

COPYRIGHT WARNING

This paper is protected by copyright. You are advised to print or download **ONE COPY** of this paper for your own private reference, study and research purposes. You are prohibited having acts infringing upon copyright as stipulated in Laws and Regulations of Intellectual Property, including, but not limited to, appropriating, impersonating, publishing, distributing, modifying, altering, mutilating, distorting, reproducing, duplicating, displaying, communicating, disseminating, making derivative work, commercializing and converting to other forms the paper and/or any part of the paper. The acts could be done in actual life and/or via communication networks and by digital means without permission of copyright holders.

The users shall acknowledge and strictly respect to the copyright. The recitation must be reasonable and properly. If the users do not agree to all of these terms, do not use this paper. The users shall be responsible for legal issues if they make any copyright infringements. Failure to comply with this warning may expose you to:

- Disciplinary action by the Vietnamese-German University.
- Legal action for copyright infringement.
- Heavy legal penalties and consequences shall be applied by the competent authorities.

The Vietnamese-German University and the authors reserve all their intellectual property rights.



Vietnamese German University
Department of Electrical Engineering & Information Technology

Frankfurt University of Applied Science
Faculty 2: Computer Science and Engineering

VEHICLE SYSTEM MANAGEMENT FOR AUTOMATIC TOLL APPLICATION

BY

DAO MINH HIEU

Matriculation number: 1184776

VGU
Vietnamese-German University
First Supervisor: Dr. THAI TRUYEN DAI CHAN

First Supervisor: Dr. THAI TRUYEN DAI CHAN

BACHELOR THESIS

Submitted in partial fulfillment of the requirements
for the degree of Bachelor Engineering in study program
Electrical Engineering & Information Technology,
Vietnamese German University, 2021

Binh Duong, Vietnam, January 2021

Vehicle System Management For Automatic Toll Application

Approved by

Dr. THAI TRUYEN DAI CHAN, First Supervisor



Thesis Committee

Disclaimer

I hereby declare that this thesis is a product of my work, unless otherwise referenced. I also declare that all opinions, results, conclusions, and recommendations are my own and may not represent the policies or opinions of Vietnamese-German University.

Dao Minh Hieu



Acknowledgement

I would like to express the most profound appreciation to my supervisor, Dr. Thai Truyen Dai Chan, for the continuous support of my study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance has helped me in all the time of researching and writing this thesis.



Abstract

Despite of having many rules and regulations in for transportation traffic, it is still to this day a chaotic environment sometimes. Therefore, finding traffic solution is a work of art in civil engineering world. However, the technology of internet and navigation solution is evolve every day, and this opens many opportunities to increase the quality of current traffic status or even solve problems that people do not even know it existing. It is such a fascinating time we are living where electronics components embedded with latest technology are affordable for hobbyist, and it means more beautiful mind can involve in finding delicate solutions, and current manual toll station is one of the problems that need a better solution. GPS technology and Google database now reach a level that is precisely, smart and fast enough on a portable smartphone to change the traditional toll to a new form by removing all of the obstacle throughout fee paying process at these station and to make it environmental friendly. This project is one of the solution by realizing an on the go payment virtual toll station, replace all the work of manual toll to a smarter automatic one.

Keywords: GPS, automatic, on the go payment

Contents

1	Introduction	9
1.1	Purpose	9
1.2	Audience	9
1.3	Motivation	9
1.4	Objectives	10
1.5	Outline	10
2	Research background	11
2.1	Introduction	11
2.2	Current toll problem	11
3	System architecture and interfaces	14
3.1	General system	14
3.2	E-wallet application	14
3.3	Central database	15
3.4	Vehicle profile device	16
3.5	Socket communication	17
3.6	Bluetooth communication	20
3.6.1	Bluetooth architecture	Vietnamese-German University 20
3.6.2	SPP Profile	20
3.6.3	Connection Process	21
3.6.4	Bonding and Pairing	21
3.7	GPS Technology	23
4	System implementation	26
4.1	E-wallet Android application	26
4.1.1	Activities and fragments management	26
4.1.2	Main Activity	28
4.1.3	Login Fragment	28
4.1.4	Home Fragment	30
4.1.5	Add Credit and Retrieve Money	31
4.1.6	Driver Registration	31
4.1.7	Vehicle Registration	32
4.1.8	Log out	32
4.1.9	Client socket interface handler	32

4.1.10 GPS tracking service	33
4.1.11 Bluetooth service	33
4.1.12 Client Encryption and Decryption service	34
4.2 Socket and Sqlite based central server.....	35
4.2.1 Server socket interface handler (SIH).....	35
4.2.2 Sqlite database handler (DBH).....	35
4.2.2.1 Login	35
4.2.2.2 Log out	36
4.2.2.3 Sign up	36
4.2.2.4 Add money	36
4.2.2.5 Retrieve money	37
4.2.2.6 Register driver	38
4.2.2.7 Get history transaction	38
4.2.2.8 Get user information.....	38
4.3 Server Encryption and Decryption service	38
4.3.1 Vehicle profile and notify application	38
4.3.2 Virgin registration service	38
4.3.3 Acceleration sensing handler.....	38
4.3.4 Bluetooth interface handler	38
5 System feature results and evaluation.....	39
5.1.1 Signup virgin vehicle	39
5.1.2 Driver alert feature	39
5.1.3 Driver registration and de-registration	39
5.1.4 Automatic paying fee feature	39
5.1.5 E-wallet credit management.....	39
5.1.6 Security data exchange	39
5.1.7 Limitation and future improvement.....	43
6 Conclusion	44
References	45

Figure 1 Abandon toll booth with degrade road condition in Ha Nam	13
Figure 2 Service usage of popular E-Wallet in Vietnam [4]	14
Figure 3 Block diagram of Payment system	15
Figure 4 Global positioning method of GPS technology	23
Figure 5 Point determination method from 4 known points in 3 dimension	24
Figure 6 Travel distance calculation strategy	25
Figure 7: E-Wallet Navigation UI	27
Figure 8: E-Wallet Login Fragment UI	29
Figure 9: E-Wallet Home Fragment	30
Figure 10: The enabling Bluetooth dialog	34



1 Introduction

1.1 Purpose

This report is submitted for partial fulfillment of the Bachelor Thesis at the Vietnamese – German University. The report demonstrates from general to detail about web application for tracing and checking in food safety and quality

1.2 Audience

The intended audience for this project and report are Dr. Thai Truyen Dai Chan and MSc.Tran Quang Nhu, who will use it as a basis to evaluate and determine a portion of the grades for the Bachelor Thesis.

1.3 Motivation



Unnecessarily construction or human interaction are the reasons pushing technology forward in order to replace them with an intelligent automation system, and traditional manual toll is not different. The availability of IoT solutions are now more and more accessible and secured enough to develop such a system that is money transaction related. The thriving of E-wallet companies in Vietnam in recent year has shifted the purchasing habit of large portion of Vietnamese consumer, hence raising liquidity of these virtual credits. This phenomenon gains trust on the banking system allowing converting real money to virtual or vice versa easier than ever. However, none of road construction companies applied this result to their fee collecting activity. Although, some of them have chosen alternative solution such as using RFID card, but the main purpose of automation is not applied when the driver interaction is still involved during the procedure of paying fee. Therefore, taking advantage of E-Wallet characteristic and GPS technology, this project will enable user to pay road fee securely on the go without any interaction

involved, and the solution will turn all physical construction digitally and place them on any road position in Vietnam via few simple configurations on database. This solution could replace the current road toll system or its alternative entirely.

1.4 Objectives

This thesis is created with the objectives of research, design, and implementation of a web application for monitoring and tracing of food safety and quality. The finalization of this project can be used to manage, monitor the quality of food from the beginning of the cultivation stage to the delivery process. A website platform is developed to collect and analyze the data received from IoT devices. Hence, all the analyzed data is displayed as a graph or exported as a table for users to easily access, control, make decisions on the quality of food.

1.5 Outline



Chapter 2:

Chapter 3:

Chapter 4:

Chapter 5:

Chapter 6:

2 Research background

2.1 Introduction

Road toll is not a modern definition, it existed at least 2700 years ago before any steam engine machine invented, where travelers had to pay to use Susa-Babylon highway under regime of Ashurbanipal [1]. Till this day in Vietnam, a toll is introduced to finance the transport infrastructure, usually national road or highway, but the general process stay the same: stop driving, pay the fee and continue driving. Although there is a solution improving this process by using a toll gate automation [2], this solution only reduce the time and labor cost of manual toll booth, but the gimmick is the same, and the drivers are still be interrupted along their driveway. This project will provide a more efficient and delegate solution by removing all the listed step throughout fee payment activity and make it truly automatic when involving the GPS technology in the process.



2.2 Current toll problem

Current manual toll systems come with many disadvantages in form of cost, efficiency and longevity of the highway in Vietnam.

The cost of a manual toll may vary depending on the construction size, the location, the geographical and the labor cost. The cost of a single national road toll booth on Quoc Lo 1A is around 7.3 billion VND (314,523 USD) [3] connecting from Northern to Southern of Vietnam, and there are 40 tolls placed along this main road for controlling and fining smaller portions of this road.[] This can add up to thousands of billions VND when including maintenance fee.

Every time a vehicle decelerates to stop at the toll to pay the fee and accelerates to get back on track, the wheels apply a friction to the concrete surface, which can be a static friction or a sliding friction at the contact point. The greater the weight and initial velocity (especially on highway) of the vehicle the greater the friction.

$$F = Mg\mu$$

F : Friction at the contact point of wheels and the road

M : Vehicle mass

g : Gravitational acceleration

μ : coefficient of friction

And this force deals a massive amount of damage to the road surface. The reason for building these

tolls is to pay back the capital of constructing the road for the contractor but at the same time  Vietnamese-German University destroying the road itself. Therefore, this action not only reduces the lifespan of the road surface but also raises the cost of maintenance higher than it should be.



Figure 1 Abandon toll booth with degrate road condition in Ha Nam

The environmental impact will be reduced greatly with this project by saving tons of building materials for a static toll. When these structures are no longer needed since the contractors already earned enough money for the responsible road, they got abandoned in the middle of the highway, blocking the traffic with unnecessary space taken.

Finally, the time it took to stop and pay the fee is around 30 seconds. This time interval will be neglectable for a casual driving speed, but for the highway, where the speed could reach up to 120km/h, the automatic toll will let drivers save up to 1 km of trip distance.

The purpose of this project is to realize an automatic toll system which neglects all the listed downside from manual toll systems and lets users manage their payment in road usage.

3 System architecture and interfaces

3.1 General system

3.2 E-wallet application

Electronic wallets are increasing their popularity in recent years in Vietnam. Moreover, due to the spreading rate and serious health impact of CO-vid19 virus, using cash is less of a choice when compared with electronic currency alternatives. Vietnamese people are slowly changing their habit and gaining trust for these transaction services, and this opens many possibilities to have more payment methods linked with these electronic wallets.

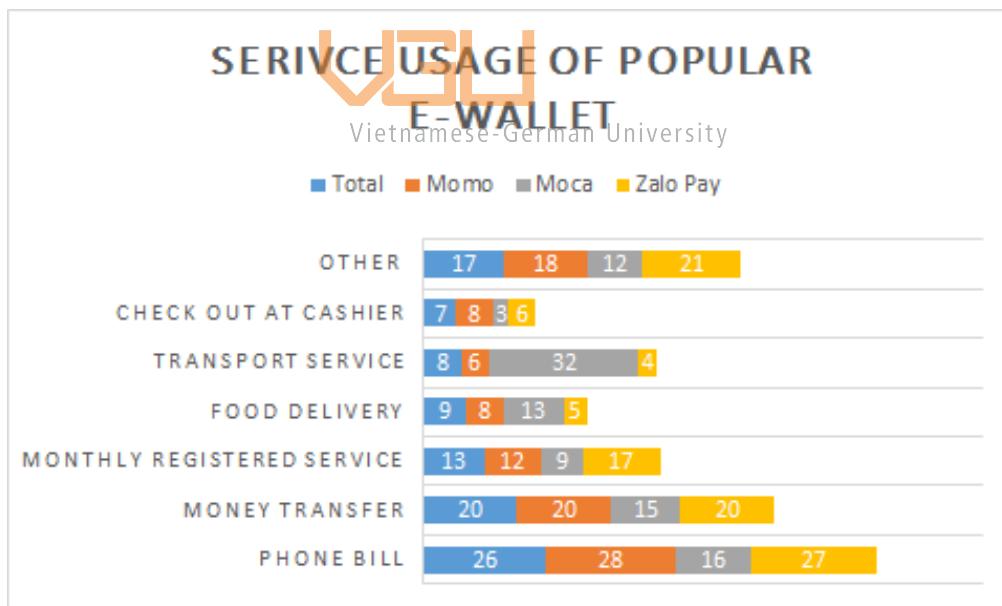


Figure 2 Service usage of popular E-Wallet in Vietnam [4]

For this reason, the payment system for road fee will be enabled through an electronic wallet mobile application linked with their bank account.

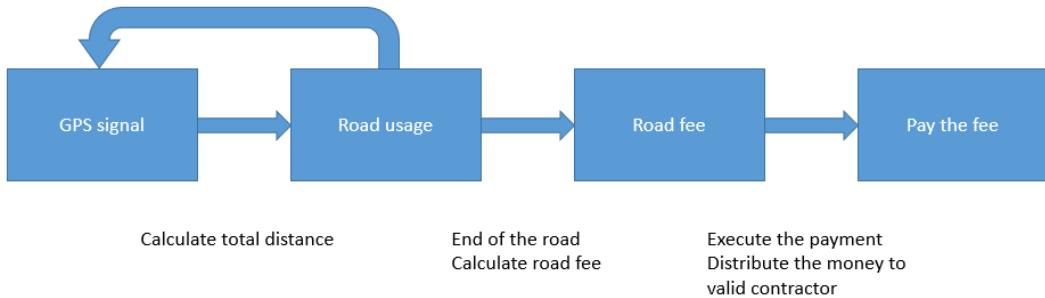


Figure 3 Block diagram of Payment system

The road fee will be based on the calculated road usage instead of paying a same fee for every distance as on manual tolls. This strategy will save a lot of money for the end user by its integrity nature and earn the capital back for contractors faster because this system can be implemented on every road and takes no extra fee to build a constant structure. All the processes will run in the background with no supervision needed.



Vietnamese-German University

With the described characteristics, this sub-system is designed to replace the roll of road fee collectors at the toll station and placing any station on anywhere at will.

3.3 Central database

3.4 Vehicle profile device

While operating a vehicle on the street, different vehicle has different impact. Therefore, the diversification of road fee per kilometer is necessarily, in order to bring equality to drivers. For this requirement, the automatic toll system need to introduce a device which can store vehicle data, especially vehicle mass, mounted permanently on the vehicle itself. Moreover, E-Wallet does not have to be attached to any vehicle as long as the user does not operate that vehicle, just like a normal wallet only belong to its owner, not the car.

The vehicle device shall be equipped with Bluetooth communication to interact with E-Wallet. There are 2 main interactions: register vehicle and register driver.

When a vehicle device is first mounted on the vehicle, it need to have a procedure to inform itself about the vehicle to later on transmit

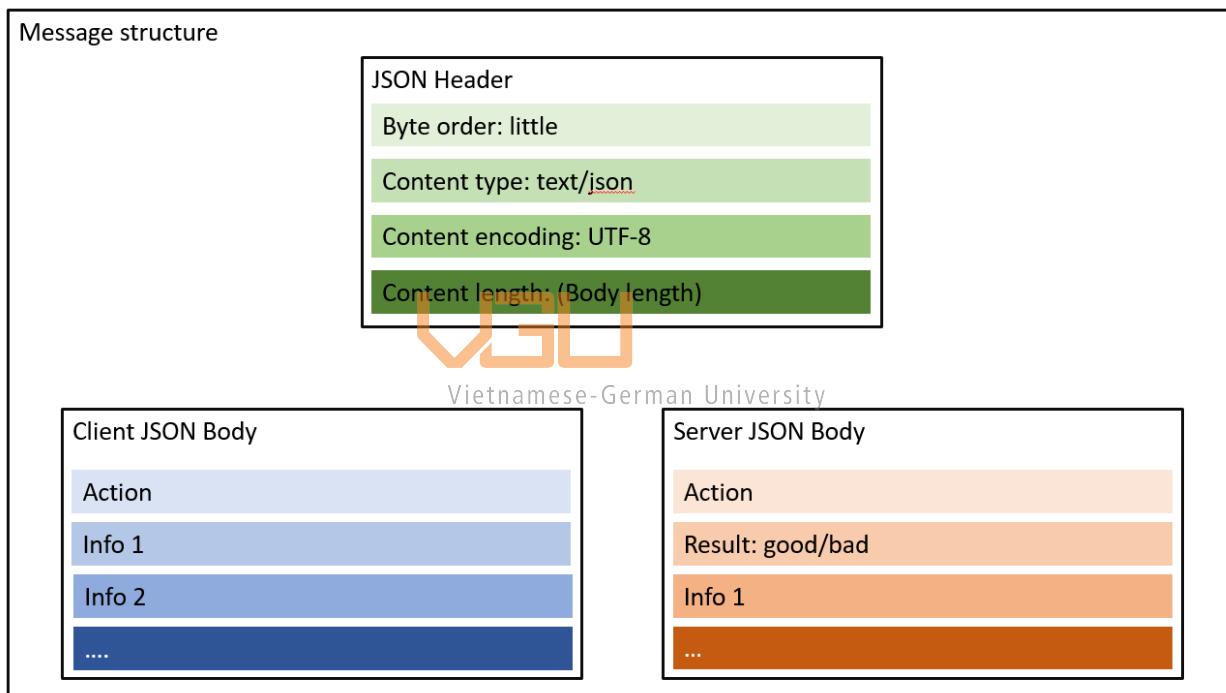


Vietnamese-German University

In this project, the road fee shall be calculated proportional to the vehicle mass.

3.5 Socket communication

Socket communication, or more specifically, network socket communication using in this project configured for TCP connection. Central server will initiate as server socket accepting client device, which is the E-Wallet. The majority communication activities are start the connection, client sending request to server, server response to client after request processed and connection closed. The request and response message will be divided into 2 parts, header and body using JSON structure.



The headers of both request and response message types are the same including Endianness byte order, JSON content type, encoding rule and length of body. Since the E-Wallet application and the Central server is created to work with each other, the information in the Header shall be check with fixed condition except the content length, since this value varied along with the body content, and this checking step will ensure the quality of the communication.

The request body of client device will consist of the Action field, which declared the type of request that the server need to process, along with related information for this request. For example, login request will have Action is login, phone number and password are 2 more information for the server to proceed logging in.

The server side on other hand, the response body will have the Result field to inform the client the status of the request and the Action field of regarded status. The existing of Action field in the response message structure is to ensure the client can distinguish which response of which request, in case there are multiple requests sent from it. Beside from Result and Action field, the response message body also consists information fields matched with the Action.

The request and response information field shall be listed in the tables bellowed:

Action	RESPONSE MESSAGE											
	result	phone number	password	budget	vehicle name	vehicle mass	login status	longitude	1st Latitude	2nd Latitude	Street name	money transaction
Login	x	x		x	x	x	x					
Logout	x											
Sign up	x											
add money	x											
retrieve money	x											
Pay fee	x											
Register driver	x											
Get history	x	x			x	x	x	x	x	x	x	x
Get user information	x	x	x	x	x	x	x	x	x	x	x	x

3.6 Bluetooth communication

3.6.1 Bluetooth architecture

For this project, the Node MCU ESP32S chip of the vehicle device support both Classic Bluetooth and Low Energy Bluetooth technology. The Bluetooth architecture of ESP chip contain 2 stacks: controller stack and host stack. Modules such as PHY, Device Manager, Baseband, Link Manager, Link Controller, and HCI are included in controller stack. On other hand, the host stack support L2CAP, GATT, ATT, GAP, SMP and SDP profiles providing the interface to application layer to operate Bluetooth service. The vehicle device uses the default Bluetooth setting for this chip, which is using VHCI (software-implemented virtual HCI interface) to communicate between host stack and controller stack, and the profile used is SPP since it provide many standard communication.



3.6.2 SPP Profile

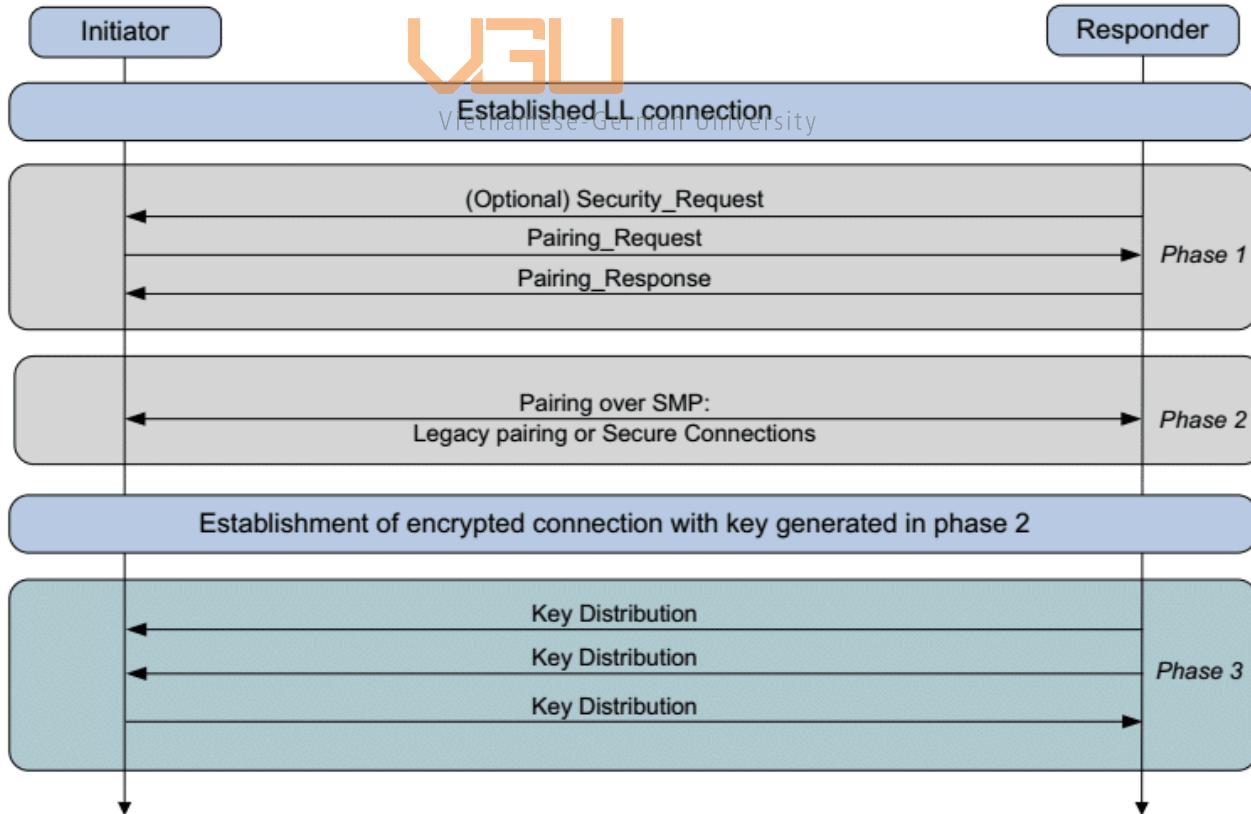
Based on ETSI 07.10 and the RFCOMM protol, SPP stands for Serial Port Profile can emulate RS-323 serial message, and it is convinient when using with Serial API from arduino, and RFCOMM protocol is used on mobile device side. The Serial Port Profile set the necessary requirements for Bluetooth devices to act as a wrieless serial cable connections using RFCOMM between two peer devices. The requirements are detailed in terms of services for applications, and by setting the features and procedures that are required for exchanging between Bluetooth devices.

3.6.3 Connection Process

The vehicle device will be an Acceptor [5], which initiates itself and form a connection to another device. This done by broadcasting inquiry request at radio frequency of 2.4 Ghz while the mobile device, an Initiator, will listen to this via discovery mode and response if chosen by the user, and two bluetooth devices shall initiate the connection.

3.6.4 Bonding and Pairing

When connection is established between the mobile device, they will proceed pairing sequence to creates bonds. This process will go through 4 phases: Pairing feature exchange, short term key generation, long term key generation, transport specification key deistribution



Pairing is the exchange of security features including feature such as Input/output (IO) capabilities, requirements for Man-In-The-Middle protection, etc. The exchange of pairing information between the mobile device and the vehicle device is done through the Pairing Request and Pairing Response packet.

Field	Code (1 Byte)	IO Cap (1 Byte)	OOB DF (1 Byte)	AuthReq (1 Byte)					Maximum Encryption Key Size (1 Byte)	Initiator Key Distribution (1 Byte)	Responder Key Distribution (1 Byte)
				BF	MITM	SC	KP	Reserved			
Bits*	8	8	8	2	1	1	1	3	8	8	8

Table 1 Pairing Request/Response

*Bit order is LSB to MSB.



3.7 GPS Technology

Global Positioning System (GPS) is based on satellite radio navigation service provided by the US Space Force [6]. By using the information from an on-board atomic clock, coordinates and a current status, the GPS satellite projects a radio signal from medium Earth orbit region (approximately 20,000 km above the ground) to a client device at the speed of light. The GPS embedded device then uses this time information to calculate the distance of itself to at least 4 satellites [7].

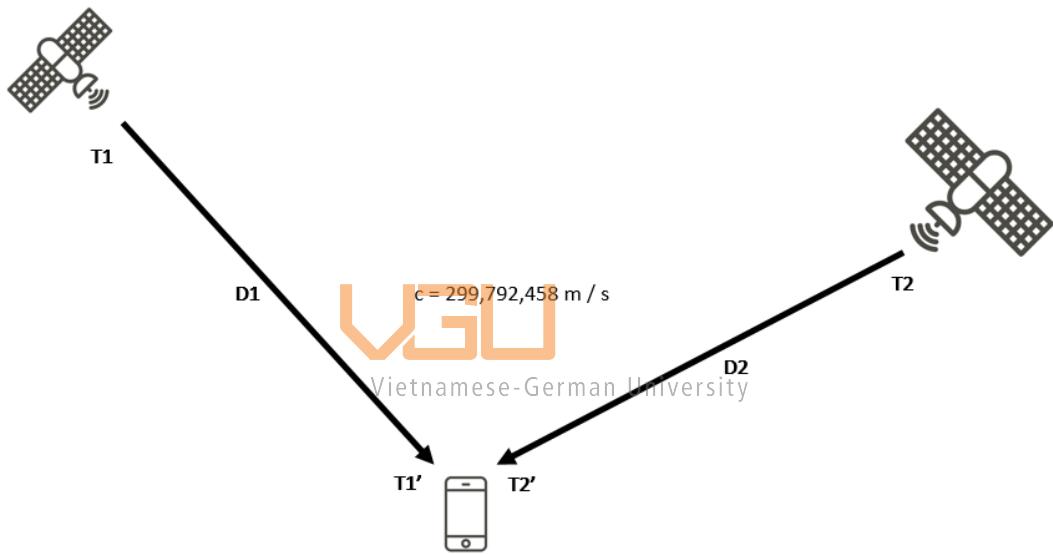


Figure 4 Global positioning method of GPS technology

$$|D| = c * \Delta T = c * (T' - T)$$

D : Distance from a satellite to the GPS device (m)

T : Time instant when the GPS signal leave the satellite (s)

T' : Time instant when client device receive the GPS signal (s)

c : Speed of light (m/s)

By knowing the distances to 4 determined points in space, a GPS device coordinate (x, y, z) can be located with the root of following system of equations:

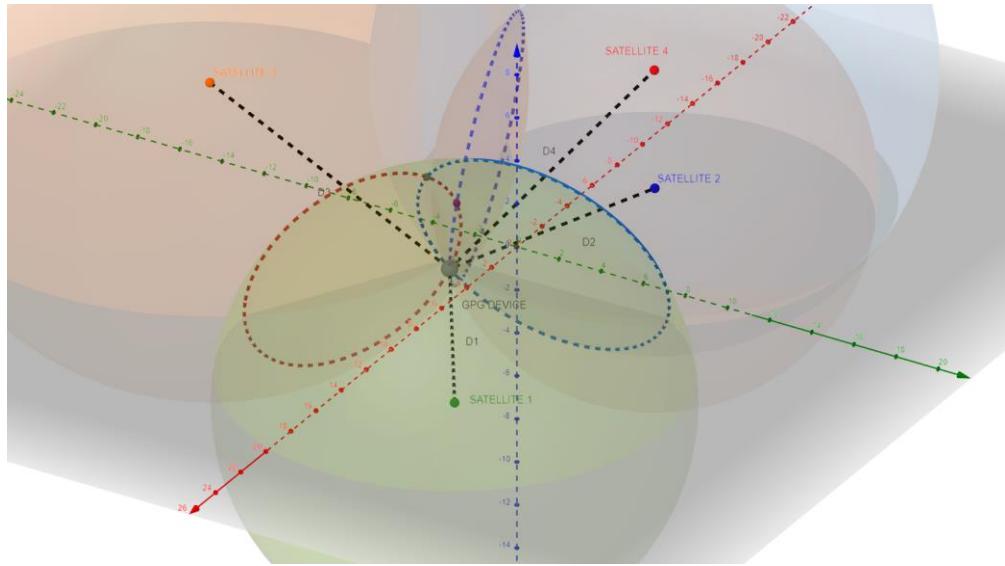


Figure 5 Point determination method from 4 known points in 3 dimension



$$D1 = \sqrt{(x - x_1)^2 + (y - y_1)^2 + (z - z_1)^2}$$

$$D2 = \sqrt{(x - x_2)^2 + (y - y_2)^2 + (z - z_2)^2}$$

$$D3 = \sqrt{(x - x_3)^2 + (y - y_3)^2 + (z - z_3)^2}$$

$$D4 = \sqrt{(x - x_4)^2 + (y - y_4)^2 + (z - z_4)^2}$$

Dx : Distance from a satellite to GPS device (m)

x_i, y_i, z_i : Satellite coordinate (m)

x, y, z : GPS device coordinate (m)

GPS technology is enabled on almost every smartphone nowadays, which is carried everyday by traffic participants. Along with an enormous geography database provided by Google Service, this combination is included in building the GPS tracking and payment subsystem to track the trajectory of

the user in real-time in each specific road path. After the user leaves the road, the collected coordinates can be calculated to output a final road usage of the user on that road. The road usage calculation can be realized by following equation:

$$D = \sum_{i=0}^k \sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}$$

D : Total road usage (m)

k : Number of coordinate samples

x_i, y_i : Latitude and longitude sample at time instant i (m)

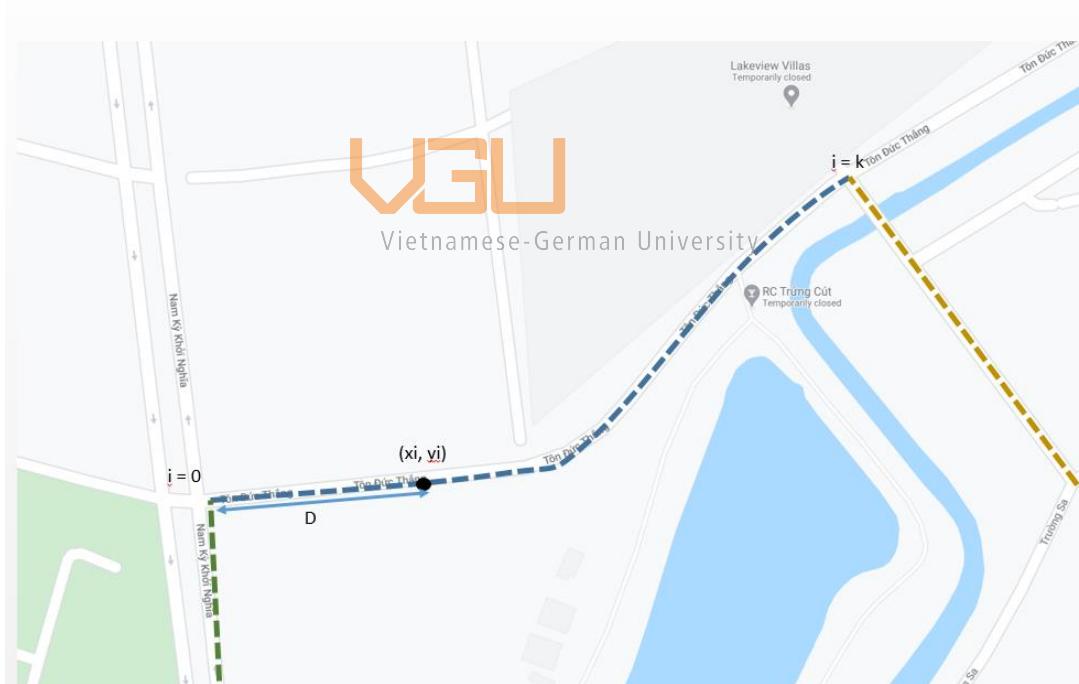


Figure 6 Travel distance calculation strategy

4 System implementation

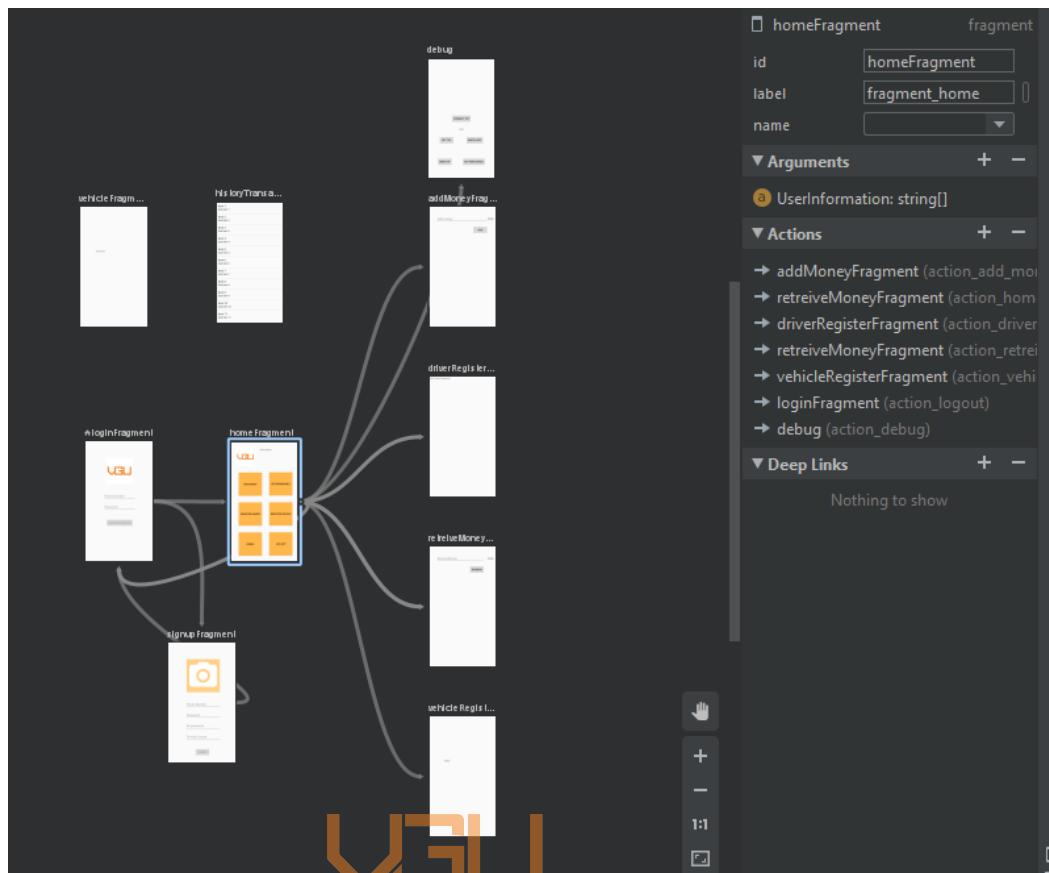
4.1 E-wallet Android application

4.1.1 Activities and fragments management

An Activity is the main visualize interface that the user interact with most of the time on an android application [8]. Activity class handles entering, pausing, exiting actions for the application while on an activity. When switching from an Activity to next Activity, the system need to save current state of previous activity, destroy current view and generate new view for next Activity [9]. This action consumes unnecessarily energy and memory resources of the mobile device, when some of the UI (User interface) can be re-use as a general theme for entire life cycle of the application. Android library provides an

alternative option called Fragment to inherit usable portion of the UI while updating required information. The API makes this possible by introduce modularity and reusability into the hosted Activity [10] via a fragment tag embedded in a XML file, which defines the user interface layout structure of the Activity [11]. The fragment tag can be constrained its position with other elements, which are encapsulated functionalities, respectively in this case.

The usage of Fragments are more reasonable since Android Studio 3.3 arrived [12]. In this version, Google introduced Navigation feature, which is a tool set allows developer to visualize and manage the navigating relationship between Fragments such as path, direction, action, etc., to ensure a consistence and predictable behavior when executing a transition [13]. This tool comes with a graph that illustrates transitions with actions and arguments properties, which are mandatory for the E-wallet application graphical interface management back-bone.



Vietnamese-German University

Figure 7: E-Wallet Navigation UI

While only E-Wallet app have one Main activity consisting a navigation bar existing throughout application processes, all other different user procedures shall be contained in Fragments system. This architecture design takes advantage of today mobile device hardware power and decrease potential errors in development process when managing multiple user interfaces and actions between them.

4.1.2 Main Activity

The Main Activity initialize when the app is first start and kept alive until user close the app. On creation of the Activity, Navigation bar shall be introduce to the environment with three main paths to corresponding Fragments: Home, History and Vehicle. Right after that, Login Fragment shall be generated and hide the navigation bar away, because user have to login and connect to central server first before access further into the app. Otherwise, the app would crashed and raised Null pointer exception, since all the data need to be used is initially null before retrieved from central server when logging in success.

4.1.3 Login Fragment

The Login fragment is an interface allow user to input their phone number and password to access further features of the E-Wallet.



Vietnamese-German University

Login is the first Fragment user encounter when Main Activity is created, and this is possible when assigning start destination properties to it [14]. Phone number and password text placeholder is the output of EditText objects creation, these objects then linked to corresponding tag in XML file of Login Layout via findViewById procedure [15], this method applied for all linkage between user interact Java objects and visual interface XML tag.



Vietnamese-German University

Figure 8: E-Wallet Login Fragment UI

Phone number text field will have a live check if the input is a number and have 10 or 11 digits (standard mobile phone number in Vietnam [16]). Password field will check if input is a string containing alphabet character, number and special character. If these conditions are fulfilled, the login Button object will active to be pressed.

On click handler of login Button [17] will send login information to central server to authorize the user availability. If the authorization success, the application will received a positive feedback along with important user information such as credit card information, E wallet credit and vehicle name to prepare a Bundle [18] to send to Home Fragment.

4.1.4 Home Fragment

The Home Fragment is an interface allow user to do multiple activities related to:

Budget management

Vehicle/Driver registration

Log out

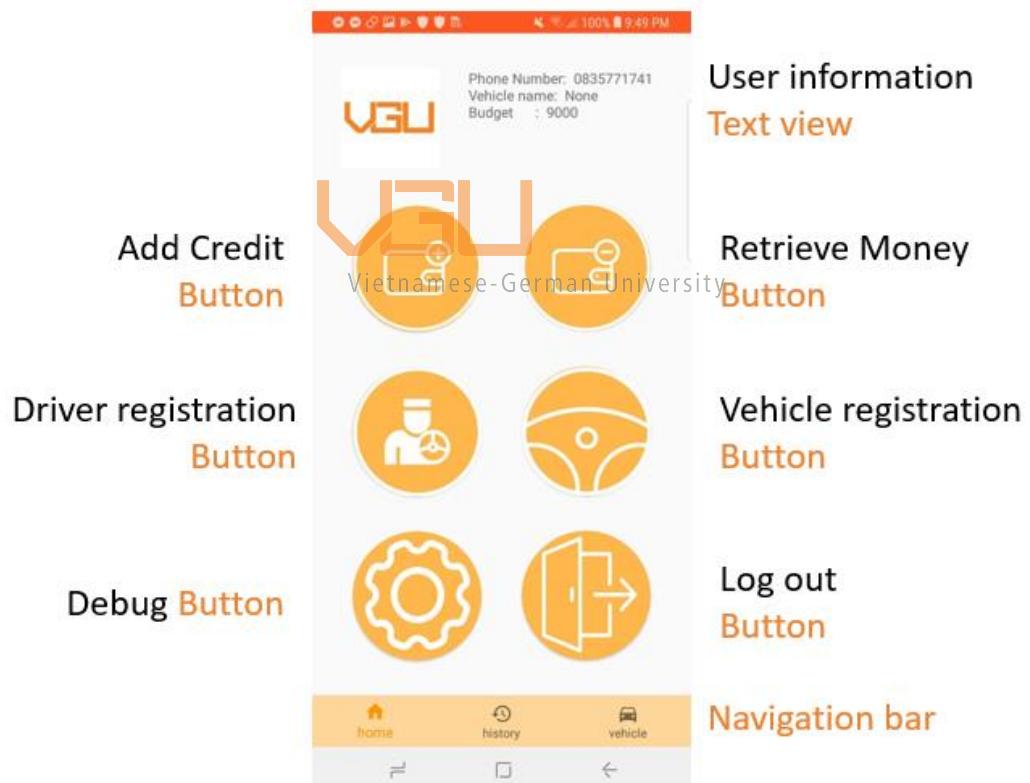


Figure 9: E-Wallet Home Fragment

4.1.5 Add Credit and Retrieve Money

These actions enable user to change their wallet credit status by adding and retrieving money to linked credit card. After this action finished, the budget data on central server side also update accordingly.

Home fragment shall run a loop thread in background to continuously fetching user information every 100ms to update budget value on User Information Text View section.

A Text Watcher [19] shall observed user input when Retrieve Money action is ongoing. This object will enable the Retrieve Button, which allows user to further proceed the action, if the input amount is less than the current credit in the budget. Otherwise, the user have to return to Home Fragment or change the input.

The ratio of credit and VND is 1:1

4.1.6 Driver Registration



This action creates an interface to start exchange information with the vehicle profile device via Bluetooth. At first, the application shall check for Bluetooth availability on the mobile device and ask for access permission if previously not granted yet. If the user does not grant the accessibility permission, the application will return to Home Fragment and wait for other actions. If permission granted by the user, the mobile device shall start searching for a registered vehicle and start exchanging information with it. Further background procedure will be described in *Bluetooth interface handler* section.

After choosing a suitable vehicle, the mobile device shall send a request to the central server to update vehicle data of regard user profile. The vehicle data contains vehicle name and vehicle mass.

4.1.7 Vehicle Registration

NaN

4.1.8 Log out

This action triggers the central server by sending a log out request along with user phone number. After receiving a positive response, application shall transition to Login Fragments, and all previous user data stored on the mobile device shall be set to null.

4.1.9 Client socket interface handler

The mobile device will a client in the TCP socket communication with respect to the central server. The client socket class shall have 3 main procedures: start connection, sending request and listening to

 response. In order to maintain consistence connection to the central server, these procedures shall run in parallel threads. Start connection thread shall run at the beginning of every Fragment. If the mobile device cannot initiate a connection with central server by throwing an I/O Exception [20] during start connection thread execution, the application will set a 1000ms timer before restart the connection.

Application shall start listening thread right after the connection is established. This thread will run in an infinite while loop only break when an IO Exception is raised. While looping, the application will continuously fetching the data from TCP socket buffer and covert to a string. When this procedure encounters an end of line indication, the application will forward all collected data to further processes.

If the application is in login session, it means the long term key between the mobile device and the central server not existed or erased (more about long term key in *Security data exchange*). Then, when listening thread captures a message from central server, it will redirect this data to JSON analyzer, which is a function derived un-encrypted JSON structured message to extract data field inside the message. If

the long term key were stored in mobile device, the listening thread will forward incoming message to the Decryption service, then forward to JSON analyzer.

Before sending any request to central server, the message must be encrypted by a temporally and long term key and sent using sending thread.

When sending or listening, the application shall check for connection status because the read and write I/O stream is initiate at the start connection thread, otherwise, the application will throw I/O or null pointer exception. The reason start connection, sending and listening action must be handled in thread is because the application can still captured new data while sending a request or update secrete key on the go.

4.1.10 GPS tracking service

4.1.11 Bluetooth service



Vietnamese-German University

Bluetooth service on mobile device shall start when application in Vehicle or Driver Registration

Fragment. Since Bluetooth is treated as an external device with respect to the CPU on mobile device, or in Android library terminology, a Bluetooth Adapter, the application need to verify the Bluetooth chip whether this mobile device is Bluetooth supported or not [21]. If the hardware requirement is fulfilled, the application shall initiate an Intent [22] and passing the previously introduced Bluetooth adapter to listen to user permission to turn on Bluetooth connectivity. An Intent act like an event handler optimized to run on Android OS instead of un-controlled thread and loop, and this class also provide a Broadcast Receiver [23] in order to captured dynamically Bluetooth messages broadcasted by OS system in publish-subscribe pattern [24]. This handling scheme will be applied on later states of Bluetooth services.

An app wants to turn Bluetooth ON for this device.

DENY ALLOW

Figure 10: The enabling Bluetooth dialog

The mobile device is an Initiator device [25] in this project Bluetooth communication, therefore, the application shall start discovery to retrieve vehicle device MAC address. After the vehicle device selected by the user, the application shall attempt to initiate the Bluetooth connection as client [26]. To proceed connection initiation, the application create a RF Communication Socket and passes in its UUID to start exchanging with vehicle device on a new thread. If there is no I/O Exception occurred, application will cancel discovery mode to prevent slowing down the connection. If the attempt is succeed, the application will finish the thread that running attempt connection and open a Bluetooth socket input and output stream declared. The listening and sending messages handler have a similar design scheme of TCP connection of the application described in chapter *Client socket interface handler*.

Due to the nature of Bluetooth communication, which is low range and peer to peer, it is not necessarily to develop a secured communication with special authorization process. The data exchange via Bluetooth service is the vehicle information, and this interchange only occur once when register the driver and once when register the vehicle.

4.1.12 Client Encryption and Decryption service

Encryption and Decryption services on mobile device side is handled by Fernet library for Java [27]. In order to encrypt or decrypt any information, the API required a key and a token. The key in this case shall be the temporally key or the long term key depending on the stage of the application. When

encrypting, the token is generated using the key and the message package needed to be sent. When decrypting, the token is the decrypted message that the listening thread passing to. Moreover on decryption service, the mobile device need to set the alive time of the token to match will the central server side, in this case, it is 60 second by default. Otherwise, even with a valid key, the TCP communication still not be possible.

4.2 Socket and Sqlite based central server

4.2.1 Server socket interface handler (SIH)

4.2.2 Sqlite database handler (DBH)

4.2.2.1 Login



SIH will provide to DBH phone number and password from login request. The DBH then check if the phone number exist in the User table or not. If the result is positive, DBH will verify the password comes with that phone number in password column. If the verification is passed, the login status of this phone number shall be set to true, and other related information on the same row will be extract to send a response. At the same time, stored the temporally key into the database for it to become long term key (detailed description will be on Chapter). Finally set the Result of the response to "good". If phone number does not exist in the database or wrong password, the Result will be set to "bad" and no further action from DBH

Table: **user**

	phone	password	budget	vehicle_name	vehicle_mass	login
	Filter	Filter	Filter	Filter	Filter	Filter
1	0835771741	Hieu2312.	9000	None	0	1
2	0988881517	Hong1908.	100000	None	0	0
3	0967881517	Thanh2103.	5987343	None	0	0
4	0915877731	Vy1404.	9999999	None	0	0

4.2.2.2 Log out

Logging out required only phone number to execute. DBH shall set the login status false, vehicle mass to 0 and vehicle name to “None”. This way, the account status will be reset to initial state before login, and the Result will be “good”. However, this action can only be executed if the given phone number is found in the database, otherwise, no action will be done along with “bad” Result.



Vietnamese-German University

4.2.2.3 Sign up

Above actions is executed through SELECT data or UPDATE data from database. Signing up an account on other hand, DBH will INSERT INTO the User table new row representing new E-Wallet account. As long as the sign up phone number did not already exist in the database, the Result will be “good”, otherwise, “bad”.

4.2.2.4 Add money

This action required phone number and the amount of money user need to input to E-Wallet. On the User table, the budget column will be increase based on the current value and the additional added regarded the phone number.

Any action related to budget management need to be recorded in History table. Recording procedure must always have a time mark to traceability purpose if the user complain about false information about their budget displayed on the E-Wallet. The time information will be captured at the moment DBH start process budget related actions. For adding money, the money amount and existed phone number will be update in History table along with time value, other section will be left “None” or zero.

Table: **history**

phone	Longitude1	Latitude1	money	time	vehicle_name	vehicle_mass	Longitude2	Latitude2	street
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter

4.2.2.5 Retrieve money

Retrieving money request is processed exact the same with adding money but subtracting. However, DBH will give “bad” result if the amount of money user want to retrieve larger than the amount of money currently available. This checking procedure should be done on mobile device side, but for the integrity factor and prevent crashing, this should also be done on central server side independently.

Pay fee

Paying fee inherits the verification steps and DBH actions of retrieving money since it has a similar nature from central server perspective. Moreover, this action required start, end GPS coordinate and street name to record to History table. The amount of money need to be subtracted is a multiplication of vehicle mass, street based fee and distant travel:

The distance is calculated based on given GPS coordinate with the formula [derive in Chapter](#). The street based fee or road fee per kilometer data is stored in Street table, and the based value can be search by

DBH using given street name in the request. DBH retrieves vehicle mass from User table with respect to the given phone number.

Table: street	
street	fee
Filter	Filter

If the user have not registered as a driver, the vehicle mass will be 0, which is invalid, so the response will have “bad” Result and no further action from DBH shall be done to prevent unwanted budget modification to E-Wallet.

4.2.2.6 Register driver



For this request, the central server will need phone number, vehicle mass and vehicle name along with the action to update vehicle status in User table with given phone number.

4.2.2.7 Get history transaction

4.2.2.8 Get user information

4.3 Server Encryption and Decryption service

4.3.1 Vehicle profile and notify application

4.3.2 Virgin registration service

4.3.3 Acceleration sensing handler

4.3.4 Bluetooth interface handler

5 System feature results and evaluation

5.1.1 Signup virgin vehicle

5.1.2 Driver alert feature

5.1.3 Driver registration and de-registration

5.1.4 Automatic paying fee feature

5.1.5 E-wallet credit management

5.1.6 Security data exchange

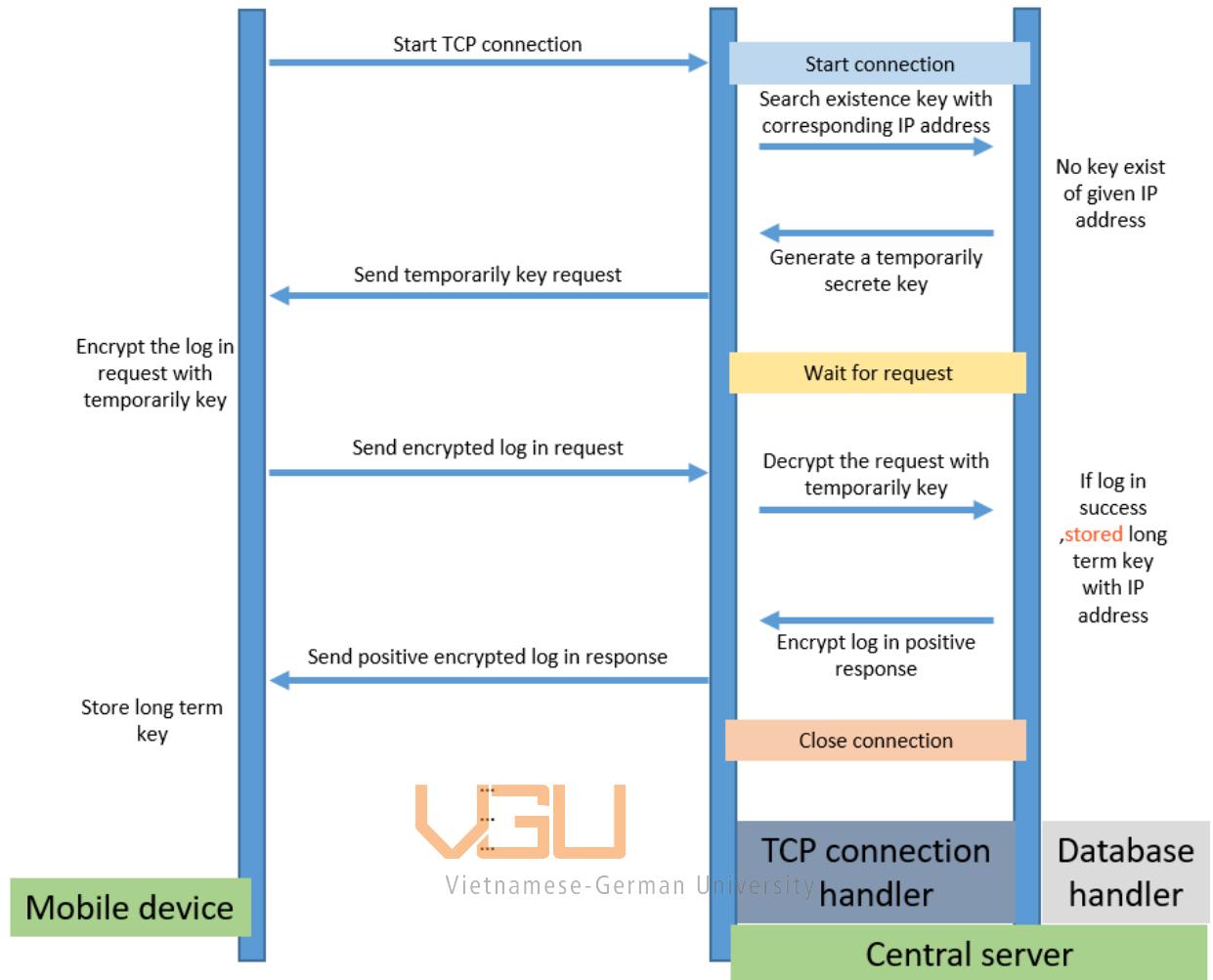
Security system used for TCP connection in this project is designed in such a way that all communication

on the central server with any random mobile device is encrypted, and if a network protocol analyzer such as Wireshark [28] try to inspect the communication, it cannot detect and extract any information while the application is running. To realize these requirements, the security data exchange procedure shall have 3 main stages:

Share long term key

Exchange data with long term key

Erase long term key



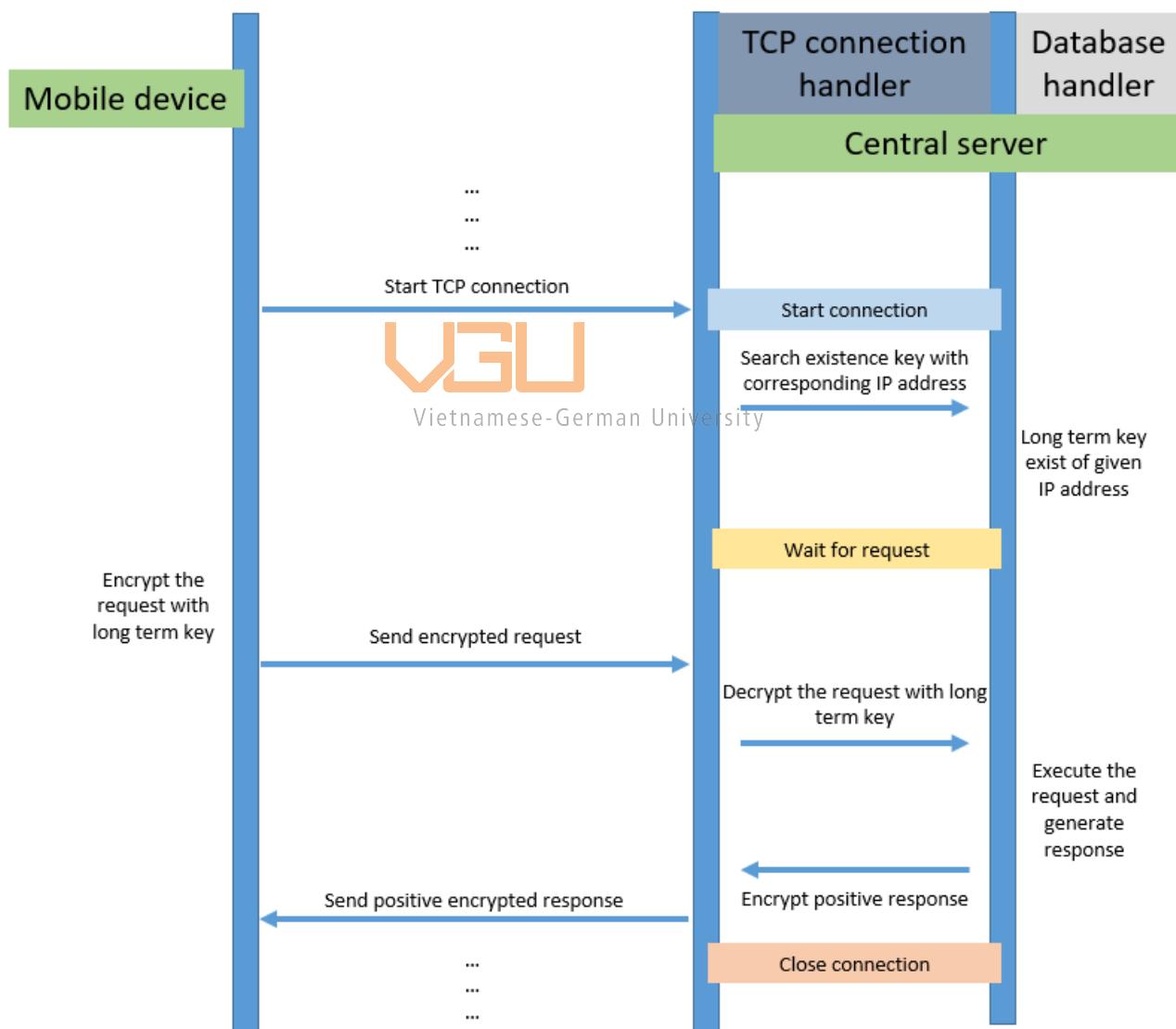
The encryption and decryption handler from both application and central server is Fernet. On mobile device side, the Fernet library is provided for Java language. On the central server side, the Fernet library is provided for Python language [29]. A symmetric authenticated cryptography communication like Fernet must have a key, which is a URL-safe based64-encoded 32-byte string, and an encryption mode, which is AES 128-bit [30] in this project .Every request sent from a mobile device to the central server must be encrypted with a temporally key or a long term key. The long term key is the official generated secrete key that stored in database to served further request handling, and the temporally key is the newly generated key at the start of a connection.

When a TCP connection is established, the central server shall use **database handler (DBH)** to search the IP address of the connection request and search in the **ipKey** table of the database.

Table: ipKey					
	ip	key1	key2	key3	
	Filter	Filter	Filter	Filter	
1	192.168.1.5	7QS1XBAyYcw	aHwgGspXJr3	-4v868HkHRG	SOoQeJ4PEW=

If the database does not consist the IP address, which means the user have not log in on the mobile device yet, the **TCP connection handler (TCH)** shall generate a fresh temporally key [31] and send it to the mobile device in **JSON message format**. On the mobile device side, it will handle this message without attempt to decrypt it and store this temporally key for the login request. The connection between the mobile device and central server shall be kept until the user proceed login action or close after 5 minutes without any response from client side. After login information is ready to be sent as request, the mobile device shall encrypt this information using given temporally key. While the TCP connection is opening, which means the temporally key generated in TCH has not been deleted, the TCH shall decrypt this message and send to DBH to proceed authorization. If the login information is valid, the DBH shall store this temporally key as a long term key along with device's IP address in the database. After that, the login success message shall be encrypted with new long term key and send to mobile device. When the mobile device decrypted the login success feedback using temporally key, this key also matured to long term key on mobile device side, in conclusion, the key sharing procedure is finished. On a circumstance where the login procedure is not success, no long term key shall be existed on both sides. At the end of this procedure, the TCH will close the TCP connection.

With a long term key created on both side of the communication, the TCH will wait for request after connection start, instead of generating new key. This communication is secured since the key sharing only occurred once and later data exchange is encrypted. However, the long term key will expire if there is no activity from the mobile device for 5 minutes. The TCH will automatically closed the connection, and when mobile device restart the connection, the sharing procedure will start again, but it is an automatically login procedure on application side if the E-Wallet is still active.



When the mobile device send a log out request, the long term key will be erased be DBH from the database, and the user have to login again to restart the whole process.

5.1.7 Limitation and future improvement



6 Conclusion



References

- [1] "Toll road," [Online]. Available: https://en.wikipedia.org/wiki/Toll_road.
- [2] N. M. J. K. Rajeshwari Hegde, "Automation of Toll Gate and Vehicle Tracking," in *International Conference on Computer Science and Information Technology*, Singapore, 2008.
- [3] H. Cong, "De xuat xay 34 tram thu phi oto vao trung tam Sai Gon," VnExpress, 17 July 2019. [Online]. Available: <https://vnexpress.net/de-xuat-xay-34-tram-thu-phi-oto-vao-trung-tam-sai-gon-3953543.html?fbclid=IwAR3UssgzzDKGp6SF7npb7B73ubHII9b6bgZICG-si9COqWi1lxz1ZBW-eZk>.
- [4] "vietnambiz.vn," 90% thi truong vi dien tu thuoc ve Zalo Pay, Moca va Momo, nhung doi thu den sau van con co hoi lon, 25 March 2020. [Online]. Available: <https://vietnambiz.vn/90-thi-truong-vi-dien-tu-viet-thuoc-ve-zalopay-moca-va-momo-nhung-doi-thu-den-sau-van-con-co-hoi-lon-20200325151851209.htm>.
- [5] "Configurations/Roles," [Online]. Available: https://www.amd.e-technik.uni-rostock.de/ma/gol/lectures/wirlec/bluetooth_info/k1_gap.html#Configurations/Roles.
- [6] U. government, "GPS.Gov," U.S. government, 2013. [Online]. Available: <https://www.gps.gov/multimedia/poster/>.
- [7] U. Government, "Featured Video: GPS SMC 2.0 Adaptability & Flexibility," GPS.Gov, 2019. [Online]. Available: <https://www.gps.gov/multimedia/videos/>.
- [8] "Activity," Google, [Online]. Available: <https://developer.android.com/reference/android/app/Activity>.
- [9] "Understand the Activity Lifecycle," Google, [Online]. Available: <https://developer.android.com/guide/components/activities/activity-lifecycle>.
- [10] "Fragments," Google, [Online]. Available: <https://developer.android.com/guide/fragments>.
]
- [11] "Layouts," Google, [Online]. Available: <https://developer.android.com/guide/topics/ui/declaring-layout>.
- [12] "Android 3.3 release note," Google, [Online]. Available: <https://developer.android.com/studio/releases#3-3-0>.
- [13] "Get started with the Navigation component," Google, [Online]. Available: <https://developer.android.com/guide/navigation/navigation-getting-started>.

[14] "Fixed start destination," Google, [Online]. Available:
] https://developer.android.com/guide/navigation/navigation-principles#fixed_start_destination.

[15] "findViewById," Google, [Online]. Available:
] [https://developer.android.com/reference/android/view/View#findViewById\(int\)](https://developer.android.com/reference/android/view/View#findViewById(int)).

[16] "Ma dien thoai Viet Nam," Wikipedia, [Online]. Available:
] https://vi.wikipedia.org/wiki/M%C3%A3_%C4%91i%E1%BB%87n_tho%E1%BA%A1i_Vi%E1%BB%87t_Nam.

[17] "Button," Google, [Online]. Available:
] <https://developer.android.com/reference/android/widget/Button>.

[18] "Bundle," Google, [Online]. Available:
] <https://developer.android.com/reference/android/os/Bundle>.

[19] "Text Watcher," Google, [Online]. Available:
] <https://developer.android.com/reference/android/text/TextWatcher>.

[20] "Class IOException," Oracle, [Online]. Available:
] <https://docs.oracle.com/javase/7/docs/api/java/io/IOException.html>.

[21] "Set up bluetooth," Google, [Online]. Available:
] <https://developer.android.com/guide/topics/connectivity/bluetooth#SettingUp>.

[22] "Intent," Google, [Online]. Available:
] <https://developer.android.com/reference/android/content/Intent>.

[23] "Broadcast Receiver," Google, [Online]. Available:
] <https://developer.android.com/reference/android/content/BroadcastReceiver>.

[24] "Publish–subscribe pattern," Wikipedia, [Online]. Available:
] https://en.wikipedia.org/wiki/Publish%E2%80%93subscribe_pattern.

[25] I. Bluetooth SIG, "Configurations and roles," in *Bluetooth Core Spec, 5nd ed., Vol 3, Part G, Chapter 2*, p. 2223.

[26] "Connect as a client," Google, [Online]. Available:
] <https://developer.android.com/guide/topics/connectivity/bluetooth#ConnectAsAClient>.

[27] C. Macasaet, "Fernet Java," [Online]. Available: <https://github.com/IOs/fernet-java8>.
]

[28] "About Wireshark," Wireshark, [Online]. Available: <https://www.wireshark.org/>.
]

[29] "Fernet (symmetric encryption)," [Online]. Available:
] <https://cryptography.io/en/latest/fernet.html#fernet-symmetric-encryption>.

[30] "Advanced Encryption Standard," Wikipedia, [Online]. Available:
] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[31] "classmethod generate_key()," [Online]. Available:
] https://cryptography.io/en/latest/fernet.html#cryptography.fernet.Fernet.generate_key.

