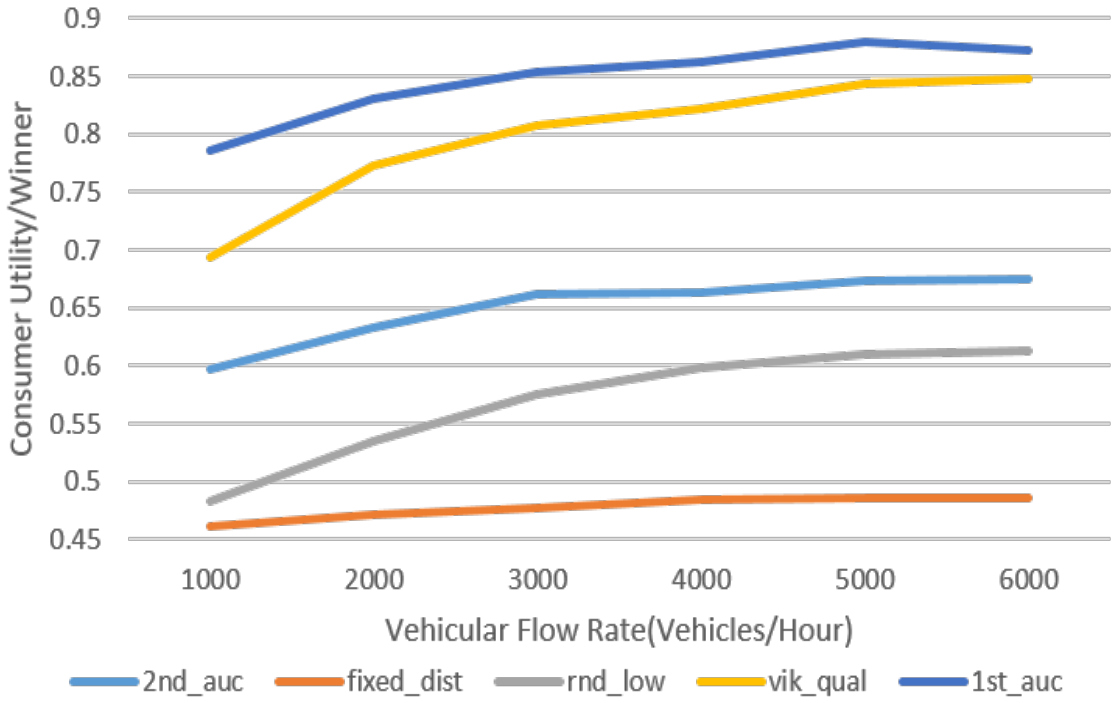

Figure 5.8: Consumer Utility/Winner vs Vehicular Flow Rate in Vehicles/Hour using normal cost distribution for First-Score Auction

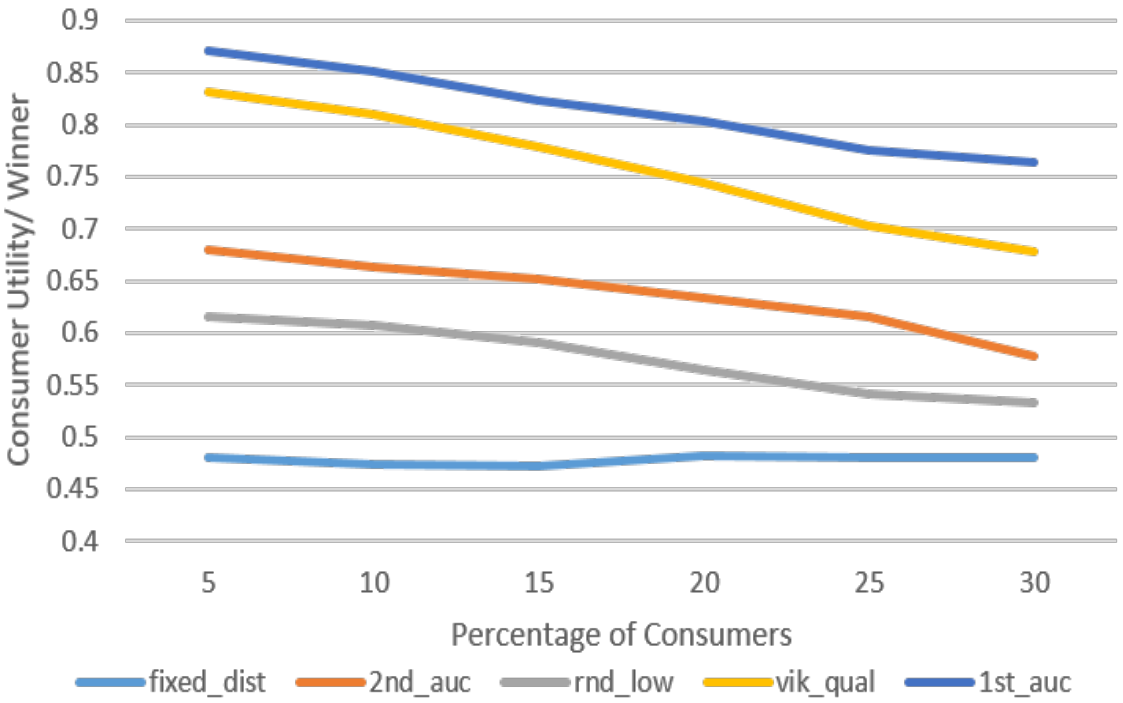

Figure 5.9: Consumer Utility/Winner vs Percentage of Consumers using normal cost distribution for First-Score Auction

increase, the market competition becomes leading to low pricing and hence more consumer utility. After a certain point, the price can't be decreased further leading to the maximum utility becoming constant.

Figure 5.3 and 5.7 illustrate that on increasing the number of selected winner, the consumer utility gradually increases. The score of each subsequent winner is decreases leading to decrease in utility. So as the number of winners increase, the consumer utility/winner average should decrease gradually. But more number of winners imply high number of supplier vehicles and as seen from Figure 5.2 and 5.6, the consumer utility increases with the number of eligible suppliers. Therefore the consumer utility vs number of winners is a balance between the above two factors while dominated by the effect of high number of eligible vehicles leading to it's constant increase.

Figure 5.4 and 5.8 depict that on increasing the traffic flow in the network, the utility of consumer nodes gradually increase. This is due to the increase in number of eligible suppliers in the network leading to high market competition and consumer utility growth.

From Figure 5.5 and 5.9 we can note that on increasing the number of consumers in the channel, the consumer utility decreases. When number of consumer increase, demand of the resources increase while the availability of resources decrease. This leads to high pricing and hence decrease in consumer utility.

As it can be seen from Figure 5.1, the communication cost of $1st\_auc$ is higher than other pricing based resource selection mechanisms. Since the auction process uses integration

function, the computational requirement of this mechanism is also higher than the others.

5.5 Summary

In this Chapter a first-score sealed bid auction ($1st\_auc$) is proposed to address the resource-selection problem in vehicular cloud. The system model is described which is similar to the one in Chapter 4. Optimal quality and price that the vehicular suppliers should bid is derived for both uniform and normal distribution of cost parameter. Also the expected profit of the vehicular consumers is maximized to obtain the optimal preference values that the consumer vehicles should declare to obtain maximum utility. A systematic elaboration of all message passing in the first-score auction is done. A detailed experimentation similar to Chapter 4 was conducted and the numerical analysis indicates that the first-score sealed bid auction achieves higher consumer utility as compared to multi-attribute Vickrey's auction, Second-Score sealed bid auction and other standard pricing based resource selection mechanisms. But the only disadvantage lies in the fact that it has more computation and communication cost as compared to the other mechanisms.

Chapter 6

IBC Based Hash Chains for Secure Resource Selection in the Vehicular Cloud

6.1 Introduction

Vehicular cloud security design is major challenge due to it's widespread and autonomous nature. Using the well-known certificate-based public key infrastructure for vehicular authentication is highly cumbersome due to the certificate maintenance of the large number of entities. Instead identity-based cryptography which uses the identity of the entities as the public key is apt for vehicular networks [58]. Asymmetric key cryptography techniques like digital signature which can be performed using the identity based cryptography concept provides a higher degree of security with the major drawback of computation cost. Therefore we propose a lightweight hash chain mechanism called Hashcryption built on top of identity based encryption. This scheme ensures sender authentication and non-repudiation due to the unique property of hash functions as one way functions with cheap computation requirements.

The pricing-based resource selection protocols have various security requirements as elaborated in Chapter 2. Conditional privacy preservation is necessary since revealing the real identities and private sensitive information of these autonomous vehicles jeopardies their personal privacy. Hence ensuring authentication, non-repudiation, secrecy of messages becomes a challenge due to the anonymity of the network. We use pseudonymous identity concept for privacy preservation as well as satisfying the security requirements. A look-up table for these pseudonyms versus the real-identity is maintained by the Trusted Authority to blacklist the attackers and for payment and reputation updation purpose. All the proposed auction mechanisms in the previous chapters are sealed-bid auctions which require that the bidding values should be confidential between the consumer and that particular supplier vehicle while remaining a secret from the other competing suppliers for fair competition. Hence identity based cryptography schemes along with the proposed Hashcryption scheme is added to these protocols to satisfy the security requirements.

The organization of this chapter is as follows: In Section 6.2, three Identity-Based

Cryptography schemes, namely Identity Based Encryption, Signature and Signcryption schemes are discussed.Then, a Hashcryption scheme which uses the concept of Hash chains and built on top of Identity Based Cryptography is proposed in Section 6.3. In Section 6.4, the existing $2nd\_auc$, vik_auc and $1st\_auc$ mechanisms proposed in Chapter 3, 4 and 5 respectively are modified by adding the Hashcryption and other identity based cryptography scheme to satisfy the desired security requirements. Section 6.5 deals with the experimentation, security and computation analysis of the proposed Hashcryption scheme. Also the security analysis of the modified pricing-based resource selection protocols are done in that section. The chapter is finally summarised in Section 6.6.

6.2 Preliminaries

In this chapter, we use the concept of Identity-Based Cryptography to provide security while preserving privacy for the proposed pricing-based resource selection protocols $2nd\_auc$, vik_auc and $1st\_auc$ protocol. Initially we discuss an identity-based encryption scheme followed by an identity based signcryption scheme. Administrator is the entity who generates the public parameters and the keys to be used by the Trusted Authority in these schemes.

6.2.1 Identity Based Encryption

Boneh and Franklin proposed an encryption scheme based on identity-based cryptography which has the security of chosen ciphertext based on the assumption that Diffie-Hellman problem is hard which is as hard as the discrete logarithm problem [59]. This encryption mechanism uses the concept of bilinear pairing. They give Weil pairing over an elliptic curve as an example of this mapping [60]. Suppose there is one additive group G_{a1} and a multiplicative group G_{a2} defined over an elliptic curve E each having order q_a which is a large prime number. A bilinear mapping $\hat{e_a} : G_{a1} \times G_{a1} \longrightarrow G_{a2}$ is defined which has the following characteristics:

- Bilinear: A mapping is called bilinear if it satisfies the condition $\hat{e_a}(cX, dY) = \hat{e_a}(X, Y)^{cd} = \forall c, d \in Z_q^*, \forall X, Y \in G_{a1}$.
- Non-degenerate: P is the generator element of the group G_{a1} then $\hat{e_a}(P, P)$ is the generator element of the group G_{a2}.
- Computable: An efficient polynomial time algorithm exists for computing $\hat{e_a}(X, Y); \forall (X, Y) \in G_{a2}$

To avoid certificate management process, they proposed an encryption scheme with four algorithms:

- $Setup_a(k_a) \longrightarrow < param_a, s_a >$: As per the security parameter k_a given by the Administrator, this algorithm generates the master-secret key s_a for the Trusted

Authority, global parameters $param_a$ to be used in the proposed security protocol also consisting of the message space M and cipher space C. Given a positive integer k_a as an input parameter, select a large prime number p_a for defining a finite field $F_{pa} =< Z_{pa}, +, \times >$. An elliptic curve E_a over the finite field is defined as E_a/F_{pa} : $y^2 = x^3 + 1$. Two cyclic groups G_{a1} and G_{a2} of order q_a, are defined having P_a as a random generator where G_{a1} and G_{a2} are subgroups of E_a/F_{ap} and $F^*_{ap^2}$ respectively. $\hat{e_a} : G_{a1} \times G_{a1} \longrightarrow G_{a2}$ is a bilinear map. Here $q_a > 2^{k_a}$ is computed from above parameters and is a prime number.

1. $s_a \longleftarrow Z^*_{qa}$: A random integer s_a from Z^*_{qa} is chosen as the master secret key for the Trusted Authority.
2. $P_{tapub1} = s_a.P_a$: Computing $s_a.P_a$ gives the public-key of Trusted Authority which is also a point in the elliptic curve. The $param_a$ and it's constituents are:
   $param_a =< G_{a1}, G_{a2}, \hat{e_a}, ml, P_a, P_{tapub1}, H_{a1}, H_{a2}, M, C >$
   $H_{a1} : \{0,1\}^* \longrightarrow G^*_{a1}$
   $H_{a2} : G_{a2} \longrightarrow \{0,1\}^{ml}$
   $H_{a3} : \{0,1\}^{ml} \times \{0,1\}^{ml} \longrightarrow Z^*_{qa}$
   $H_{a4} : \{0,1\}^{ml} \longrightarrow \{0,1\}^{ml}$
   and $M = \{0,1\}^{ml}$, $C = G^*_1 \times \{0,1\}^{ml}$ where ml is the message length.

- $Extract_a(s_a, ID) \longrightarrow d_{aID}$: This algorithm is used by the Trusted Authority by using it's master-secret key s_a and the $param_a$ to compute the private key d_{aID} for a node having identity as ID.

  1. $Q_{aID} = H_{a1}(ID)$
     Using the hash function, it translates ID to a point in G^*_{a1}.
  2. $d_{aID} = s_a.Q_{aID}$
     It computes the private key d_{aID} which is also a point on the elliptic curve.

- $Encrypt_a(M, ID) \longrightarrow C$: A node can use the receiver's identity as public key for encryption and send to the receiver the message confidentially which can only be decrypted by receiver's private key. Let ID be the identity of the receiver. The following is the encryption process on receiving a message M:

  1. $Q_{aID} = H_{a1}(ID)$
  2. $\omega_a \in \{0,1\}^{ml}$ which is selected in a random manner.
  3. $t_a = H_{a3}(omega_a, M)$
  4. $C =< t_aP_a, \omega_a \oplus H_{a2}(g^{t_a}_{ID}), M \oplus H_{a4}(\omega) >$. Here $g^{t_a}_{ID} = \hat{e_a}(Q_{aID}, P_{tapub1})$ and C is the ciphertext.

- $Decrypt(C, d_{aID}) \longrightarrow M$: On receiving a message, a node uses it's private key as given by the TA to decrypt the message. Let $C =< U_a, V_a, W_a >$ be the ciphertext encrypted using the public key ID. We check that $U_a \notin G^*_{a1}$) otherwise we reject the ciphertext. Then we decrypt the message by doing the following steps:

  1. First we get $\omega_a = V \oplus H_{a2}(\hat{e_a}(d_{aID}, U_a))$.
  2. The original message M is decrypted as $W \oplus H_{a4}(\omega_a)$
  3. Then we get the t_a as $H_{a3}(\omega_a, M)$
  4. Finally we double check whether $U_a = t_a P_a$. In case the condition fails, we reject the ciphertext.

6.2.2 Identity Based Signature and Signcryption

Barreto proposed a light weight signature scheme and a combination of signature and encryption scheme based on identity-based cryptography [61]. It also possesses the security of chosen ciphertext based on the assumption that Diffie-Hellman problem. They use a slightly different version of bilinear pairing which was used by the identity based encryption process. Suppose the security requirement of the system is k_b. We choose a k_b bit prime number p_b and three groups G_{b1}, G_{b2} and G_{b3} all of order p_b. The generator element of G_{b1} is P_b and of G_{b2} is Q_b. A bilinear mapping $\hat{e_b} : G_{b1} \times G_{b2} \longrightarrow G_{b3}$ is defined which has the following characteristics:

- Bilinear:It is a bilinear mapping if $\hat{e_b}(cX, dY) = \hat{e_b}(X, Y)^{cd} = \forall c, d \in Z^*_q, \forall (X, Y) \in G_{b1} \times G_{b2}$.
- Non-degenerate: $\hat{e_b}(X, Y) = 1 \; \forall X \in G_{b1}$ and $\forall \; Y \in G_{b2}$ if and only if X is the identity element of the group G_{b1} and is the infinity point of the elliptic curve over which the group is defined.
- Computable: An efficient polynomial time algorithm exists for computing $\hat{e_b}(X, Y); \forall (X, Y) \in G_{b3}$
- Isomorphism: A publicly computable and efficient isomorphic function which may or may not be invertible is declared such that $\psi : G_{b2} \longrightarrow G_{b1}$. where $\psi(Q_b) = P_b$.

Identity Based Signature Scheme

Initially we discuss the signature scheme proposed which consists of four algorithms:

- $Setup_b(k_b) \longrightarrow < \; param_b, s_b \; >$: As per the security parameter k_b given by the Administrator, this algorithm generates the master-secret key s_b for the Trusted Authority, global parameters $param_b$ to be used in the proposed security. The Administrator chooses bilinear map groups G_{b1}, G_{b2} and G_{b3} and the generator

elements P_b of G_{b1} and Q_b of G_{b2} as explained previously. The groups G_{b1}, G_{b2} are chosen such that they have isomorphism property. Then determination of $g_b = \hat{e_b}(P_b, Q_b)$ is done to express in the public parameter list.

1. $s_b \longleftarrow Z^*_{pb}$: A random integer s_b from Z^*_{pb} is chosen as the master secret key for the Trusted Authority
2. Now we choose the public key for the TA as $Q_{pub2} = s_b.Q_b$. The public parameter list as denoted by The public parameters are $param_b =< G_{b1}, G_{b2}, G_{b3}, P_b, Q_b, g_b, Q_{pub2}, \hat{e_b}, \psi, H_{b1}, H_{b2}, H_{b3} >$. The hash functions are
   $H_{b1} : \{0,1\}^* \longrightarrow Z^*_{pb}$
   $H_{b2} : \{0,1\}^* \times G_{b3} \longrightarrow Z^*_{pb}$
   $H_{b3} : G_{b3} \longrightarrow \{0,1\}^{ml}$are chosen where ml is the message length.

- $Keygen_b(s_b, ID) \longrightarrow S_{bID1}$ When an identity is provided to the Trusted Authority, it determines the private key of the node with identity ID as: $S_{bID1} = \dfrac{1}{H_{b1}(ID) + s_b}.P_b$
- $Sign_b(M, S_{bID1}) \longrightarrow \Phi$: A node uses it's private key S_{bID1} in order to generate a signature from a message $M \in \{0,1\}^*$ as $\Phi =< h_b, S_{b2} >$
  1. $t_b \longleftarrow Z^*_{pb}$. Initially it chooses a random number.
  2. It generates $m_b = g_b^{t_b}$
  3. A hash value h_b of the message with m_b is determined as $H_{b2}(M, m_b)$
  4. Using it's private key, it generates the second constituent of the signature $S_{b2} = (t_b + h_b)S_{bID1}$
- $Verify(M, \Phi) \longrightarrow (Accept/Reject)$ Another node on receiving message M and the signature on the message as h_b, S_{b2}, who wants to authenticate it, uses the private key of the sender. it verifies if
  $h_b = H_{b2}(M, \hat{e_b}(S_{b2}, H_{b1}(ID)Q_b + Q_{pub2})g^{-h_b})$

Identity Based Signcryption Scheme

The $Setup_b(k_b) \longrightarrow < param_b, s_b >$ is same as in Identity-Based Signature Scheme in the previous section.

- $Extract_b(s_b, ID) \longrightarrow S_{bID2}$: When an identity is provided to the Trusted Authority, it determines the private key of the node with identity ID as: $S_{bID2} = \dfrac{1}{H_{b1}(ID) + s_b}.P_b$
- $Signcrypt_b(M, ID_R, S_{bID2}) \longrightarrow (C_b)$ When the sender with identity ID wants to send a message M to the receiver with identity ID_R, it encrypts the message with the receiver's public key and signs it with his private key S_{bID2}. The ciphertext obtained is $C_b =< c_b, S_{b2}, T_{b2} >$

1. Initially it chooses a random number as $t_b \longleftarrow Z^*_{pb}$.
2. It generates $m_b = g_b^{t_b}$
3. $c_b = M \oplus H_{b3}(m_b) \in \{0,1\}^{ml}$is calculated.
4. A hash value h_b of the message with m_b is determined as $H_{b2}(M, m_b)$
5. Using it's private key, it generates the second constituent of the signature $S_{b2} = (t_b + h_b)\psi(S_{bID1})$
6. The last element of the ciphertext $T_{b2} = t_b(H_{b1}(ID_R).P_b + \psi(Q_{pub2}))$

- $Vericrypt(C_b, ID, S_{bIDR2}) \longrightarrow (M, Accept/Reject)$: Here S_{bIDR2} is the private key of the receiver node. The message is verified and decrypted by the receiver as:
  1. m_b is calculated as $\hat{e_b}(T_{b2}, S_{bIDR2})g_b^{t_b}$
  2. The message M is decrypted as $c_b \oplus H_{b3}(m_b)$
  3. $h_b = H_{b2}(M, m_b)$ is the hashed value calculated for verifying the signature.
  4. The message M is accepted iff $m_b = \hat{e_b}(S_b, H_{b1}(ID).Q_b + Q_{pub2})g_b^{-h_b}$

6.3 IBC Based Hash Chains for Light Weight Authentication

In this section, we propose a hash chain mechanism (Hashcryption) built on top of identity based cryptography schemes as discussed in the previous section for authentication without using digital signatures. Suppose there are entities A and B who communicate via message passing consecutively for a long time. We define a Hash function $H_{c1} : \{0,1\}^* \longrightarrow \{0,1\}^*$ which is known to both A and B.

1. $hash\_gen() \longrightarrow hash\_chain$: This algorithm generates a $hash\_chain$ of length spl which is more than the number of messages to be passed between the entities. We assume the sender entity A has knowledge of the value of spl.
   - The entity choses a random value $IV \longleftarrow \{0,1\}^*$.
   - It generates $hash\_chain = \{H^1, H^2, ..., H^{spl}\}$ where $H^1 = H_{c1}(IV)$, $H^2 = H_{c1}(H^1)$,... , $H^{spl} = H_{c1}(spl - 1)$
2. $Signcrypt_b(H^{spl}, ID_B, S_{IDA2})) \longleftarrow (C_{HA})$ The entity A having identity ID_A signs and encrypts the last element of $hash\_chain$ using its private key S_{IDA2} and the identity of the receiver ID_B as the public key.
   $A \longrightarrow B : C_{HA}$. Sender A then sends the ciphertext to the receiver B.

3. $Vericrypt(C_{HA}, ID, S_{bIDR2}) \longrightarrow (Accept/Reject, H^{spl})$: On receiving the ciphertext, first the receiver B decrypts and verifies the message and stores the value of H^{spl} for future authentication purpose.

4. $Hashencrypt(M_1, H^{spl-1}, ID_B) \longrightarrow C_1$: Suppose the message passing phase starts and A has to send the first confidential message M_1 to B. It first concatenates the message M_1 with the previous hash value H^{spl-1} to generate $M_1^{'} =< M_1, H^{spl-1} >$. It then encrypts $M_1^{'}$ as $Encrypt_a(M_1^{'}, ID_B)$ to create C_1. Finally it sends the ciphertext C_1 to entity B.

5. $Hashdecrypt(C_1, H^{spl}, d_{aIDB}) \longrightarrow (M_1, Accept/Reject)$ After receiving the ciphertext $C_1^{'}$, B decrypts C_1 to get $M_1^{'}$ using it's private key as $Decrypt(C_1, d_{aIDB}) \longrightarrow M_1^{'}$. It then verifies whether $H_{c1}(H^{spl-1}) = H^{spl}$. If the condition is satisfied the message is accepted since it comes from an authenticated source.

For the subsequent message passing, the sender A sends the previous element of the $hash\_chain$ H^{spl-2} which is followed by H^{spl-3} and the similar pattern continues. At the receiver end, the entity B performs hash operation on the new value received and if that matches the hash value obtained through the previous message, it accepts the current message.

6.4 Secure Pricing-Based Resource Selection Protocols

Initially the vehicular cloud network is setup by the TA by generating the public parameters for all the vehicles and it's own master-secret keys. Suppose the security requirement of the system is k. Initially the TA uses $Setup_a(k)$ and $Setup_b(k_b)$ as described in Section 6.2.1 to generate two set of public parameter lists $param_a$ and $param_b$ which is announced in the system for the knowledge of all consumer and supplier vehicles. Along with it two master-secret keys s_a and s_b are generated for it's own use for generating the private keys of the registered vehicles whenever required.

Suppose the vehicle V requests the TA for pseudonymous and key pairs generation.

1. TA creates a set of pseudonym pid from the real identity of the vehicle, preferably by use of a hash function, each equipped with a time-stamp t_{pid} which denotes the expiry time of that pseudonymous identity. A pseudonymous identity is denoted as $ID =< pid, t_{pid} >$. The TA maintains a lookup table where it stores the real identities of the vehicles with their pseudonymous identity list.

2. For each pseudonymous identity ID, the TA uses $Extract_a(s_a, ID)$ to generate d_{aID} which is the private key to be used for message encryption purpose. It also produces

the private key S_{bID1} for signing messages by applying $Keygen_b(s_b, ID)$. Finally, it creates the third private key S_{bID2} for signcryption purpose using $Extract_b(s_b, ID)$.

3. It sends to the vehicle the list of pseudonymous identities and the private keys attached with each identity $< ID, d_{aID}S_{bID1}, S_{bID2} >$

We use two more algorithms to get the freshness of pseudonymous identities and the message:

- $pid\_fresh(ID) \longrightarrow (Accept/Reject)$: When a vehicle A with identity ID initially tries to communicate with another vehicle B, the receiver vehicle B checks if $t_{pid} > t_{cur} + t_{com}$ where t_{cur} is the current time and t_{com} is the communication time of A and B. The communication request is accepted only if the condition is satisfied. We assume that both the entities have knowledge of t_{com}.

- $msg\_fresh(M, t_M) \longrightarrow (Accept/Reject)$: Every message M is associated with a timestamp t_M, which can not be tampered. When a message $M^{'} =< M, t_M >$ is received by an entity, it checks if $t_M + t_{ft} > t_{cur}$. The message is accepted only when the condition is satisfied. Here t_{ft} is the time for which the message remains fresh after which it should be discarded and is constant for all entities.

In the subsequent sections we assume that the pseudonymous identity used by the consumer vehicle V_c is id_{Vc} and the associated private keys are d_{ac}, S_{bc1} and S_{bc2}. For the supplier vehicle V_{sj}, we assume the identity to be id_{Vsj} and the corresponding private keys as d_{asj}, S_{bsj1} and S_{bsj2}. Now we discuss three secure pricing-based resource selection protocols, namely $2nd\_auc$, vik_auc and $1st\_auc$ protocol.

6.4.1 Secure Second-Score Auction

Here the consumer vehicle wants to rent the entire resources of N supplier vehicles by using the $2nd\_auc$ protocol. The details of each message is described in Section 3.4.

1. $V_c \rightarrow * :< M_1^4 || t_1^4, \Phi_1^4 >$ The consumer vehicle generates a service availability message M_1^4, a timestamp t_1^4 and creates a signature it as $Sign_b(M_1^4 || t_1^4, S_{bc1}) \longrightarrow \Phi_1^4$.

2. $V_{sj} : Verify(M_1^4 || t_1^4, \Phi_1^4) \longrightarrow (Accept/Reject)$. The supplier vehicles first verifies the message if it has been actually signed by an authenticated consumer vehicle. It then checks the freshness of the message by $msg\_fresh(M_1^4, t_1^4) \longrightarrow (Accept/Reject)$. Then it checks the freshness of the pseudonymous identity used by the consumer vehicle by $pid\_fresh(id_{Vc}) \longrightarrow (Accept/Reject)$ to decide whether it will participate in resource provisioning.

3. $V_{sj} \rightarrow V_c : C_{2sj}^4$ All the interested supplier vehicles signcrypt service availability reply message M_{2sj}^4 containing their private value θ_j and last hash chain value

which has to remain confidential. The supplier vehicles generate a hash chain using $hash\_gen()$ and $hash\_chain^1 = \{H_1^1, H_1^2, ..., H_1^{spl}\}$ and attach the last element of the chain H_1^{spl} to the message.It signs the entire message using $Signcrypt_b(M_{2sj}^4||H_1^{spl}||t_{2sj}^4, id_{Vc}, S_{bsj2}) \longrightarrow (C_{2sj}^4)$

4. V_c: $Vericrypt(C_{2sj}^4, id_{Vsj}, S_{bc2}) \longrightarrow (M_{2sj}^4||H_1^{spl}||t_{2sj}^4, Accept/Reject)$ makes the consumer vehicle to decrypt and verify the authentication of the message. It checks the freshness of the message using $msg\_fresh(M_{2sj}^4||H_1^{spl}, t_{2sj}^4) \longrightarrow (Accept/Reject)$.Then it checks the freshness of the pseudonymous identity of the supplier vehicle V_{sj} by $pid\_fresh(id_{Vsj}) \longrightarrow (Accept/Reject)$. Finally, the consumer vehicle segregates the suppliers moving in it's direction by dir_check$(n^{'}, msg_lst^{'}, dir_{Vc}) \rightarrow (msg_list, egl_list, n)$ to create egl_list of n eligible supplier vehicles. It stores the initial hash values of the eligible suppliers H_1^{spl}.

5. V_c →TA:< $M_3^4||t_3^4, \Phi_3^4$ > sign the reputation request message along with it's timestamp $Sign_b(M_3^4||t_3^4, S_{bc1}) \longrightarrow \Phi_3^4$

6. TA: $Verify_b(M_3^4||t_3^4, \Phi_3^4) \longrightarrow (Accept/Reject)$ It verifies the authenticity of the message and then checks the freshness by $msg\_fresh(M_3^4, t_3^4)$. Finally it encrypts the reputation list of the eligible suppliers as $Encrypt_a(Rep\_list, id_{Vc}) \longrightarrow C_{rep}$ since it has to remain confidential.

7. TA $\longrightarrow$ V_c : C_{rep} : The consumer vehicle finds the original Rep_list by $Decrypt(C_{rep}, d_{ac})$. It performs second score auction by second_score_sel$(n, N, \alpha, msg_lst, Rep_list) \rightarrow win_list$ to generate the winner list and the price that will be provided to each winner. It generates a series of hash chains $hash\_chain^{w1}, hash\_chain^{w2}, ..., hash\_chain^{wN}$ for $Nwinners$. It signcrypts the last element of each hash chain $H_{w1}^{spl}, H_{w2}^{spl}, ..., H_{wN}^{spl}$ by concatenating it with the timestamp t_{Hj} and sends it to the individual winner suppliers by $Signcrypt_b(id_{Vc}||H_{wj}^{spl}||t_{Hj}, V_{sj}, S_{bc2}) \longrightarrow (C_{Hj})$ where $j \in$1,N.

8. $V_c \longleftarrow V_{sj} : C_{Hj}$ The supplier vehicle first performs $Vericrypt(C_{Hj}, id_{Vc}, S_{bsj2})$ and then checks message freshness by $msg\_fresh(H_{wj}^{spl}, t_{Hj})$ and stores H_{wj}^{spl}.

9. $V_c \leftrightarrow V_{sj}$: service_provision. Suppose V_c wants to send the first message M_{sp1} to V_{sj}. It uses $Hashencrypt(M_{sp1}, H_{wj}^{spl-1}, id_{Vsj})$ to create ciphertext C_{sp1} and sends it to V_{sj}. Then V_{sj} performs $Hashdecrypt(C_{sp1}, H_{wj}^{spl}, d_{asj})$ to decrypt and verify the authentication of the message M_{sp1}. Next if V_{sj} wants to send M_{sp2} to V_c, it performs $Hashencrypt(M_{sp2}, H_1^{spl-1}, id_{Vc})$ to send C_{sp2} to V_c. Finally the consumer vehicle performs $Hashdecrypt(C_{sp2}, H_1^{spl}, d_{ac})$ to decrypt and verify the authentication of the message.

10. V_c →TA: Φ_5^4 The consumer signs V_c →TA:$< M_5^4||t_5^4, \Phi_5^4 >$ sign the message containing the list of suppliers who successfully provided service along with it's timestamp by $Sign_b(M_5^4||t_5^4, S_{bc1}) \longrightarrow \Phi_5^4$. Finally TA $Verify_b(M_5^4||t_5^4, \Phi_5^4) \longrightarrow (Accept/Reject)$. It verifies the authenticity of the message and then checks the freshness by $msg\_fresh(M_5^4, t_5^4)$.

The last phase occurs in the same way as in Section 3.4 without using any security mechanism.

6.4.2 Secure multi-attribute Vickrey's Auction

We apply the security mechanisms on the Vickrey's Auction elaborated in Section 4.3. The security mechanisms applied are quite similar to the previous secure second-score mechanism. Only in the step 3 of the previous mechanism, the supplier vehicles calculate the optimal quality and pricing value and encrypt it instead of their private cost θ_j. Also in step 7, the consumer vehicle uses the selection algorithm for Vickrey's Auction vik_score_sel in Algorithm 7 instead of using second_score_sel.

6.4.3 Secure first-score sealed bid auction

The first-score sealed bid auction has been elaborated properly in Section 5.3. Now, we apply some identity-based security schemes to the protocol.

1. $V_c \rightarrow * :< M_1^6||t_1^6, \Phi_1^6 >$ Similar to the first step of Section 6..1, the consumer vehicle generates a service availability message M_1^6, a timestamp t_1^6 and creates a signature it as $Sign_b(M_1^6||t_1^6, S_{bc1}) \longrightarrow \Phi_1^6$.

2. V_{sj} : $Verify(M_1^6||t_1^6, \Phi_1^6) \longrightarrow (Accept/Reject)$. The supplier vehicles first verifies the message if it has been actually signed by an authenticated consumer vehicle. It then checks the freshness of the message by $msg\_fresh(M_1^4, t_1^4) \longrightarrow (Accept/Reject)$. Then it checks the freshness of the pseudonymous identity used by the consumer vehicle by $pid\_fresh(id_{Vc}) \longrightarrow (Accept/Reject)$ to decide whether it will participate in resource provisioning. It then sends $V_{sj} \rightarrow V_c :< M_{2j}^6||t_{2j}^6, \Phi_{2j}^6 >$ All the interested supplier vehicles sign service availability reply message using $Sign_b(M_{2sj}^6||t_{2sj}^6, S_{bsj2}) \longrightarrow (\Phi_{2j}^6)$

3. V_c: $Verify(M_{2sj}^6||t_{2sj}^6, \Phi_{2j}^6) \longrightarrow (Accept/Reject)$ consumer vehicle to verify the authentication of the message and checks the freshness of the message using $msg\_fresh(M_{2sj}^6, t_{2sj}^6)$. Then it checks the freshness of the pseudonymous identity of the supplier vehicle V_{sj} by $pid\_fresh(id_{Vsj})$. Finally, the consumer vehicle segregates the suppliers moving in it's direction by dir_check$(n', msg_lst', dir_{Vc}) \rightarrow (msg_list, egl_list, n)$. It determines optimal quality weights to declare by qual_pref _calc$(dsbn, \underline{\theta}, \tilde{\theta}, org_qual_req, n, \mu, \sigma) \rightarrow qual_req$.

4. $V_c \rightarrow * :< M_3^6||t_3^6, \Phi_3^6 >$ The consumer vehicle signs and broadcasts the optimal quality preference list along with the number of eligible suppliers as $Sign_b(M_3^6||t_3^6, S_{bc1}) \longrightarrow \Phi_3^6$.

5. $V_{sj} : Verify(M_3^6||t_3^6, \Phi_3^6) \longrightarrow (Accept/Reject)$. The supplier vehicles first verifies the message if it has been actually signed by an authenticated consumer vehicle. It then checks the freshness of the message by $msg\_fresh(M_3^6, t_3^6)$ It calculates the optimal quality to bid as qual_firstprice_calc$(dsbn, qual_req, \theta_j, cost_coef, n, \mu, \sigma) \rightarrow (qual_prov, p_j)$.

6. $V_{sj} \rightarrow V_c : C_{4sj}^6$ All the interested supplier vehicles signcrypt quality and price bidding message M_{4sj}^6 containing and last hash chain value by $Signcrypt_b(M_{4sj}^6||H_1^{spl}||t_{4sj}^6, id_{Vc}, S_{bsj2}) \longrightarrow (C_{4sj}^6)$ similar to step 3 of Section 6.4.1.

7. In the mean while the consumer vehicle requests for the reputation list from the TA and receives it similar to Step 5 and 6 of Section 6.4.1.

8. $V_{sj} \rightarrow V_c : C_{4sj}^6$ After the consumer receives the bids from the supplier vehicles, it performs $Vericrypt(C_{4sj}^6, id_{Vsj}, S_{bc2}) \longrightarrow (M_{4sj}^6||H_1^{spl}||t_{2sj}^4, Accept/Reject)$ It checks the freshness of the message using $msg\_fresh(M_{4sj}^6||H_1^{spl}, t_{4sj}^6)$. It stores the initial hash values of the eligible suppliers H_1^{spl}. It performs first_auc_sel$(n, N, \alpha, qual_req, msg_lst, Rep_list) \rightarrow win_list$ to generate winner list. Then it follows the Step 7 of Section 6.4.1 from hash chain generation scheme.

Step 8 and 9 of Section 6.4.1 is followed for service provisioning. In Step 10, the message M_7^6 from Section 4.3 is used in place of M_5^4 which contains three lists of suppliers. The last phase of payment and reputation transfer doesn't require any security mechanism.

6.5 Experimentation and Analysis

Here we perform formal verification of Hashcryption scheme and computationally compare it with Signcryption scheme. Also we analyse the security of protocols proposed in Section 6.4.

6.5.1 Formal Verification of Hashcryption Scheme

We use the AVISPA (Automated Validation of Internet Security Protocols and Applications) tool for the cryptanalysis $hashcryption$ scheme [62]. We want the service provisioning messages to be confidential and from authenticated sources. Message passing was done between two entities as per Section 6.3. Figure 6.1 and 6.2 show that the scheme is safe and both message secrecy and authentication is achieved for OFMC model checker and CL-ATSE protocol analyzer mode.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/amtprt1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
```

Figure 6.1: Safe state for OFMC model checker

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/amtprt1.if

GOAL
  As Specified

BACKEND
  CL-AtSe
```

Figure 6.2: Safe state for CL-ATSE protocol analyser

6.5.2 Computational efficiency of Hashcryption scheme

Table 6.1 shows the computational requirement of the proposed Hashcryption scheme with respect to the existing Signcryption scheme. Hashencryption and Hashdecryption is cheaper than Signcryption and Vericryption scheme if we consider the timing values from [63]. They show that T_{exp}, T_{iso}, T_{blp} and T_{mtp} have similar timing requirement which is equal to $4T_{mul}$, $40T_{add}$ and $40000T_h$. So T_h is ignored since it's value is negligible. Hashencrypt takes $130T_{add}$ as compared to $241T_{add}$ requirement of Signcrypt. Hashdecrypt takes $50T_{add}$ as compared to $181T_{add}$ Vericrypt requirement.

6.5.3 Security Analysis of Pricing-Based Resource Selection Protocols

The security requirements for the pricing-based resource selection mechanism that are satisfied by the proposed protocols in Section 6.4 are:

Scheme	Sign/Hashencrypt	Veri/Hashdecrypt
Signcryption	$T_{exp} + 2T_{mul} + T_{add} + 2T_{iso} + 3T_h$	$2T_{exp} + 2T_{mul} + T_{add} + 2T_{blp} + 3T_h + T_{exp}$
Hashcryption	$T_{exp} + T_{mul} + T_{mtp} + T_{blp} + 3T_h$	$T_{mul} + T_{blp} + 4T_h$

Table 6.1: Computational analysis of Hashcryption

1. Privacy preservation of vehicles: The vehicles use the pseudonymous identities for authentication, message secrecy and other security purposes without revealing sensitive personal information about the vehicles. Thus conditional privacy preservation is achieved for the vehicles [36].

2. Traceability of vehicles: The TA stores the real identities of the vehicles along with their pseudonymous identities in a lookup table. Despite of privacy preservation property, any required vehicle can be traced by TA. This is important for identify and blacklist attackers and other malicious vehicles. Also monetary transfer from consumer to supplier vehicles and reputation maintenance requires the real identity of the vehicles which can be achieved by this traceability property.

3. Ensuring message confidentiality: In the pricing-based resource selection mechanism, message containing the quality and price of the service which is sent which is the private information of the vehicle. Since it is sent in encrypted form, other supplier vehicles can't determine the price and quality bidding value so as to have advantage in the market.

4. Prevention of replay attacks: Since every message is attached with a timestamp and at the receiver end, the message freshness is checked before accepting it, replay attack by the vehicles is not possible.

5. Prevention of message tampering: All the messages which reflect the quality of service parameters to be provided and the final payment value is signed. Providing message integrity is an important feature of digital signature. Both the consumer and supplier vehicles have copies of these contract message. Suppose the receiver wants to tamper with the message for his profit. Since it doesn't have the private key of the sender, it can't sign the tampered message which will ultimately have no value. Similarly, after sender the original signed message if the sender creates another message for it's profit and signs it, the receiver will oppose showing it's copy of the old message and hence the new message will not be accepted by the authority.

6. Sender Authentication and non-repudiation: All the message in the system are authenticated either by Signature scheme or Hashcryption scheme. They use the private key sender which is generated only by TA using it's master-secret key. Hence all the messages come from authenticated vehicles and no impersonation attack is possible in the system. Sender non-repudiation is an important property of digital signature which is satisfied by all the messages that are signed using the Signcryption scheme. For Hashcryption scheme, the first hash value is signed by the sender. Suppose after sending the subsequent new message, sender vehicle denies the responsibility of not sending the new message. The receiver can prove that hashing

the value in new message yields the previous value which is already signed. Since hash is a one-way function, the receiver can't obtain the reverse hash value. Therefore sender non-repudiation is also achieved for Hashcryption scheme.

6.6 Summary

In this chapter, we propose Hashcryption scheme and then use cryptography mechanisms to secure the $2nd\_auc$, vik_auc and $1st\_auc$ protocol proposed in Chapter 3, 4 and 5 as per requirements. Initially three Identity-Based Cryptography schemes are discussed. Then, the Hashcryption scheme which uses the concept of Hash chains and built on top of identity based encryption and Signcryption scheme is elaborated. To ensure message authentication, secrecy, prevention of message tampering and other security purposes, identity based encryption, signature, Signcryption and Hashcryption are performed on the messages passed during $2nd\_auc$, vik_auc and $1st\_auc$ mechanisms for resource selection purpose. A formal verification of the proposed Hashcryption scheme using AVISPA tool is carried out. We also show that Hashcryption scheme is computationally efficient than Signcryption scheme. Finally, a detailed security analysis of the modified $2nd\_auc$, vik_auc and $1st\_auc$ protocol shows that they satisfy the security requirements as presented in Chapter 2 of this research work.

Chapter 7

Conclusion

This work aims to address the resource selection problem in the Vehicular Cloud. Initially, the concept of the Vehicular Cloud is introduced along with its application areas and open issues. The architecture of the Vehicular Cloud, its subdivision based on mobility and the entity providing the service is elaborated. We take up the Vehicular Cloud resource selection problem due to its intricate nature. It is highly dependent on resource pricing, trustworthiness of vehicular suppliers, quality of services provided, market demand and has various security requirement. In addition, the pricing of resources in vehicular cloud is addressed as a subproblem taking into account the market demand before concentrating on the resource selection problem. Therefore, our research problem is formulated as designing a secure pricing-based resource selection mechanism for utility maximization in the Vehicular Cloud.

We design the utility,cost and valuations functions of the consumer and the supplier vehicles. A second-score sealed bid auction is proposed for addressing the resource selection problem in the vehicular cloud. Here, the quality of service parameter is relaxed and the entire resource unit is provided by the supplier vehicle to the consumer vehicle. It helps the supplier vehicles to determine the optimal price to bid for obtaining the desirable profit without decreasing it's probability of winning. This bidding price was proved to be a dominant strategy. The winner selection problem for the consumer vehicles was also solved using a scoring function. Three standard pricing-based resource selection methodologies, namely fixed-price distance based selection, random-pricing distance based selection and minimum random-pricing selection were elaborated to be used in future for comparison purpose. Another auction mechanism called multi-attribute Vickrey's auction was also proposed which takes the quality of services into account in contrast to the previously proposed second-score sealed bid auction. The third mechanism called first-price sealed bid auction takes the market demand as the topmost priority factor for addressing the resource pricing and selection. A comprehensive experimentation proved that the first-price sealed bid auction yields better utility for the consumer vehicles as compared to the previously proposed mechanisms. However higher computation and communication cost is it's drawback. Also, these protocols are highly insecure and authentication of participating vehicles, confidentiality of sealed bid messages, privacy preservation of the vehicles, and integrity of the messages negotiated pricing and quality have to be addressed.

Finally a weight hash chain mechanism called Hashcryption built on the top of Identity-Based Cryptography techniques is proposed for sender authentication in case of confidential messages. It is found to be computationally efficient as compared to the other signature-based encryption scheme. Identity-Based Cryptography schemes along with the Hashcryption technique is added to the proposed auction protocols and the analysis shows that they satisfy the security requirements.

Chapter 8

Future Work

This research work has certain limitations which can be addressed in future. Some of them are briefly explained below:

1. While proposing solution mechanisms, we have only considered a single consumer and multiple suppliers scenario. This can be rectified to provide solution mechanisms in cases where there are multiple consumers and suppliers as in proper markets.

2. Service availability ratio of the Vehicular Cloud and the latency of its formation can also be considered. Also, the mechanisms to determine the number of resources required by the consumers as per its needs have to be considered.

3. Optimal task division issue has to be taken into consideration in the service provisioning phase for maximizing reward of the system. When virtualization is done in the service provisioning phase, the number of virtual machine migration overhead is another factor that has to be taken into account. Additionally, service provisioning phase of the Vehicular Cloud has not been fully exploited yet which has a future scope.

4. Finally other issues related to the Vehicular Cloud like designing a standardized Vehicular Cloud architecture, increasing information quality by sensing and aggregation of vehicular data and removing redundancy in vehicular information and exploiting the field of green vehicular computing has a future scope.

References

[1] Eltoweissy, M., Olariu, S., and Younis, M., 2010. "Towards autonomous vehicular clouds". In International Conference on Ad Hoc Networks, Springer, pp. 1–16.

[2] Whaiduzzaman, M., Sookhak, M., Gani, A., and Buyya, R., 2014. "A survey on vehicular cloud computing". *Journal of Network and Computer Applications,* **40**, pp. 325–344.

[3] Jeong, J., Jeong, H., Lee, E., Oh, T., and Du, D. H., 2016. "Saint: Self-adaptive interactive navigation tool for cloud-based vehicular traffic optimization". *IEEE Transactions on Vehicular Technology,* **65**(6), pp. 4053–4067.

[4] Kumar, N., Lee, J.-H., Chilamkurti, N., and Vinel, A., 2016. "Energy-efficient multimedia data dissemination in vehicular clouds: stochastic-reward-nets-based coalition game approach". *IEEE Systems Journal,* **10**(2), pp. 847–858.

[5] Arif, S., Olariu, S., Wang, J., Yan, G., Yang, W., and Khalil, I., 2012. "Datacenter at the airport: Reasoning about time-dependent parking lot occupancy". *IEEE Transactions on Parallel and Distributed Systems,* **23**(11), pp. 2067–2080.

[6] Abdelhamid, S., Hassanein, H., and Takahara, G., 2015. "Vehicle as a resource (vaar)". *IEEE Network,* **29**(1), pp. 12–17.

[7] Fleming, W. J., 2008. "New automotive sensors—a review". *IEEE Sensors Journal,* **8**(11), pp. 1900–1921.

[8] SINTRONES Technology Corporation. In-vehicle computer. `http://www.sintrones.com/in-vehicle-computer.html`. [Online; accessed 2-April-2018].

[9] Intel Corporation. CPU Power. `https://ark.intel.com/products/97462/Intel-Core-i7-7920HQ-Processor-8M-Cache-up-to-4_10-GHz`. [Online; accessed 2-April-2018].

[10] Nvidia Corporation. GPU Power. `https://www.nvidia.com/en-us/geforce/products/10series/geforce-gtx-1050`. [Online; accessed 2-April-2018].

[11] Eichler, S., 2007. "Performance evaluation of the ieee 802.11 p wave communication standard". In Vehicular Technology Conference, 2007. VTC-2007 Fall. 2007 IEEE 66th, IEEE, pp. 2199–2203.

[12] Jiang, D., and Delgrossi, L., 2008. "Ieee 802.11 p: Towards an international standard for wireless access in vehicular environments". In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, IEEE, pp. 2036–2040.

[13] Kenney, J. B., 2011. "Dedicated short-range communications (dsrc) standards in the united states". *Proceedings of the IEEE,* **99**(7), pp. 1162–1182.

[14] Wikipedia contributors, 2013. Communications, air-interface, long and medium range — wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Communications,_Air-interface,_Long_and_Medium_range&oldid=568175561`. [Online; accessed 2-April-2018].

[15] Ghazizadeh, P., Florin, R., Zadeh, A. G., and Olariu, S., 2016. "Reasoning about mean time to failure in vehicular clouds". *IEEE Transactions on Intelligent Transportation Systems,* **17**(3), pp. 751–761.

[16] Gupte, S., and Younis, M., 2012. "Vehicular networking for intelligent and autonomous traffic management". In Communications (ICC), 2012 IEEE International Conference on, IEEE, pp. 5306–5310.

[17] Liu, B., Jia, D., Wang, J., Lu, K., and Wu, L., 2017. "Cloud-assisted safety message dissemination in vanet–cellular heterogeneous wireless network". *ieee systems journal,* **11**(1), pp. 128–139.

[18] Gerla, M., 2012. "Vehicular cloud computing". In Ad Hoc Networking Workshop (Med-Hoc-Net), 2012 The 11th Annual Mediterranean, IEEE, pp. 152–155.

[19] Gerla, M., Lee, E.-K., Pau, G., and Lee, U., 2014. "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds". In Internet of Things (WF-IoT), 2014 IEEE World Forum on, IEEE, pp. 241–246.

[20] Bitam, S., Mellouk, A., and Zeadally, S., 2015. "Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks". *IEEE Wireless Communications,* **22**(1), pp. 96–102.

[21] Mell, P., Grance, T., et al., 2011. "The nist definition of cloud computing".

[22] Hussain, R., Son, J., Eun, H., Kim, S., and Oh, H., 2012. "Rethinking vehicular communications: Merging vanet with cloud computing". In Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on, IEEE, pp. 606–609.

[23] Zheng, K., Meng, H., Chatzimisios, P., Lei, L., and Shen, X., 2015. "An smdp-based resource allocation in vehicular cloud computing systems". *IEEE Transactions on Industrial Electronics,* **62**(12), pp. 7920–7928.

[24] Wikipedia contributors, 2018. Quality of service — wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Quality_of_service&oldid=831211959`. [Online; accessed 2-April-2018].

[25] Ardagna, D., Casale, G., Ciavotta, M., Pérez, J. F., and Wang, W., 2014. "Quality-of-service in cloud computing: modeling techniques and their applications". *Journal of Internet Services and Applications,* **5**(1), p. 11.

[26] Aloqaily, M., 2016. "User experience-based provisioning services in vehicular clouds". PhD thesis, Université d'Ottawa/University of Ottawa.

[27] Lai, C., Zhang, K., Cheng, N., Li, H., and Shen, X., 2017. "Sirc: A secure incentive scheme for reliable cooperative downloading in highway vanets". *IEEE Transactions on Intelligent Transportation Systems,* **18**(6), pp. 1559–1574.

[28] Haddadou, N., and Rachedi, A., 2013. "Dtm 2: Adapting job market signaling for distributed trust management in vehicular ad hoc networks". In Communications (ICC), 2013 IEEE International Conference on, IEEE, pp. 1827–1832.

[29] Wikipedia contributors, 2018. Pricing — wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Pricing&oldid=831477797`. [Online; accessed 2-April-2018].

[30] Henry Hazlitt - FEE Foundation for Economic Education, 2018. How should prices be determined? `https://fee.org/articles/how-should-prices-be-determined/`. [Online; accessed 2-April-2018].

[31] Al-Roomi, M., Al-Ebrahim, S., Buqrais, S., and Ahmad, I., 2013. "Cloud computing pricing models: a survey". *International Journal of Grid and Distributed Computing,* **6**(5), pp. 93–106.

[32] Mershad, K., and Artail, H., 2013. "Finding a star in a vehicular cloud". *IEEE Intelligent transportation systems magazine,* **5**(2), pp. 55–68.

[33] Brik, B., Lagraa, N., Lakas, A., and Ghamri-Doudane, Y., 2015. "Rcs-vc: Renting out and consuming services in vehicular clouds based on lte-a". In Global Information Infrastructure and Networking Symposium (GIIS), 2015, IEEE, pp. 1–6.

[34] Kong, Q., Lu, R., Zhu, H., Alamer, A., and Lin, X., 2016. "A secure and privacy-preserving incentive framework for vehicular cloud on the road". In Global Communications Conference (GLOBECOM), 2016 IEEE, IEEE, pp. 1–6.

[35] Raya, M., Papadimitratos, P., and Hubaux, J.-P., 2006. "Securing vehicular communications". *IEEE wireless communications,* **13**(5).

[36] Lin, X., Lu, R., Zhang, C., Zhu, H., Ho, P.-H., and Shen, X., 2008. "Security in vehicular ad hoc networks". *IEEE communications magazine,* **46**(4).

[37] Li, B., Pei, Y., Wu, H., Liu, Z., and Liu, H., 2014. "Computation offloading management for vehicular ad hoc cloud". In International Conference on Algorithms and Architectures for Parallel Processing, Springer, pp. 728–739.

[38] Arkian, H. R., Atani, R. E., Diyanat, A., and Pourkhalili, A., 2015. "A cluster-based vehicular cloud architecture with learning-based resource management". *The Journal of Supercomputing,* **71**(4), pp. 1401–1426.

[39] El Sibaï, R., Atéchian, T., Abdo, J. B., Tawil, R., and Demerjian, J., 2015. "Connectivity-aware service provision in vehicular cloud". In Cloud Technologies and Applications (CloudTech), 2015 International Conference on, IEEE, pp. 1–5.

[40] Meneguette, R. I., Boukerche, A., and de Grande, R., 2016. "Smart: an efficient resource search and management scheme for vehicular cloud-connected system". In Global Communications Conference (GLOBECOM), 2016 IEEE, IEEE, pp. 1–6.

[41] Salahuddin, M. A., Al-Fuqaha, A., and Guizani, M., 2016. "Reinforcement learning for resource provisioning in the vehicular cloud". *IEEE Wireless Communications,* **23**(4), pp. 128–135.

[42] Tamani, N., Brik, B., Lagraa, N., and Ghamri-Doudane, Y., 2017. "Vehicular cloud service provider selection: A flexible approach". In GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, pp. 1–6.

[43] Meneguette, R. I., and Boukerche, A., 2017. "A cooperative and adaptive resource scheduling for vehicular cloud". In Computers and Communications (ISCC), 2017 IEEE Symposium on, IEEE, pp. 398–403.

[44] Investopedia, 2018. Law of diminishing marginal utility. `https://www.investopedia.com/terms/l/lawofdiminishingutility.asp`. [Online; accessed 2-April-2018].

[45] Wikipedia contributors, 2018. Quasilinear utility — wikipedia, the free encyclopedia. `https://en.wikipedia.org/wiki/Quasilinear_utility`. [Online; accessed 2-April-2018].

[46] Wang, X., Sun, J., Huang, M., Wu, C., and Wang, X., 2012. "A resource auction based allocation mechanism in the cloud computing environment". In Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, IEEE, pp. 2111–2115.

[47] Prasad, A. S., and Rao, S., 2014. "A mechanism design approach to resource procurement in cloud computing". *IEEE Transactions on Computers,* **63**(1), pp. 17–30.

[48] Lin, W.-Y., Lin, G.-Y., and Wei, H.-Y., 2010. "Dynamic auction mechanism for cloud resource allocation". In Proceedings of the 2010 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, IEEE Computer Society, pp. 591–592.

[49] Game Theory.net, 2018. Dominant strategy. `http://www.gametheory.net/dictionary/DominantStrategy.html`. [Online; accessed 2-April-2018].

[50] Nisan, N., Roughgarden, T., Tardos, E., and Vazirani, V. V., 2007. *Algorithmic game theory*. Cambridge university press.

[51] SUMO- Simulation of Urban MObility, 2018. Home page. `http://sumo.dlr.de/index.html`. [Online; accessed 2-April-2018].

[52] Amazon Web Services, Inc., 2018. Amazon web services (aws) - cloud computing services. `https://aws.amazon.com/`. [Online; accessed 2-April-2018].

[53] OpenStreetMap, 2018. Welcome to openstreetmap. `https://www.openstreetmap.org/`. [Online; accessed 2-April-2018].

[54] Dr. Tom Mathew, IIT Bombay, 2018. Lecture 12 : Vehicle arrival models: Headway - nptel. `http://nptel.ac.in/courses/105101008/12`. [Online; accessed 2-April-2018].

[55] Che, Y.-K., 1993. "Design competition through multidimensional auctions". *The RAND Journal of Economics*, pp. 668–680.

[56] Krishna, V., 2009. *Auction theory*. Academic press.

[57] David, E., Azoulay-Schwartz, R., and Kraus, S., 2006. "Bidding in sealed-bid and english multi-attribute auctions". *Decision Support Systems,* **42**(2), pp. 527–556.

[58] Sun, J., Zhang, C., Zhang, Y., and Fang, Y., 2010. "An identity-based security system for user privacy in vehicular ad hoc networks". *IEEE Transactions on Parallel and Distributed Systems,* **21**(9), pp. 1227–1239.

[59] Boneh, D., and Franklin, M., 2001. "Identity-based encryption from the weil pairing". In Annual international cryptology conference, Springer, pp. 213–229.

[60] Wikipedia contributors, 2015. Weil pairing — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Weil_pairing&oldid=695555571`. [Online; accessed 13-May-2018].

[61] Barreto, P. S., Libert, B., McCullagh, N., and Quisquater, J.-J., 2005. "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps". In International conference on the theory and application of cryptology and information security, Springer, pp. 515–532.

[62] The AVISPA Project Automated Validation of Internet Security Protocols and Applications, 2015. Welcome to the avispa home page! `http://www.avispa-project.org/`. [Online; accessed 13-May-2018].

[63] He, D., Zeadally, S., Xu, B., and Huang, X., 2015. "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks". *IEEE Transactions on Information Forensics and Security,* **10**(12), pp. 2681–2691.

Dissemination

1. S. Mishra, S.Maity, and S.K. Jena,"IBC based verifiable hash chains for reliable internet access in intelligent transportation systems", In Information Communication and Embedded Systems (ICICES),(pp. 1- 6), IEEE, 2017, Chennai, India.

2. S. Mishra, S.K. Mishra, B. Sahoo, M.S. Obaidat, and D. Puthal,"First Score Auction for Pricing-Based Resource Selection in Vehicular Cloud", International Conference on Computer, Information and Telecommunication Systems (CITS), July 11-13, 2018, Colmar, France.(accepted)