Mobile-Device-Based Solution for Non-motorized Users and Traffic Signal Control System Interactions

Yifan Ling

A thesis

submitted in partial fulfillment of the

requirements for the degree of

MASTER OF SCIENCE IN CIVIL ENGINEERING

University of Washington

2022

Committee:

Yinhai Wang

Xuegang (Jeff) Ban

Edward McCormack

Program Authorized to Offer Degree:

Department of Civil and Environmental Engineering

University of Washington

ABSTRACT

Mobile-Device-Based Solution for Non-motorized Users and Traffic Signal Control System Interactions

Yifan Ling

Chair of the Supervisory Committee:

Yinhai Wang

Department of Civil and Environmental Engineering

Pursuing smart traffic systems for non-motorized users has been becoming more important in the past few years. Non-motorized road users are requiring more efficient and user-friendly infrastructure facilities with improved equity, especially at the intersection areas. However, most existing achievements in this field either proposed overcomplex solution and led to lacking reliability and scalability, or proposed something that were not keeping pace with time enough to improve users’ accessibilities. Therefore, in this research, a new system is proposed to replace the traditional push-button switch or traffic lights. The system utilized a roadside device as the communication media between signal controller and user, and users only need to install a mobile phone app to use the system. Compared to existing similar solutions, our solution introduced a smart gateway to achieve multiple protocols integration. The proposed phone app that can also classify users according to their motions, different non-motorized user groups can now easily view their waiting time and sending crossing request manually or automatically without searching for the physical push-button switch and press it. Our experiments indicates that our system is a touch-free, quick responding, reliable and highly accessible for all user groups. In addition, this proposed system is the first equity-aware solutions for both normal and vulnerable users and can completely replace the traditional physical push-button system.

Table of Contents

List of Figures

List of Tables

ACKNOWLEDGEMENTS

Remembering the people who supported me the most throughout my academic life is important. Therefore, I want to thank my parents for giving me both mental and financial support during my study. With their selfless support, I managed to spend most of my academic life in a foreign country relatively easily, without the need of worrying too much about surviving, especially during the pandemic.

It is also a privilege to study and work at the fantastic UW STAR Lab. I want to thank Professor Yinhai Wang for providing me a spot in this lab and funding me for my research work. He did not only give us advice about our academic work, but also provided his opinions on this constantly-changing world, and many of his opinions are quite helpful and inspired me to judge things from different perspectives as before. In addition, I also want to thank my lab members for providing me helps and knowledges on my projects, especially Hao (Frank) Yang, who introduced me a lot of new technologies that I had never even heard of, and those turned out to be very useful to my projects.

I am also grateful that Professor Jeff Ban and Professor McCormack could be my committee members. My graduation schedule turned out to be a little too tight, but their helps really made the whole process a lot easier. I would also like to thank the Washington State Department of Transportation (WSDOT) for funding the project entitled “Extending the SR-522 SPaT Challenge to Active Transportation Users”, and the Pacific Northwest Transportation Consortium (PacTrans) at Regional University Transportation Center (UTC) for Federal Region 10, for funding my research.

Different from many other students and researchers major in transportation engineering, I have a special interest in cetacean photography, identification, and protection. Therefore, I would like to thank all the whale researchers, photographers, and my friends. And most importantly, I would like to all my 14,000+ followers of my social media accounts for their support. Although these people did not directly contribute to my thesis, they provided significant spiritual support during my academic life.

Most people will pay their gratitude only to human, but I also want to include some animals here. One animal is my cat Max. He has been living with me for more than 4 years, and in most of the time, he was gentle and well-behaved, and helped me went through countless lonely and struggling nights. I also want to thank all the 153 killer whale individuals I have encountered in the Salish Sea. They are the most amazing wild lives on this planet and are the main source of my happiness, especially the Southern Resident Killer Whale J39 Mako. I wish them long lives.

Chapter 1. Introduction

1.1 General Background

Traditional traffic infrastructures lacking optimizations has becoming a more significant issue in recent years. Smart, reliable, and user-friendly infrastructure facilities are currently one of the most needed innovations in transportation industry, and this type of infrastructure is especially important at the intersection areas. Many researchers have already been working on this topic and showed that there are lot of potential approaches to achieve the goal. However, although these research teams all gave out solutions to solve the problem, most of these solutions proposed are either too complex to use, too expensive, lacking scalability, lacking reliability, or lacking efforts on improving users' accessibilities. However, among these research projects, a trend can be observed: the most practical, user-friendly, and flexible platform for solving the issue is mobile device. Mobile device has already become one of the most essential tools in lives of almost all people, and the current hardware installed in the mobile phones can provide strong and reliable computing power. These advantages mean that if mobile devices are chosen as the platform, researchers can potentially be able to develop a reliable, easy-to-upgrade, and powerful system to replace the traditional push-button switch and optimize the intersection areas. However, there still has to be a method to connect the mobile phone with the infrastructure to make the system really usable. The most popular solution for this in recent years is edge devices. For specifically solving this issue, the edge device needs to be compact, robust, and powerful, and that is what the UW STAR Lab is capable of developing, and this final piece of puzzle makes the whole project feasible.

1.2 Signal Phase and Timing (SPaT)

Signal Phase and Timing (SPaT) refers to the operations conducted, and information provided by a specific intersection or the connected intersection network. As intelligent transportation system (ITE) becoming more popular and significant in today’s transportation infrastructure developments, SPaT information is now critical to many aspects of the transportation projects, especially the when the projects are related to pedestrians or drivers, fast and precise SPaT information is indispensable. SPaT can be provided as a service to different types of the road users including pedestrians, bikers, drivers etc. To provide SPaT services, usually both onboard equipment (OBE) and roadside equipment (RSE) are required. RSEs are commonly used to send the information out from the signal controllers so that the information can be spread out for users to collect, and OBEs are usually used to receive, or even translate and show the information received from the RSEs. With the SPaT service provided, the safety level of the intersections can potentially be improved, and it is very important that road users can cross the intersections in a fast and safe manner. SPaT services can not only provide the possibility of sending and receiving signal timing information as a one-way procedure, but also provide the possibility of road users interacting with transportation infrastructures, and such interactions can greatly improve the efficiency of the intersection. Therefore, SPaT service is critical to transportation development and will be used more widely as an important part of road users-infrastructure communications in the future.

1.2.1 Current Practice

In today’s transportation infrastructure industry, the connection between road users and transportation infrastructure is extremely limited. At most intersections, traditional systems are still in use, and the only connection between traffic lights and road users is road users observing the signals with their own eyes and make reactions. There is a common practice to add interactions between road users and infrastructures, which is the push-button on the light pole. These buttons are designed to let some of the road users active a specific timing plan in the signal controller. However, these buttons do not always work properly, and some of them were not even physically connected to the traffic lights, they are only there to make road users feel that they can have some control. People who use the push-button do not really know what are going on behind the button, the reaction time is a question, the changes to the timing plan is a question, and even the functionality of the button is a question to the users, and this is very unideal to improve the efficiency of the intersection and may even potentially cause negative effects on road users. Also, currently none of the push-button in service took user accessibility into consideration during the design and has no contribution to improve equity. There are some intersections used as test platforms for new technologies to evaluate their feasibilities, but those are not considered mature technologies that are widely applied. Therefore, the current practice is still not satisfying and not technologies and solutions are needed.

1.2.2 Problem Statement

People walking, jogging, and even biking or using a wheelchair can all be classified as non-motorized users. Because there are plenty of regulations for motorized users to follow, compared to motorized road users, non-motorized road users, who do not have many regulations and rules and are more diversified and random, is a more complex group to manage. But in reality, although motorized users do not conflict with non-motorized users in most cases, some scenarios join the two groups together, and among all such scenarios, one of the most important ones is when non-motorized road users crossing the road. To provide these users with safe and user-friendly infrastructures is an important task which needs more research and need improvements.

However, traditional transportation infrastructures cannot fulfill the task. Physical push-button switches on light poles do not have good access for all types of non-motorized road users. Many of these push-button switches are either poorly designed or placed on locations with low accessibility. In some cities and regions, these push-button switches have even become “placebo buttons” [1] that only look and feel like functional, but are malfunctioning or not even designed to send triggers to the signal controllers, they are just installed to comfort non-motorized road users.

1.3 Idea Generation

Although most of the current approaches really solved all the problems in reality, some of them still have potential to become a solution for these problems in the future, and were taken into consideration for the project. The UW STAR Lab’s past projects has improved some of the old methods. For instance, although video cameras still cannot reach close to 100% correct detection rate, due to the evolution of AI algorithms, the accuracy of video cameras has been greatly improved, and due to the endeaver of the lab members on video camera supporting accessory design, the performance and realiabity of this solution has already been greatly improved. However, in extreme cases, the camera can still make false judgement and even break down, because the system has to take all the computing stresses and part of it, which is the camera, need to be exposed to the outer environment, and these are currently inevitable issues, and these issues result in it becoming a far from perfect and therefore unideal solution for the project.

Improving the physical push-button is another solution that was taken into consideration. The physical push-button is reliable, because it is directly connected with the signal controller and make physical contact with users. Therefore, it is unlikely for it to make mistakes on counting users with crossing demands. However, the COVID-19 pandemic has already shown that physical contacts with users may result in negative impact on public health. In addition, it does not have the ability to optimize its performance by classify users and always keep good accessiblity because it cannot recognize user type and its physical position is predetermined. These are also inevitable and it will be very hard to improve the existing system. Therefore, the focus is turned to mobile devices.

Figure 1-1 Feature summary of the new solution.

Although a handful of researchers has been working on the mobile phone approach of helping non-motorized users crossing the road, some imperfections still exist. However, mobile phone is a very flexible platform which can provide unlimited possibilities. Accessibility problem can be solved by using mobile phone's wireless connection function; user classification problem can be solved by detecting users' movements or ask users to classify themselves; functionality and reliabilty can be solved by moving stressful works to edge devices, thus make the mobile phone side simple and unlikely to make mistakes; and finally, due to the nauture of mobile devices, it does not require users to touch and public equipmnet therefore will not harm the public health. And the above is how the solution was generated.

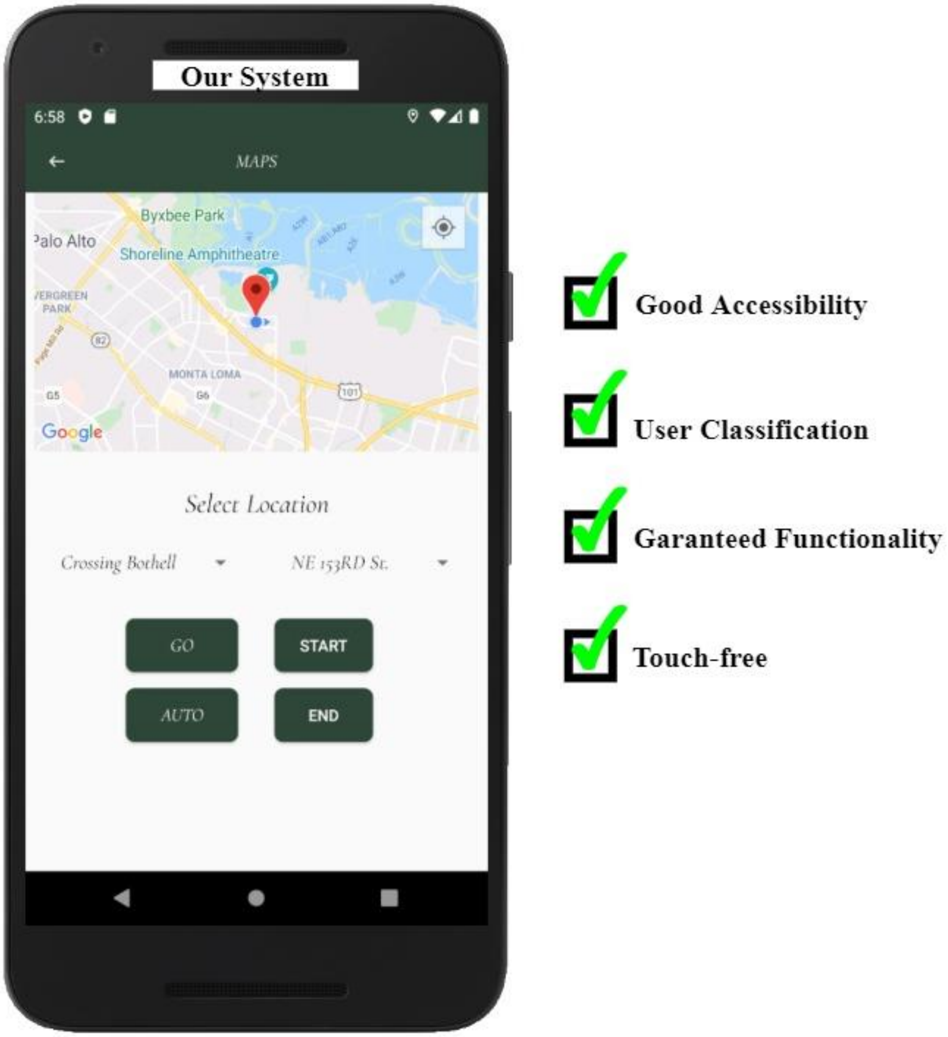


Figure 1-2 Feature summary of the new solution.

1.4 Research Objectives

The system is designed to have the following key features:

- A highly integrated mobile phone app that can both help ordinary non-motorized road users crossing the road while also help researchers collecting pedestrian behavior data in a restricted availability and range without disturbing users' privacy. With carefully designed user interfaces, non-motorized road users can easily know the remaining waiting time and send triggers to the controller.
- Fast, stable, and reliable wireless connection between mobile phone and traffic infrastructure. Thanks to the Smart Gateway developed by the team member, the new system can provide an extensive signal transmitting range in the targeted area, and non-motorized road users can use the app functions from tens of meters away, and eliminated the need of non-motorized users pressing the push-button switch right in front of the traffic light pole. And due to the message transmission logic, chance of user private data leakage is very low.
- Powerful roadside device that reliably connects the mobile phone user and the signal controller. Our roadside device uses UDP protocol to provide fast wireless communications and no need to worry about problems such as losing data packets. Together with wired connection between the roadside device and the signal controller, internal connections within the whole system are seamless.
- User equity is considered throughout the project. Using wireless connection, user direct input and user classifications, users with inconveniences have more choices when they are willing to tell their presence to the signal controller. Also, we provided the possibility for

signal controllers changing the signal timing plans based on the type of non-motorized users who want to cross the road.

Chapter 2. State of the Art

2.1 Transportation Infrastructure Connecting Technology

When discussing about connected transportation infrastructures, DSRC is usually the first technology that comes into mind. V2I (vehicles to infrastructure) communication, V2V (vehicle to vehicle) communication, and V2X (vehicles to other non-motorized users) can be accomplished using DSRC communication technology. According to the Society of Automotive Engineers [2] the format of message DSRC-supported devices can send and receive is defined as “Dedicated Short Range Communications Message Set Dictionary.” For DSRC technology, although it has received much attention, the most updated standard of the technology is as old as 2016, and that version is labeled as the SAE J2735-2016 Standard. “the purpose of this SAE Standard is to support interoperability among DSRC applications through the use of a standardized message set, and its data frames and data elements” [3]. Communication and control with high efficiency and reliability must be a key feature of intelligent transportation system. And to encourage research on connected vehicles (CV), the United States Department of Transportation has highlighted the need of an interoperable by adding interoperability as one of the most important parts in the “ITS Strategic Plan 2015-2019” [4]. While a broad concept in scope, the main goal of interoperability is to ensure that communications between devices in ITS applications can persist over time and in different locations, especially when the devices to be communicating were not necessarily built at the same time, nor by the same manufacturer etc. [4, 5]. The SPaT Challenge is aimed to bring CV technology efficiently and safely to all 50 states. Regardless the manufacturer of the equipment, the location the equipment is built, and the time it needs to be used. The standard of the technology needs to be consistent in order to clearly defining the information transferred between different types of user groups over time.

SAE’s philosophy when it comes to DSRC for CV applications is to try to use the wireless communication bandwidth, itself with a finite capacity, as efficiently as possible by defining compact messages via a three-component hierarchy that makes use of the Abstract Syntax Notation revision One (ASN.1) [3]. The top part in the whole system are the messages themselves, then it is the data frames, which are used to build up the messages. And after that, it is the data elements. These are the attributes that define each data frame [3]. It is worth mentioning that the data frames do not necessarily build up messages, they can also build up other data frames. As messages, data frames and data elements work together, they build up a messaging hierarchy to complete the system.

SAE J2735-2016 mentioned various different types of CV messages, among them, the most frequently mentioned type is Basic Safety Message (BSM). BSMs are the cornerstone of V2V safety applications, are often sent at a frequency of 10 Hz, and the information used to define them is obtained from sensors within the vehicle [6]. According to SAE standard, the primary data frame that builds up the BSM messages is BSMcoreData, which is composed of both data elements and data frames that are essential to deliver any BSM message. These frames and elements include, but are not limited to latitude, longitude, elevation, transmission state, speed, heading, steering wheel angle, brake system, status, vehicle size, etc. [3]. To clarify a bit on how data frames themselves can be composed of other data frames, one can note that vehicle size is a data frame, itself comprised of two data elements, vehicle width and vehicle length [3]. Although BSM messages are part of the CV research, it will not be used in this project because it still needs to be simplified.

According to the National Operations Center of Excellence [7], the issuer of the SPaT Challenge, the focus of the challenge will be to equip intersections with the necessary hardware to enable SPaT broadcasts via DSRC. NOCoE also notes that additional message broadcasts of the MapData (MAP) and Radio Technical Commission for Maritime Services Corrections (RTCM) varieties should take place in conjunction with the SPaT broadcasts [7]. The grouping of these three messages allows vehicles to determine their location with respect to the intersection, as well as obtain state information on signal indications that are relevant to their desired movements [8].

The SAE J2735 mentioned that "the MapData message is used to convey many types of geographic road information" [3]. For better understanding, a more detailed overview of the contents of the message based on SCRT (2018) is illustrated in the following. The MAP message has a basic concept, which is overall location of the intersection is set to be the middle point of the intersection, and each intersection has a unique integer identifier labeled. After this geometry has been set up, based on the current coordinate, lane geometry will then be calculated according to a distance between the predefined center point and the stop line of each lane. The rest of the lanes will then be set as a serious of individual dots or nodes along the centerline of the calculated lane. The location of the dots can be defined in 2 different ways: One is that giving the dot a precise coordinate with longitude and latitude, the other one is calculate the distance between the current dot and the previous dot, and therefore get the location. Crosswalks can also be calculated with the similar way as the way to calculate lane geometry. The message will also contain the information about vehicle movements allowed from each lane for both inbound and outbound. After all the above information is setup, the paths of vehicle movements can have relation with the signal timing information. These connections are then mapped to corresponding signal groups that define signal phasing [8].

SPaT messages are the messages that need to be transmitted between the transportation infrastructure and other users. They further have a variety of applications including improvements in safety, operations, and reduction in the environmental impact of fossil-fuel-based vehicular transportation [6].

As with the MAP message, the following will provide a more concise summary of the information conveyed in the SPaT message based upon SCRT (2018). In the MAP message, each SPaT message can be referred to a specific intersection as a unique identification has already been given. The SPaT messages are able to send status information of the intersections both generally (as an individual object) and specifically (as precise as which signal phase). As for the general intersection information, the messages can show whether the controller of the intersection is conducting a fixed or actuated control plan. The messages can also show as well as if it is running in special modes such as failure flash mode. When the SPaT message about the intersection is in detail, it can send the intervals of green, amber, and red, and give out an estimate of how soon the specific phase or the light will end at any given time, along with the confidence of these estimates, and it can also tell the time until the green indication will show again. Finally, the SPaT message can also run a function called “Connection Maneuver Assistance,” which is focused on pedestrian crossings. This feature allows for the message to include information on pedestrian actuations as well as actual pedestrian detection in the crosswalk (if supporting detection infrastructure is available) to alert drivers that active users may be in the crosswalk (for applicable conflicting movements) [8].

The last type of message that can be potentially useful for the SPaT Challenge is the RTCM message. To help vehicles on the road more precisely determine the locations of the lanes in interest predefined by the MAP message, global positioning system (GPS) is used and a correction factor of the GPS information calculated by the current atmospheric conditions is added to the system. Correction factors can either be computed at a base station or edge device at a specific intersection or can be calculated remotely, such as being calculated at a traffic management center (TMC)). Whether to apply RTCM messages or not is determined by a variety of factors, these factors include who complex the intersection geometry is, such as if there are lanes specifically designed for turning movements, as well as whether the intersection is impacted by the urban heat island effect or not. However, the RTCM technology has some limitations, for example, it is worth noting that not all GPS systems within vehicles can apply the information from the RTCM messages [8]. As with the preceding two message types, the information presented here is more of a high-level summary of key message features as obtained from SCRT (2018); further information for RTCM message can be found in SAE (2016). Finally, it is important to state that transportation researchers has been trying to improve the vehicle localization precision, and it is clear that applying RTCM messages is for certain not the only way to complete the mission. For example, studies including Rohani et al. [9] and Shen et al. [10] present some vehicle localization solutions that do not rely on fixed base stations.

2.2 CV Technology Based Safety Application

3 different categories can be used to differentiate CV Technology Based Safety Application depending on what type of users are the senders and receivers of the information: V2V, V2I and V2X. The following paragraphs will present an overview of different safety applications in each of the three aforementioned categories, as well as studies that have investigated such applications [11].

V2V safety applications usually use direct DSRC communication between vehicles. Several possible V2V safety applications as indicated by USDOT are presented in the following [11]:

- Intersection Movement Assist (IMA): Suitable to be used at both controlled and uncontrolled intersections, drivers will receive warning alerts of high-crash risk probability at specific intersections and will be suggested to not proceeding through the intersection.
- Left Turn Assist (LTA): When driving into a specific intersection, drivers will be warned to not turning left in order to avoid positive corner collision with the vehicles on the targeted lane.
- Forward Collision Warning (FCW): Drivers will receive warning message of potential collision of the driver's vehicle and the rear end of the vehicle at the front.
- Emergency Electronic Brake Lights (EEBL): When V2V communications are available, drivers will be warned when the downstream vehicle performs a hard brake, regardless of whether the driver can immediately see the braking vehicle or not.
- Blind Spot Warning/Lane Change Warning (BSW/LCW): When performing a lane change, the driver will be warned if there is a vehicle staying or approaching in the driver's blind spot along the targeted lane.
- Do Not Pass Warning (DNPW): Drivers will receive a "do not pass" message if there exists potential risk of head-on collision when performing the pass.

Although sounding similar, USDOT and NHTSA denote LTA and IMA as separate applications [11]. Specifically, IMA is proposed to address the following crash types: “straight crossing paths at non-signal, left turn into path at non-signal (LTIP), right turn into path at signal (RTIP), running red light, and running stop sign” [11]. LTA is intended solely to address crashes where a left-turning vehicle would be hit by a through-moving vehicle in the intersection [11].

V2I technology based safety applications usually require the communication between road side equipment or other infrastructure components and vehicles. The following presents several common V2I applications per USDOT (NDb) [12]:

- Red Light Violation Warning (RLVW): If the SPaT messages indicate that there is a possibility that the driver will run a red light, the driver will receive a warning message.
- Curve Speed Warning (CSW): If the driver is driving too fast to go through a curve safely, the driver will receive a warning message.
- Stop Sign Gap Assist (SSGA): When potential scenarios of collision at a stop-sign-controlled intersection, drivers will receive warning.
- Spot Weather Impact Warning (SWIW): Drivers will receive warning messages about severe weather conditions if the driver plan to drive through it.
- Reduced Speed/Work Zone Warning (RSWZ): Drivers will be warned if there are some regulatory traffic conditions, such as reduced speed limit, in a work zone.
- Pedestrian in Signalized Crosswalk Warning: Drivers will be alerted if there are some pedestrians in the crosswalks that the driver plan to drive through during a turn. According to the Connected Vehicle Reference Implementation Architecture Team, this warning was designed for use in transit applications, but it can be generalized for all vehicles [13]

The USDOT is currently funding 3 different CV technology pilot programs: the New York City DOT Pilot (NYCDOT Pilot), the Tampa-Hillsborough Expressway Authority Pilot (THEA Pilot), and the Wyoming DOT Pilot (WYDOT Pilot). All 3 programs involves the installation of RSE, the testing vehicles are modified to be able to sending and receiving DSRC messages in order to test V2I, V2V and applications in real world under different circumstances. As of late 2018, the pilot projects were in a phase of operations and maintenance, where applications are continuing to be tested and have their performance evaluated [14]. The main goal of the NYCDOT Pilot is to test a variety of DSRC-enabled safety applications along instrumented corridors in Manhattan and Brooklyn [15]. The THEA Pilot will have a large focus on improving traffic operations in Downtown Tampa, as well as targeted safety applications such as providing warnings to prevent wrong-way driving [16]. Finally, the WYDOT Pilot focuses on a test site on Interstate 80 (I-80) to test safety and mobility applications primarily aimed at freight and commercial vehicles; compared to the other sites this site is subject to extremely adverse winter weather and applications surrounding weather alerts and guidance information will be among the central applications [17]. Table 1 shows the CV applications that were proposed for each of the test sites per USDOT [15, 16, 17].

Table 2-1 CV Applications for USDOT Pilots (table created from combination of (USDOT, NDc, USDOT, NDd, USDOT, NDe))

Project	Category	Application
NYCDOT Pilot	V2I Safety	Speed Compliance
		Curve Speed Compliance

		Speed Compliance/Work Zone
		Red Light Violation Warning
		Oversize Vehicle Compliance
		Emergency Communications and Evacuation Information
	V2V Safety	Forward Collision Warning
		Emergency Electronic Brake Lights
		Blind Spot Warning
		Lane Change Warning/Assist
		Intersection Movement Assist
		Vehicle Turning Right in Front of Bus Warning
	V2I/I2V Pedestrian	Pedestrian in Signalized Crosswalk
		Mobile Accessible Pedestrian Signal System
	Mobility	Intelligent Traffic Signal System
THEA Pilot	V2I Safety	End of Ramp Deceleration Warning
		Wrong Way Entry

		Pedestrian in Signalized Crosswalk Warning
		Pedestrian Transit Movement Warning
	V2V Safety	Emergency Electronic Brake Lights
		Forward Collision Warning
		Intersection Movement Assist
		Vehicle Turning Right in Front of a Transit Vehicle
	Mobility	Mobile Accessible Pedestrian Signal System
		Intelligent Traffic Signal System
		Transit Signal Priority
	Agency Data	Probe Data Traffic Monitoring
WYDOT Pilot	V2V Safety	Forward Collision Warning
	V2I/I2V Safety	I2V Situational Awareness
		Work Zone Warnings
		Spot Weather Impact Warning
	V2I and V2V Safety	Distress Notification

Table 1 shows that both THEA and NYCDOT focused on pedestrians’ mobility and safety improvements while implementing CV applications. It is worth noting that both of these projects studied the application of Mobile Accessible Pedestrian Signal applications. Mobile Accessible Pedestrian Signal application presents signal status information to pedestrians and can allow them to make a call for signal service at intersections with pedestrian actuation [18].

Apart from those research teams that work directly for the USDOT CV pilot projects, there are some other research teams that are developing applications for improving pedestrians’ mobility and safety. One application that was developed for the Safe Intersection Crossing Project as funded under the Accessible Transportation Research Initiative (ATTRI), which is a cooperative research effort from USDOT, FHWA, the Federal Transit Administration (FTA), the ITS Joint Program Office, and the National Institute of Disability, Independent Living, and Rehabilitation Research (NIDILRR) [19]. ATTRI research has sought to address the transportation needs of people with disabilities, veterans with disabilities, and elderly people through projects with focus on technological solutions in the areas of "wayfinding and navigation, assistive technologies, automation and robotics, data integration, and enhanced human service transportation" [19]. In Pennsylvania, researchers at Carnegie Melon University (CMU) developed a mobile app for Safe Intersection Crossing Project. The app could create communication between pedestrians and the signal controller, and the system was tested at a test site in Pittsburgh, PA. The app the CMU team developed allowed users to see SPaT information and make sure their requests were fulfilled by the signal system. Based on detection of app users, the system could estimate when the pedestrian would arrive, and adjust the signal timing plan according to the request, such as adding additional green time if the current situation is permitted. To properly use this system, users not only needed to run the app, but also had to equip their phones with customized sleeve (or case) that fit over the phone and extended it to have the necessary DSRC capabilities to communicate with RSE [20]. In Minnesota, Liao et al. [21] developed a Mobile Accessible Pedestrian Signals (MAPS) system with a focus on improving the crossing experience for pedestrians with vision impairment. They also developed an app to work with their system, the app they obtained enabled users to obtain intersection geometry data, and it also allow users to send crossing request for a given crossing direction to the signal controller.

Currently, because there are not many CV testbeds available yet, many research teams focus more on the performance and efficiency of the important factors related to DSRC as well as some other ways to transfer safety information. Yin et al. [22] simulated a DSRC vehicular ad hoc network in which vehicles were using a collision avoidance algorithm. They pointed it out that although DSRC did not have serious communication latency, the throughput capacity of this technology still has space to be improved. Liu et al. [23] developed a V2X communication system rooted in Wi-Fi that allowed vehicle to pedestrian communication and determined through field tests with actual vehicles and pedestrians that communications worked well when the distance between devices was less than 150 m. Other research team put more emphasis on applications of the technology. Sugimoto et al. [24] developed a collision risk estimation algorithm for vehicle and pedestrian crashes that relies on cellular communications between vehicles and pedestrians and a vehicle's GPS system. They pointed out that one of the tests of their application showed ability to give drivers more reaction time to respond to pedestrians that were not immediately within their sight. Hussein et al. [25] developed a crash prediction algorithm based on communications between vehicles and pedestrians. The algorithm they developed was able to be run on a smartphone to access current location and direction of the smart phone user, then the location information of the users can be shared among other users on the road, with these being done, time and location of the potential collisions can be estimated, and a warning message might be sent to the smart phone users based on how severe the estimate result will be. Anaya et al. [26] developed an app and collision prediction algorithm for vehicle-pedestrian crashes that estimated collision risk and warned pedestrians of said risk via the app. This app relied on Wi-Fi connection and the results showed that packet delivery ratio was negatively impacted because of people's bodies blocking the Wi-Fi signals.

2.3 Security Overview

Cyber security is a very important aspect that needs to be considered when developing communications between mobile devices and roadside units (RSU), and its robustness directly impact the reliability of the communication system. Currently, an increasing number of smart devices comprise a new series of targets for cyberattacks due to increased [27, 28]. In most cases, cyberattacks only happen when the attacker is within the communication range of the victim, and depending on what type of technology the communication is based on, the attacking distance varies. Therefore, cyber security is addressed in the connected environment for a variety of applications including, but not limited to, vehicle-to-vehicle (V2V) communications, vehicle-to-infrastructure communications (V2X), and even train control systems [29, 30]. No matter the application, secure and uniform practices should be applied to the entire connected environment encompassing vehicles, traffic signals, work zones, and many other parts of the connected vehicle ecosystem [31]. To date, several studies have focused on cyber security in the connected vehicle environment [32, 33, 34].

In real life CV application, to prevent collection, V2V and V2I communications are needed, and currently the main communication protocol for both V2V and V2I is DSRC. DSRC uses multiple standards – IEEE 802.11p [35] wireless access for physical layer and medium access control functions, IEEE 1609.2 [36] for security services, and IEEE 1609.3 [37] for network services. When using DSRC as the communication protocol, it is possible that a malicious node hacks into the DSRC supported devices and sends harmful information. Also, denial of service (DoS) is another potential type of attack. Lyamin et al. [38] studied the jamming DoS attacks in IEEE 802.11p when a malicious node corrupts the exchanged safety messages in a platoon. For most such attacks, the IEEE 1609.2 standard provides methods to authenticate and encrypt messages, and the centralized solution can be applied to protect the CV environment via applications such as the Connected Vehicle Cloud (CVC) system developed by Ericsson [39]. The CVC system represents a novel platform for vehicles, various services and support provided by OEM partners. The security layer provided in the CVC ensures that the communication between the vehicle and the system is encrypted. Zhang et al. [40] built a defense framework for malware and presented a lightweight malware defense function which can operate in vehicles.

Application of mobile phone based infrastructure connection on the other hand brings more challenges to the SPaT system. The phone apps themselves suffer security vulnerabilities that can lead to personal data leakage and malware infection [41]. The issue of personal data leakage from mobile phones typically results from unsafe mobile apps which are embedded with specific code to steal and transmit sensitive data [42]. Malwares is another great threat to the mobile based SPaT system, and among various of malwares, Botnets are considered the greatest threat. Botnets are used to send email spam, carry out distributed denial of services (DDoS) attacks, and for hosting phishing and malware sites [43, 44]. Currently, Botnets are slowly switching target to smart devices such as smart phones because these devices are widely used, and most of them have hardware that are powerful enough to run Botnets and may even add more power for a bot-master.

With PC-based botnets, cybercriminals often use zombies within botnets to launch DDoS attacks, which may happen in the near future on mobile platforms [45].

2.3.1 Cyber Security Overview on Connected Infrastructure

SAE defines cybersecurity as “measures taken to protect a cyber-physical system against unauthorized access or attack” [3]. As what is mentioned above, cyber-physical system is defined as a system made up of communications and computer devices used for control applications [3]. For this project, the main components of the cyber system of interest are vehicles installed with OBE, the signal controller and associated RSE, and the mobile device used by pedestrians. Because this project aims to set up the communications between mobile device and the RSE as well as the RSE and vehicles’ OBE, it is important to focus on different types of cybersecurity challenges to ensure the system’s safety. The following part discusses some common cybersecurity challenges and some potential ways to address the possible issues.

Schlack [46] described cybersecurity issues facing the network of traffic signals in Washtenaw County, Michigan. He mentioned that the county’s traffic signal controllers can communicate using either 900MHz or 5.8GHz bands, a hacker can easily find the controllers’ network service set identifier (SSID), and interfere with the traffic controllers using only a radio and a laptop. In a test conducted by Ghena et al. [47], it was found that with such simple tools one could activate the management malfunction unit (MMU), and potentially even control the signal timing. As a result of the experiment, it was recommended that agencies should use encryption methods, make SSIDs invisible to the public, use firewalls to prevent access to unused ports, and make sure that firmware is always set to the most recent version [46, 47]. Perrine et al. [48] provided an overview of potential vulnerabilities of traffic signal control systems. They mentioned a very common problem, which is the use of default or simple usernames and passwords combination for signal controller. They further discuss how conventional security practices for traffic operations applications have a decreasing amount of security features as one moves from the network security level to the operating system level, to the application level [48]. Although this project was not mainly focused on cyber security, this type of potential issues is still worth mentioning because this project involves mobile app communication with the signal controller and RSU. Therefore, it is very important to limit the app only retain an essential amount of functionality to ensure safe and efficient use and does not allow for any unintended means of accessing/manipulating control plans maintained by the controller as was done by Ghena et al. [47].

In term of cybersecurity for CV applications, Zhao et al. [49] discuss issues directly related to V2X messaging. They pointed out that attacks on V2X communications could result in message loss, fake information change, reception delays, etc. They also discussed that authenticating messages as a means of security may not always be practical, especially in real-time safety applications due to data transmission and processing limits [49] Alnasser et al. [50] provided a comprehensive view of cybersecurity challenges for V2X communications. The team listed different types of threats for IEEE 802.11p and the LTE-V2X communication protocols. In terms accessing to communication information, the team listed the following potential types of attacks: blackhole, jamming, flooding, and platooning. Blackhole as well as greyhole attacks means attackers blocking some of or even all the communications from a specific device; authentications can sometimes stop this type of attacks. Flooding is on the opposite side of blackhole, instead of blocking messages, attackers send numerous additional messages to a specific device to prevent it from receiving them from other sources. Jamming attacks result when attackers send signals to disrupt communications, and coalition attacks involve coordinated attack efforts by multiple actors

[50]. Message integrity threats can be categorized into 3 categories. One such attack involves maliciously modifying the contents of the message. However, although internal attacks are usually hard to check, external attacks be stopped using encryption and authentication. Another form of message integrity attacks is changing the time order in which messages are received and altering the location data via GPS spoofing [50].

2.3.2 Mobile Application Development on Cybersecurity

As this project involves mobile phone application, the cybersecurity of it is unneglectable. Mobile phone has become one of the most essential equipment for everyone's daily life and can now serve multiple roles and complete multiple tasks. However, mobile phones are also very vulnerable to various types of cyber-attacks, which need serious attention to be prevented and stopped. As this project highly relies on a mobile app, it is important to ensure that potential vulnerabilities are addressed so that its potential of malfunction can be reduced. In the following section, 5 cybersecurity challenges in total faced in the app development faced in app development will be introduced.

The first as well the biggest challenge is data encryption. Once being encrypted, data in the messages can become a form which is usually unreadable without decryption. Data should have some level of encryption in order to protect users' privacy, since a significant number of messages transferred may contain users' private information, thus users' information will not be leaked and illegally used. Once the messages are encrypted, even if they are leaked, it is very difficult to decode it in a short time. Because sensitive information such as location of the users are needed to localize the non-motorized users on the street, encryption is needed for this type of information to be safely delivered. The UW STAR Lab has adequate experience of applying encryption to some of its projects on mobile sensing. It is worth noting that the lab has already developed a sensor known as the Mobile Unit for Sensing Traffic Version Two (MUST-II). The MUST-II can recognize mobile devices through Bluetooth or Wi-Fi when a given device is within the detection range of the MUST-II sensor. To provide anonymity and avoid data hijacking for illegal use of personal information, the unique identifiers of all mobile device detected are encrypted using a secret algorithm.

Another important security concern worth mentioning during the mobile app development is user authentication. User authentication is a significant method to protect user privacy and ensure individual without authorization cannot properly use the app. Very similar to encryption, user authentication also focus on protecting data privacy, however, the differences between the two is that encryption is able to protect the security of data even when the data leaks. On the other hand, user authentication can prevent non-authorized users or some malicious users from using the account owned by authorized users of a given app. The most common type of user authentication in the industry is requiring users to have username and password set and ask them to type the username and password combo to log into the app. In the recent few years, two-factor authentication is becoming more and more popular and has already been widely used. Compared to the traditional password authentication, two-factor authentication uses a second device or platform, such as mobile phone, as a second lock. The software will generate a one-time passcode for usage of an app and send it to the second lock to check user's proper identity. If the user fail to correctly respond the second lock within a preset amount of time, the one-time passcode will expire to prevent force decryption, and the user will have to request a one-time password for logging into the app. To protect the information in an easy way, simply change a strong and complex password-username combination from default setting or predictable values can be very helpful to stop illegal or unwanted access to the sensitive information.

The third cybersecurity concern for mobile app development is the possibility of reverse-engineering. Frequent customer interaction with an app makes it more valuable in many senses, but a wider audience also opens it up to increased risk of hacking and nefarious usage [51]. By using communication purpose in detail, hackers sometimes can understand the logic used during the app development, and this may become a bug result in back office attacks, such as attacking the server's database which stores information for properly using the app. More seriously, reverse-engineering can sometimes make user credentials as well as other personal information stored on the server-side be stolen. Some methods are proved to be useful to prevent reverse engineering. One method is to store important code on a secured cloud or local server rather than simply storing in the app itself. This will greatly decrease the possibility for the hackers to access the code. Also, very similar to encryption, applying hashing algorithms on obscure data and convert it into a format that is difficult to be understood without knowing the logic behind the hashing algorithm used.

Although a little too general, the fourth concern during mobile app development is future preparation. During the development period, mobile apps are usually designed to stop only cyber-attacks that are already existed. Therefore, mobile apps are usually uncapable of foreseeing the possibility of future cybersecurity challenges, and developers cannot always accurately predict what type of challenges will come and how to prevent it from harming the app. But based on the analysis of the current app development trends, some of the future challenges are not impossible to be predicted. For instance, the communication between an app and Internet of Things (IoT) devices should be addressed [52]. With more IoT devices are purchased on the market, a flexible app framework can make future updates on preventing various upcoming attacks much easier.

The final cybersecurity issue during mobile app development is insecure codes. Even if all the aforementioned issues are considered and prevented, the use of insecure code can easily ruin all previously efforts. A handful of cybersecurity crisis in the industry are caused by using insecure code during the development. For instance, some of them are cause by neglecting abnormal situations during the app development. Also, when expanding the functionality of the app, developers may accidentally use insecure libraries that themselves have serious bugs, and hackers can use the library as the gateway to harm the rest part of the app. Checking and ensuring the security of the code itself is necessary before app release and there are multiple methods to reduce the probability of creating insecure code [53]. The first one is to use code scanning strategies that can help find common security issues. The second one is that during the development period, carefully checking the third-party libraries for cybersecurity vulnerabilities. Although libraries usually work well in most cases, they may still break down in extreme cases and leaves a chance for hackers.

2.4 Mobile Phone Based Infrastructure Connection Project Summary

Previous works have demonstrated that pedestrian safety can only be improved by utilizing and optimizing traditional button-pushing and signal timing [54] under limited circumstances. A novel SPaT serves is the key target of the scenario of interest, and to serve the non-motorized road users, safety and equity should also be taken into consideration. Therefore, the combination of accessibility, safety and equity for non-motorized road users are essential to what researchers should pay attention to. Many previous works have been done to realize the solution to the targeted scenario. Researchers from Carnegie Mellon University developed a mobile app that helped the non-motorized users to cross the road. The team took advantage of vehicle-to-infrastructure (V2I) communication, which has produced both hardware devices such as dedicated short-range communication (DSRC) radios and V2I messaging standards [55]. After giving the phone a sleeve that supports DSRC communication, a user with disability can use the app called PedPal to send triggers to the signal controller, while also see the current timing information such as wait time and green light countdowns. The team used DSRC RSU as a data transfer media to communicate with the signal controller, and if the DSRC sleeve is not a desired option, the user must use a cloud service to get the communication. The project provided a feasible solution, but users should either use an extra sleeve or use the cloud service, which in many cases would be a problem depending on the carriers' service coverage of the users. Minnesota researchers Liao et al. also proposed a system called Mobile Accessible Pedestrian Signals (MAPS) to help people blind or visually impaired [56] to cross the road more safely. A mobile app was also involved in the system. In their mobile app, users can get various information about the intersection, including some geometrical data such as number of lanes and orientation of the street. The app utilizes 3G or Wi-Fi as the connection method to a server, which also uses 3G or Wi-Fi to connect to the signal controller. Although the project gave a neat and simple solution and added some extra safety features, it did not provide solutions to the problems that the CMU project had. Some other projects also put their efforts more on non-motorized road users' safety issue. Wang Tianyu et al. from Dartmouth College designed an Android mobile app called WalkSafe [57] to help people walking more safely. It utilizes the back camera of the phone to record the environment and use machine learning technology to identify potential danger around the user. Although it did not connect the user with any infrastructure, it provided a good sample of how sensors inside mobile phone can help the pedestrians to walk safer. It still cannot replace the communication between user and infrastructure but provided us a good example of mobile phone sensor aided pedestrian safety innovation. Khosravi, Sara, et al. proposed a system called Smart Walk Assistant (SWA) to raise the safety level of pedestrians. A RSU is included in the system to help the communication. Both sender and receiver side have highly-customized equipment to ensure both two pathways: pedestrian-to-infrastructure (P2I) and pedestrian-to-vehicle (P2V) [58] can work properly. This project did raise the safety level and improved the equity and accessibility of the pedestrian, especially the ones with disabilities such as visual impairments. It also realized the connection between pedestrian and infrastructure, and even added vehicles into account. However, because the system is highly customized, its complexity is way too high to be an affordable solution which can be used everywhere. Furthermore, not much reliability test and stress tests has been conducted for the system, leaving the system reliability questionable. A team led by Rahimian et al. utilized a Vehicle-to-Pedestrian (V2P) mobile phone app that warns pedestrians when they initiate unsafe crossings [59], but the successful rate was only 59%, which was not ideal. Other technologies have potential to improve the targeted scenario. Attanayake et al. used A mobile based app to assist drivers to be incorporated with the proposed signaling system to enhance the end-effect [60]. However, the system still needed image processing to obtain the real-time data of pedestrians at crosswalks [60], which could lead to unreliability. And for the pedestrian monitoring tasks, some other methods were also developed to complete the task. Jang et al. used a collection of drone videos of general vehicle-pedestrian crossing behaviors to reflect on an analysis system to apply on assessing the risks of road safety [61]. And a team led by Kothuri et al. utilized inductive loops and a thermal camera to count bicycles and passive infrared counters and pedestrian signal actuation data to count pedestrians [62], and for the similar task Lesani et al. used two-dimensional LiDAR sensor with a set of distinct laser channels and a given angular resolution between each channel [63]. However, these methods were too costly since drones and inductive loops should be involved.

Chapter 3. The SPaT Mobile Network Framework

3.1 Overall Framework Structure

To provide users a reliable and fast experience when communicate with the signal controller, it is critical to optimize the components from the basic design logic. To keep the user experience neat and simple, the mobile phone side was kept unmodified and did not require any extra equipment to be fit onto it, and this greatly reduced the cost of using and upgrading the system and the complexity of installing the setup. Although wireless communication is inevitable in the system, we avoided methods that can be unpredictable such as cellular network which can introduce new problems such as unpredictable service coverage. All other components are directedly connected to maximize the reliability and data transmitting speed. We only maintained the minimum number of components in the system and reduced the risk of malfunctioning and breakdown, and this also benefits the maintenance and upgrading procedures because most of the components are onsite and the logic behind the system is simple and easy to understand.

5 main components (shown in Figure 3-1) are involved in the communication structure: Mobile phones (Android), Smart Gateway, edge device, signal controller and traffic lights. These components are connected to each other either wired or wirelessly and the data transfer is bidirectional.

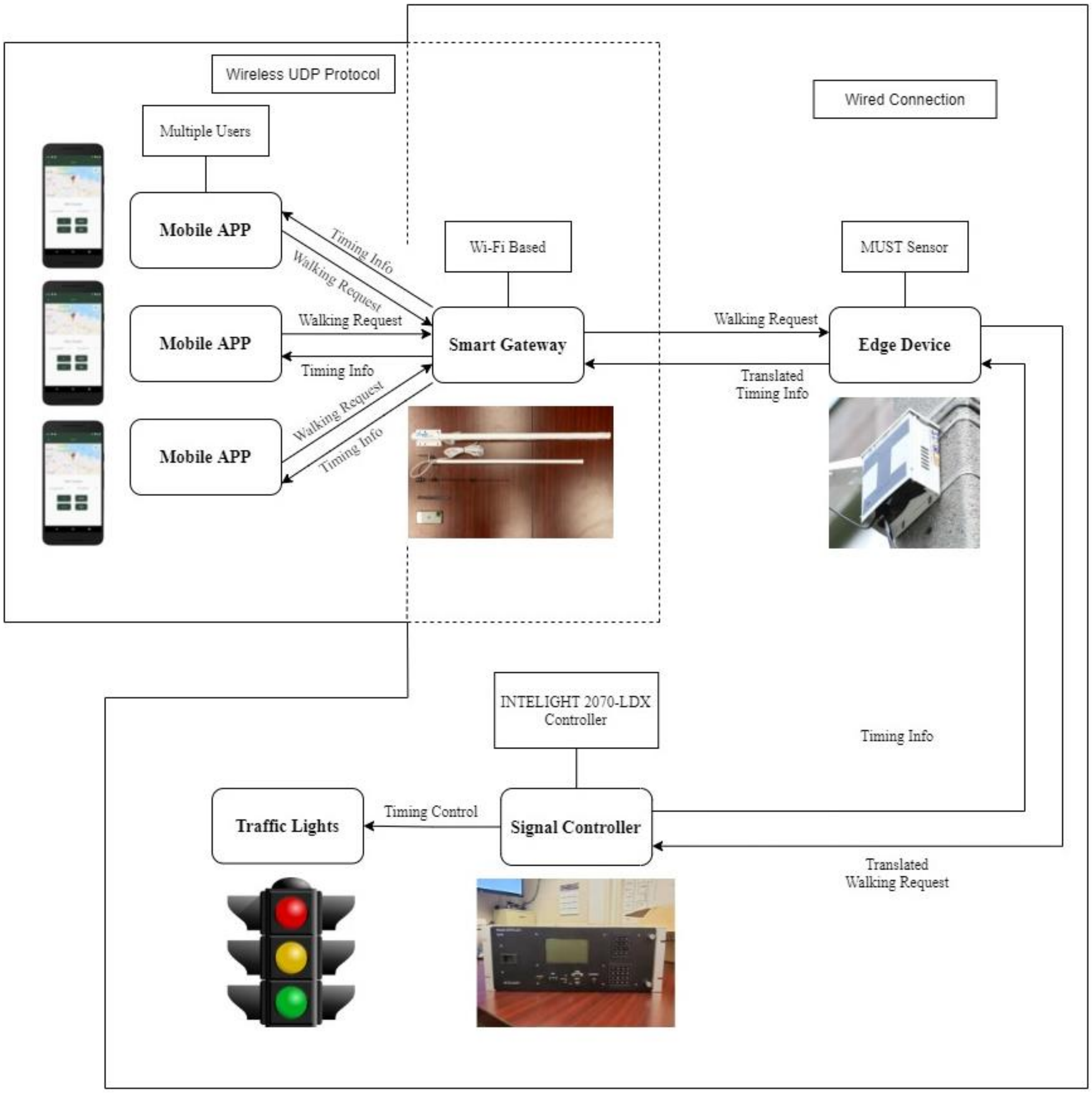


Figure 3-1 The overall structure design of the project.

Mobile Phones:

In the current phase, the app is only available to the smart phones Android platform due to time and cost, and need Android 8 or higher Android version. An IOS version may be available in the future to fulfill the need of a larger user group. The phone needs to connect to the Wi-Fi service we provide with the Smart Gateway to allow the UDP work, and allow the app to read information such as GPS location in the phone. The Wi-Fi service is called HiController and need to connect manually when it is the first time to use the service. Because GPS service is needed for the app to fully function properly, an open environment, which is also the targeted usage scenario, is preferred. Indoor environment may result in the app failing to achieve the needed data.

Smart Gateway:

The Smart Gateway system sends and receives information and works as a bridge connecting the mobile phone and edge device. It uses 2.4 GHz Wi-Fi to communicate with mobile phones, and the information interaction range can reach at least 50 meters and up to 150 meters depend on factors such as weather or the number of obstacles like cars, and a signal coverage area at this scale can hand most of the intersections in the country. Also, the latency of the data transfer can be controlled to within 1 second to reduce the danger caused by data inaccuracy. The Smart Gateway is weather sealed and does not need frequently cleaning after the initial installation. The antenna requires some vertical rooms, but this will not be a problem in most cases. The Smart Gateway connects directly to the edge device to ensure instant data transfer.

Edge Device:

The edge device is one of the most important components in the whole structure because it serves as an interpreter to make the communication between roadside infrastructure and non-motorized users possible. The edge device is developed by STAR Lab researchers based on NVIDIA Jetson Xavier AGX (a type of modular computer which has a 8-core ARM CPU to support the calculation work) and can run MAXTIME software supplied by the controller manufacturer Intelight, and the software allows developers to control the signal timing plans of the controller on Linux operating system. The edge device can process the request from the mobile phone and transform it into commands that can control the signal controller, and can also transform the timing information from the signal controller back to the data that the mobile phone app can read.

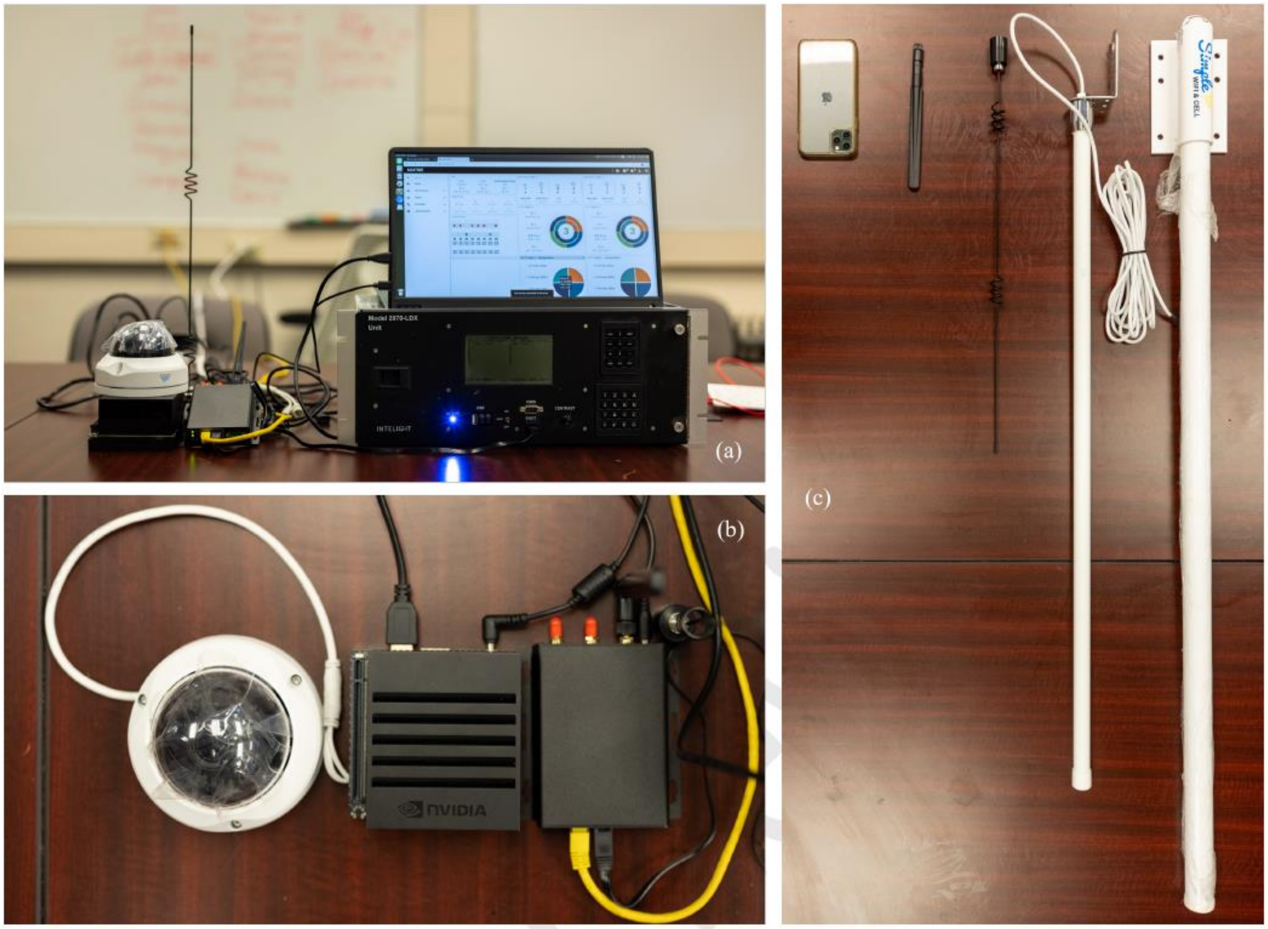


Figure 3-2 Edge device and Smart Gateway hardware setup. (a) shows the signal controller and its controller interface. (b) shows the edge device. (c) shows the antenna system.

Signal Controller:

The signal controller model is the INTELIGHT 2070 LDX signal controller, which is manufactured by Q-free Inc. This controller is not a customized model specifically made for this project, but a model that is currently available on the market, and this ensures the universality of the project and people who want to use the system in the future will not have to spend an enormous amount of funds to modify the expensive traffic signal controller. The size of the 2070LDX signal controller is identical to normal controllers on the market, but the one we are using is one of the most advanced signal controllers. This specific model meets almost all the traffic control standards and provides an extra robust, reliable, and industry-leading platform with connectivity for researchers to develop more functions based on it. The controller can be either connect using ethernet cable or via Wi-Fi signals, allowing it to be controlled externally with different types of methods. In addition, the controller comes with a software called MAXTIME, and the simple UI of the software allows users to easily adjust the timing plan with a computer. The software works on both Windows and Linux, which means it is suitable for edge devices as well. The most important feature is that this signal controller provides hundreds of different APIs for users to call, and this makes it possible for researchers to control the signal controller without physically accessing it or using the MAXTIME software, but with any other devices that is connected with the controller, as long as it is capable of using the APIs and can run scripts written by the researchers. Because as an isolated system, the signal controller does not have the ability to send and receive data wirelessly, it needs the help of the edge device to do the job.

Figure 3-3 2070LDX traffic controller unit.

Traffic Lights:

The traffic lights are controlled by the Intelight 2070LDX controller. Traffic lights follow the timing plan in the signal controller and reflect the changes developers made to the timing plan.

Users can either use manual mode or auto mode on the app, but will both eventually send a trigger from their mobile phones to the smart gateway using the UDP protocol. It is no longer needed to avoid losing packet during the data transfer process, because the data transfer fully depends on a developed connection when UDP protocol, once the connection is established, no packet will be lost. Furthermore, because the mobile phones only send necessary messages to the smart gateway and the information is concise, the transfer can be completed instantly.

After the initial data sending, the smart gateway will receive the requested information and pass the information to the edge device installed on the roadside. In ideal situation, the data receiving distance can reach 150 meters. The edge device is programmed to translate the mobile phone triggers to commands that the signal controller can understand. The trigger works as a virtual push button and the signal controller will change the timing base on the trigger and send the updated timing information back to the edge device. The edge device will process the timing information and broadcast it through the Smart Gateway. The mobile phone can then extract the necessary data from the processed information and show it to the users.

3.2 User app

3.2.1 Overall Design

The workflow of the mobile app is shown in Figure 3 below.

The protocol we used for the data transfer between the app and the edge device was UDP protocol. Compared to HTTP and DSRC protocol, UDP protocol is more suitable for time-sensitive applications because it does not have retransmission delays. It is also good for information broadcasting because it has small data packets and can send and receive data very fast while also retaining good encryption standards without developing end-to-end communication. Also, because DSRC need special equipment to support, and is no longer being updated, in terms of the potential of being used by the general public, it is not the best choice.

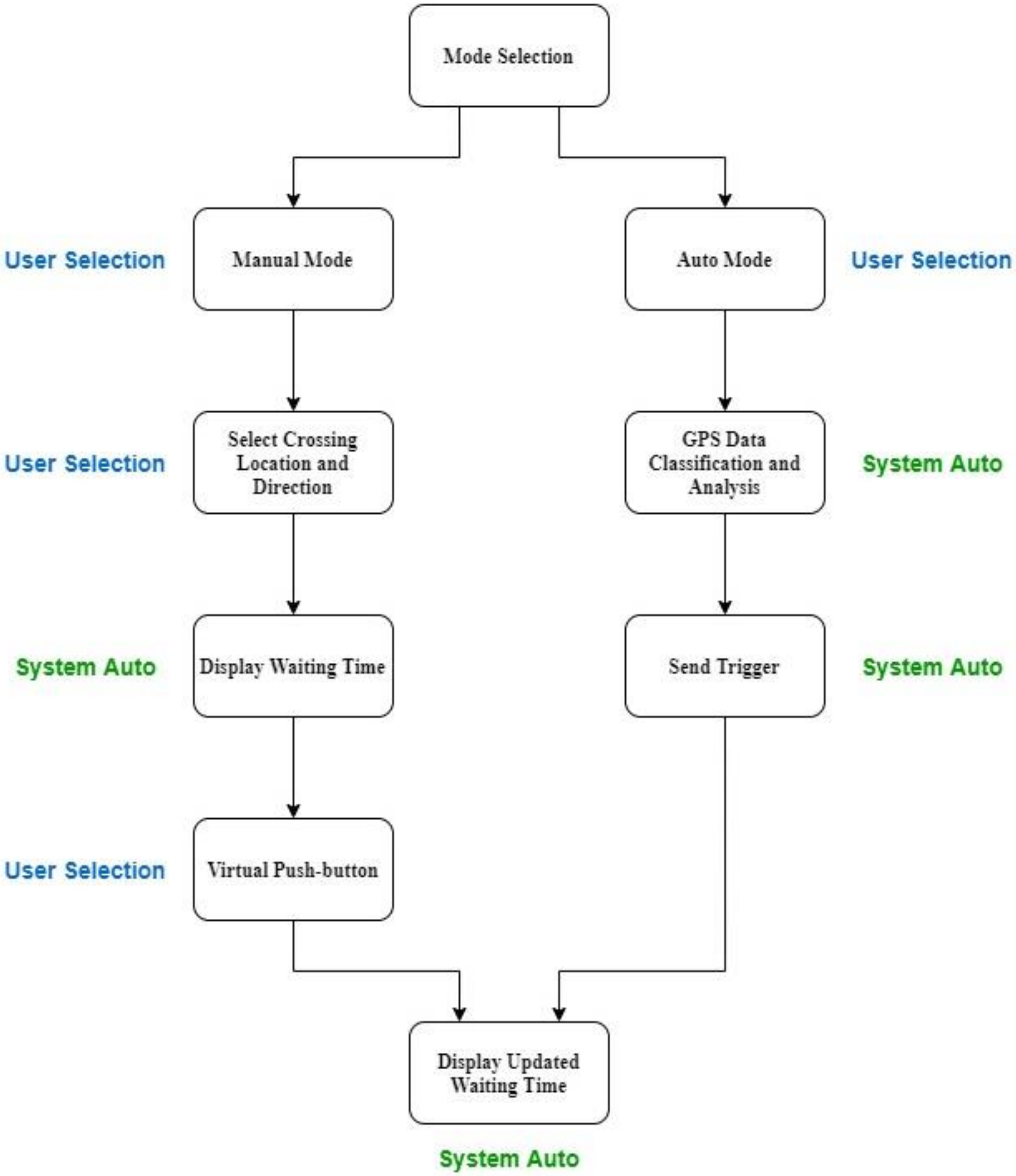
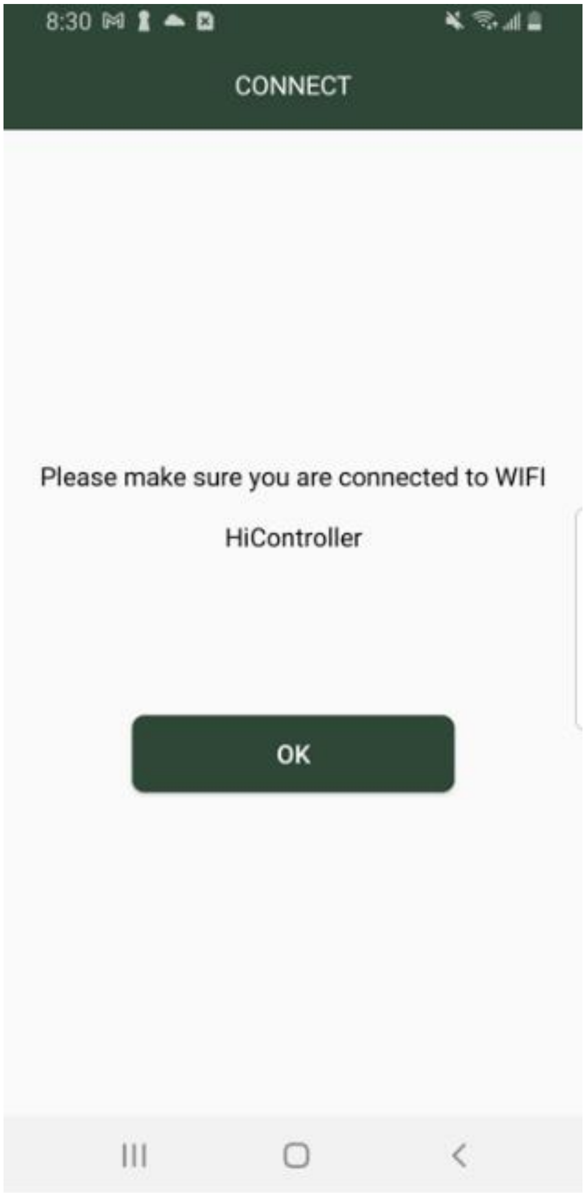


Figure 3-4 Workflow of the mobile phone Android app.

3.2.2 App Pages Design



Please make sure you are connected to WIFI

HiController

Figure 3-5 The welcome page of the mobile app.

The app is designed to be concise, intuitive, and user-friendly. Green and light grey are chosen as the overall tone of the user interfaces and provide a clean and simply user experience. On the first page, it reminds the user to make sure that the phone is connected the Wi-Fi "HiController", which is specifically used for this app. For most smartphones on the market, after once been connected to this Wi-Fi, the phone will remember it and automatically connect to it the next time it finds the Wi-Fi signal.

Figure 3-6 The loading page of the mobile app.

The loading page of the mobile app also use green as the theme color. The page will be shown for 3 seconds, and on the page, are the a greet and the organizations that supported this project.

Figure 3-7 The function navigation page of the mobile app.

The navigation page of the app has mainly two choices for the users. If users want to cross the road, sending walking request, or even just want to know how long they should wait for the green signal, they can click on the "Walking Request" button on the screen to enter the main page. If users are willing to know the contact information of the developers, they should click the "Contact" button to view the information.

Contact Information

STAR Lab, University of Washington

☎ (206)616–2696

Washington State Department of Transportation

☎ (360)705–7000

Figure 3-8 The contact information page of the mobile app.

The contact information page also shows the logo of the project supporters. If users want to call either of the supporters, just click on the phone number or the phone logo, the app will automatically dial the number for the users.

There are two versions of the app (shown in Figure 3-9 and Figure 3-10) involved in this project. One is the app for normal users who will not participate in the development and the other version is the app for the app developers. The developers' version included 2 more buttons to manually collect user data (Start and Stop) on the main page to let developers start or stop recording. The collected data will be saved as .xls file into the internal storage of the mobile phone. The data collected is processed and analyzed for user classification which works as a process in app version for real users.

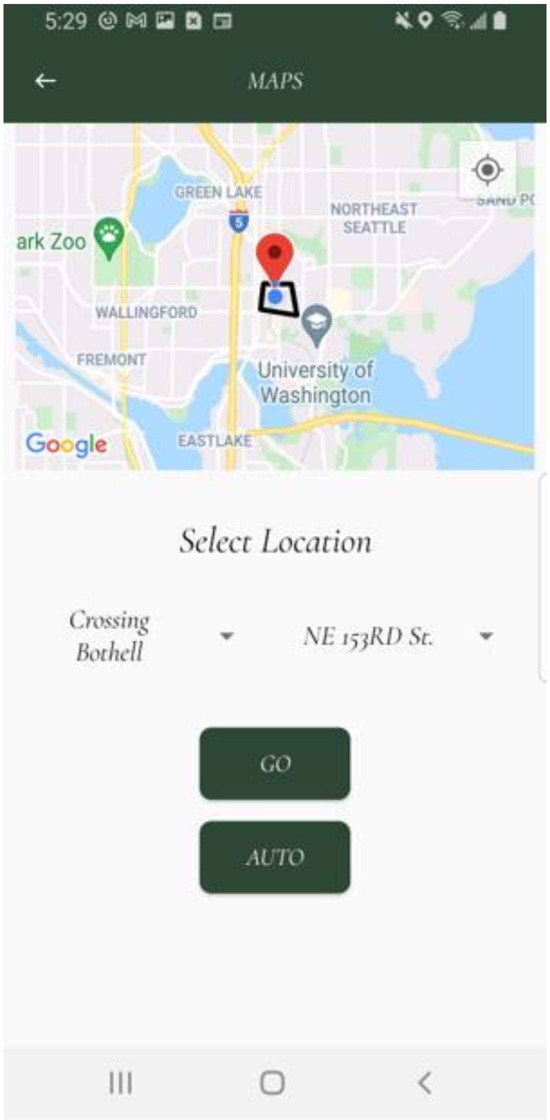


Figure 3-9 The normal user main page of the mobile app.

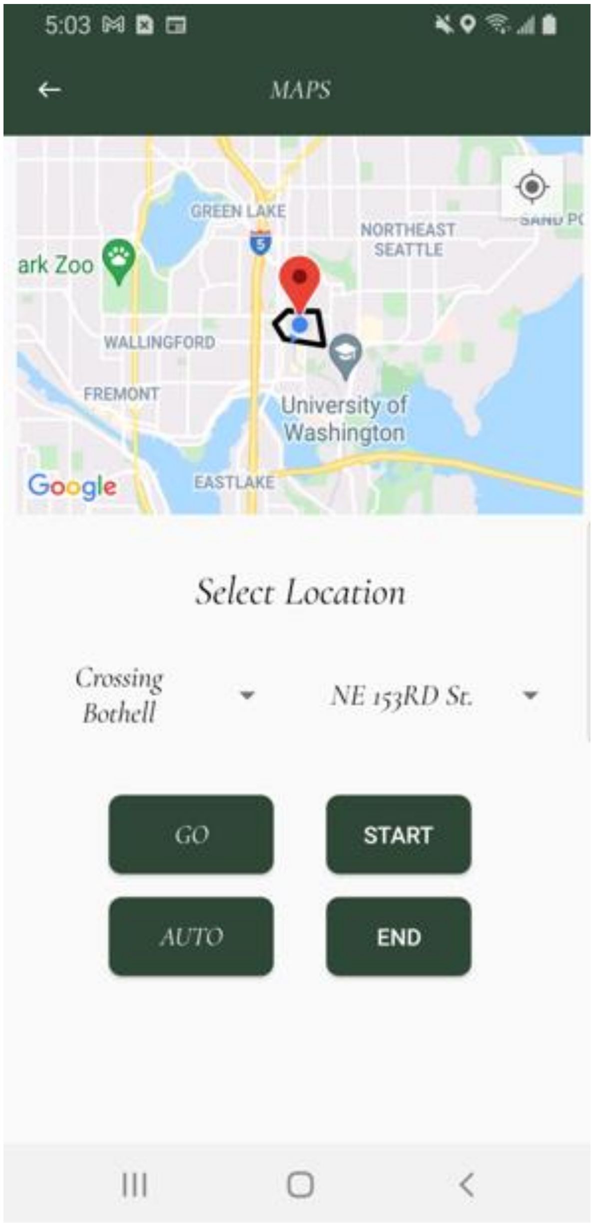


Figure 3-10 The developer main page of the mobile app.

3.2.3 Manual Mode Logic

For a real user there are 2 choices to tell the signal controller that they want to cross the road. The first way is manual mode, the user can select which crossroad he or her is currently at and which direction they want to cross by using the drop-down menus on the top of the page. After the selection, press the “GO” button, and it will guide the user to the timing page, and shows how much time still needed to wait until the user can cross the road. If the user considers the remaining time is too long, he or she can press the “Virtual Push Button” to send a virtual trigger to the signal controller and will get an updated remaining time within 2 seconds.

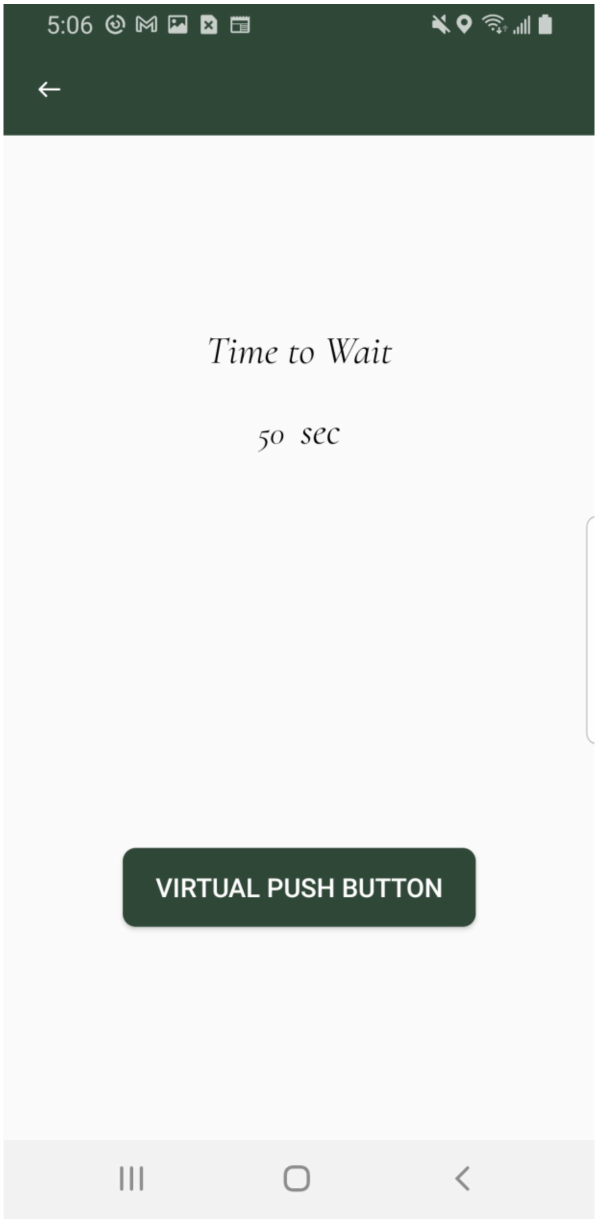


Figure 3-11 Waiting Time Countdown Page.

3.2.4 Auto Mode Logic

If the user chooses to use auto mode, all he or she needs to do is to press that “AUTO” button at the bottom. The app will then start to record user’s direction, coordinate, and speed, to analyze if he or she is biking, jogging, walking or is disabled and work out a conclusion.

Time to Wait

51 sec

Push Button Successfully

Figure 3-12 Waiting time countdown page - virtual push-button activated.

After the user enters the detection range, the trigger with the conclusion will be sent automatically to the edge device and the edge device will activate the proper timing plan. The signal controller will send the updated information back to the user app for waiting time display.

3.2.5 User Classification Logic

In auto mode, the app records user's coordinate and speed data from the GPS service and direction data from magnetometer of the mobile phone. Speed and directional data are used to determine what type of user is using the app, and the crossing direction is determined by reading the directional data when the user stops at the crossroad. If the user is moving fast and has many directional changes, the system will consider he or she to be a jogger. If the user is moving fast but does not have frequent directional changes, the system will consider he or she to be a biker. If the user is moving slow but not extremely slow, the system will consider he or she to be just walking. If the user is moving extremely slow, the system will consider he or she to be disabled. All the four scenarios can have corresponding timing plans as backup. Sometimes limiting the service area is need, when the users have already connected to the Wi-Fi, but they are too far away, a targeted service range is set to prevent them from using the service. In this case, when they click "AUTO", a message says "Not In Range" will show up.

3.2.6 User Data Collection Function

For better serving the users, some data needs to be collected by the phone. Because data collection has privacy issue, when start the app, it will ask you to grant the app access to the data which is needed for analyzing user behaviors.

For people who cannot move as agilely as normal people, the app provide users an option to set their identity as "Additional Care Needed" for extra help. For disabled people, selecting this option is highly recommended since it will no longer need the app to use user classification to decide whether the user needs extra care or not, although it is feasible for the app do the job automatically.

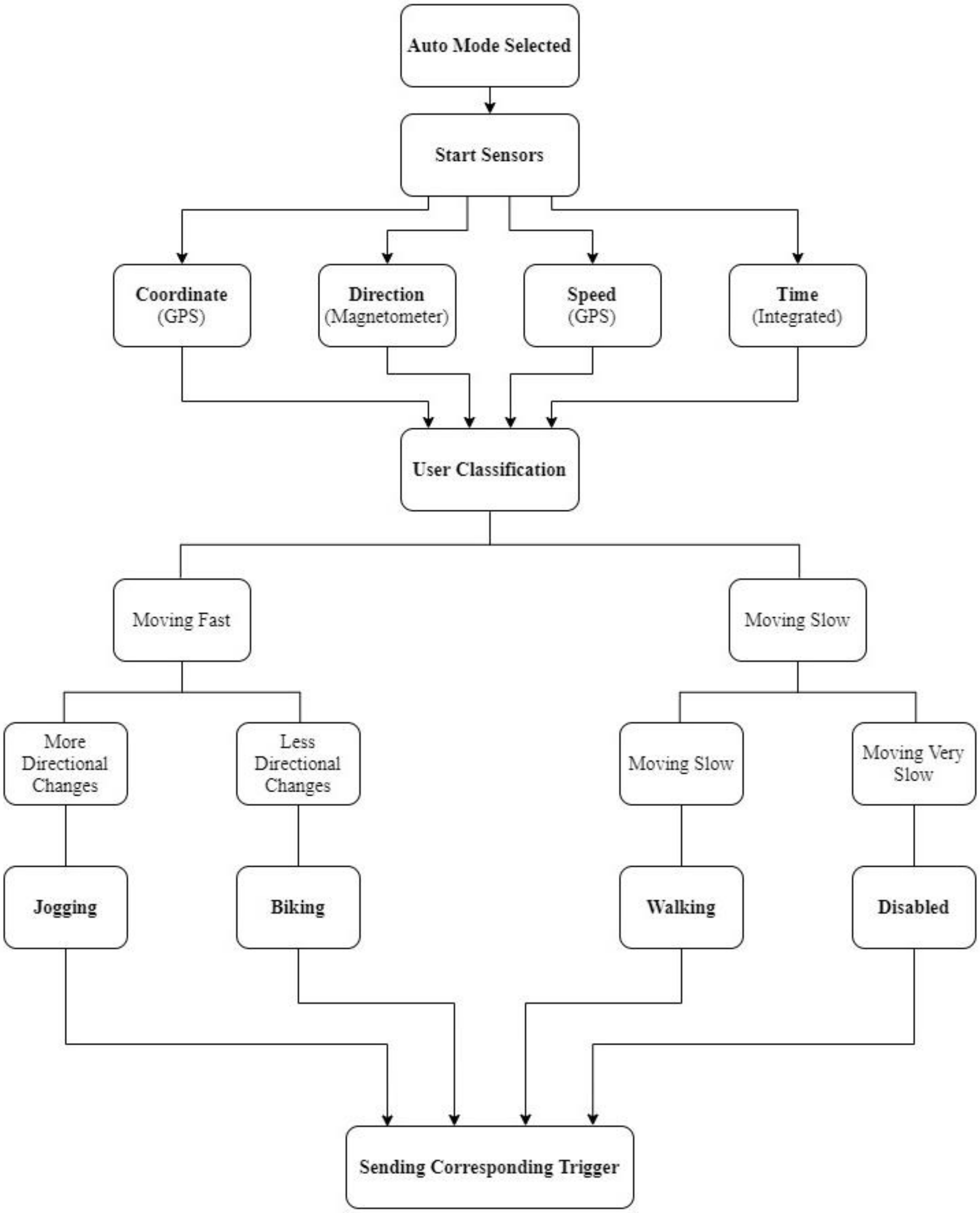
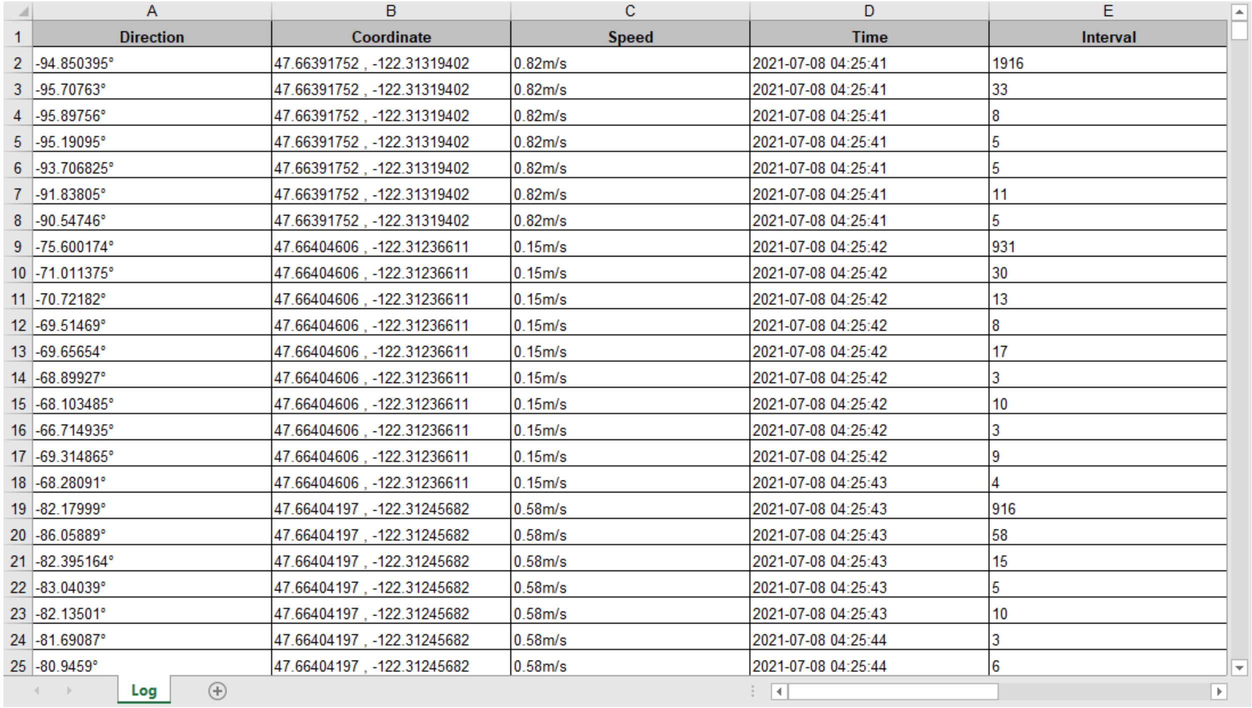


Figure 3-13 User classification logic.

To protect user privacy to greatest extent, the app will only read motional and geographical information. Without detecting the users inside the preset target zone, the app will only read but not record users' motional and geographical data.



	A	B	C	D	E
1	Direction	Coordinate	Speed	Time	Interval
2	-94.850395°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	1916
3	-95.70763°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	33
4	-95.89756°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	8
5	-95.19095°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	5
6	-93.706825°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	5
7	-91.83805°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	11
8	-90.54746°	47.66391752 , -122.31319402	0.82m/s	2021-07-08 04:25:41	5
9	-75.600174°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	931
10	-71.011375°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	30
11	-70.72182°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	13
12	-69.51469°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	8
13	-69.65654°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	17
14	-68.89927°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	3
15	-68.103485°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	10
16	-66.714935°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	3
17	-69.314865°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:42	9
18	-68.28091°	47.66404606 , -122.31236611	0.15m/s	2021-07-08 04:25:43	4
19	-82.17999°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:43	916
20	-86.05889°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:43	58
21	-82.395164°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:43	15
22	-83.04039°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:43	5
23	-82.13501°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:43	10
24	-81.69087°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:44	3
25	-80.9459°	47.66404197 , -122.31245682	0.58m/s	2021-07-08 04:25:44	6

Figure 3-14 Sample information collected by the mobile app.

Using Google Map service and GPS unit inside the mobile phone, the phone can read speed, direction, and coordinate 2 times per second to classify user type. 2 times per second was tested to be a frequency that balance the detection data volume and the stability. Faster than this frequency can potentially result in partial data loss. Although the reason for losing part of the data is still not clear, it is highly possible that the loss was due to Google's self-protection mechanism.

It is also worth noting that because only limited people participated in data collection, the data volume is still very limited. However, new data is constantly added to the database to make the classification more accurate. After passing the field test, which has been postponed for various reasons, to proof the real-life stability of the app, AI technology may be added for this function, and that may greatly help the accuracy of the prediction result.

Chapter 4. Experiment and Result

4.1 Communication Experiment

4.1.1 Hardware and Software Preparation

The simulation is conducted outdoor near the University of Washington STAR Lab, More Hall. Two lab members were involved in the simulation experiment because of the pandemic. And because it was difficult to shut down a road and access the traffic light, we used MAXTIME software to run as a substitute to the traffic light because it could supervise the status of the signal timing, which is the mean role of traffic light in this project. Therefore, only 4 (instead of 5) main components were prepared for the experiment:

Mobile Phone:

A total of 2 mobile phones were prepared and both installed with Android 8 operation system. The mobile phones were installed with our test version mobile app, and were preconnected with the Wi-Fi signal HiController and were fully charged. Both mobile phones were water resistant for unexpected weather conditions.

Smart Gateway:

The Smart Gateway was connected to the roadside device and was placed next the mobile phone testers. It was powered by the roadside device and the antenna was adjusted to point at the sky, which is also how it ideally should be installed on actual traffic lights.

Roadside Device:

The roadside device is powered by a portable charger and was directly connected to the Smart Gateway and the Intelight 2070LDX controller. The roadside was preinstalled with the required software, and was connected to a monitor, which not only allowed the researchers to monitor the status of the signal timing plans lively, but also replaced physical traffic lights and saved some time and cost.

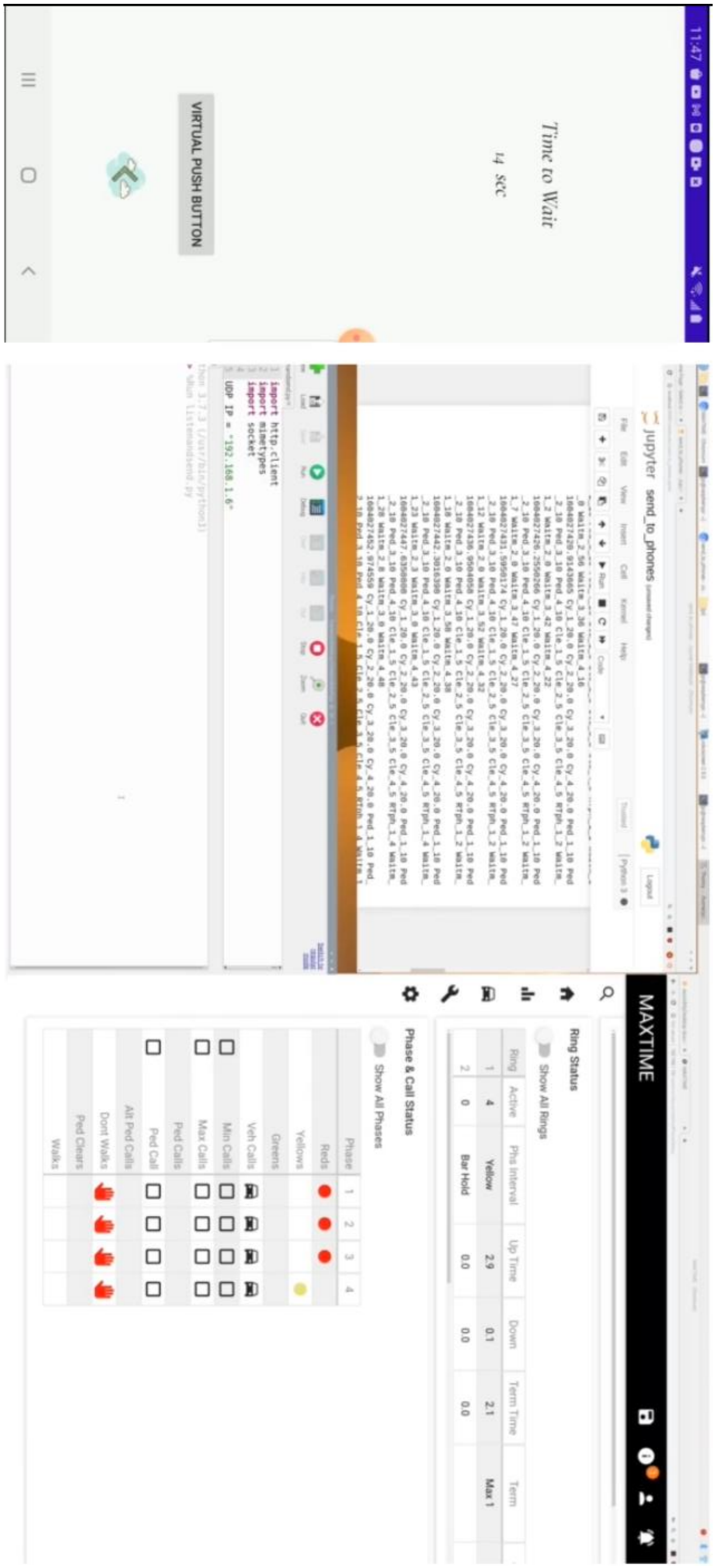
Signal Controller:

The Intelight 2070LDX signal controller was pre-programmed to simulate the real-world working environment. The signal controller needed to power its own power supply, so it was also connected to the portable charger.

4.1.2 Simulation Experiment

Connection Test:

Because the Wi-Fi signal coverage range is the service range, our researchers tested the service coverage by walking away from the Smart Gateway with the mobile phones and constantly monitoring the status of the mobile phones' Wi-Fi connection. We had the 50 meters distance mark and 100 meters distance mark on the ground. The result showed that in most cases, both test mobile phones lost their signal long after the researchers passed the 100 meters distance mark, and this indicated that the service region provided by the Smart Gateway was more than enough for the users.



```
import http.client
import mimetypes
import socket

UDP_IP = "192.168.1.6"
```

Ring	Active	Phs Interval	Up Time	Down	Term Time	Term
1	4	Yellow	2.9	0.1	2.1	Max 1
2	0	Bar Hold	0.0	0.0	0.0	

Phase	1	2	3	4
Reds	●	●	●	
Yellows				●
Greens				
Veh Calls				
☐ Min Calls	☐	☐	☐	☐
☐ Max Calls	☐	☐	☐	☐
Ped Calls				
☐ Ped Call	☐	☐	☐	☐
Alt Ped Calls				
Dont Walks	✋	✋	✋	✋
Ped Clears				
Walks				

Figure 4-1 Test interfaces.

Location Verification:

The Auto Mode of the mobile phone App need accurate GPS data to work, therefore, it is needed to verify if the GPS signal was showing user's location correctly. We sent the location data from the phone to a PC and open the coordinate in Google Map Satellite view, and compare the point (2 different shapes of detecting area were provided, each covered both large open spaces and building-concentrated area) on the map with the locations the researchers were standing at. The results showed that the GPS could work properly, and the errors were neglectable.

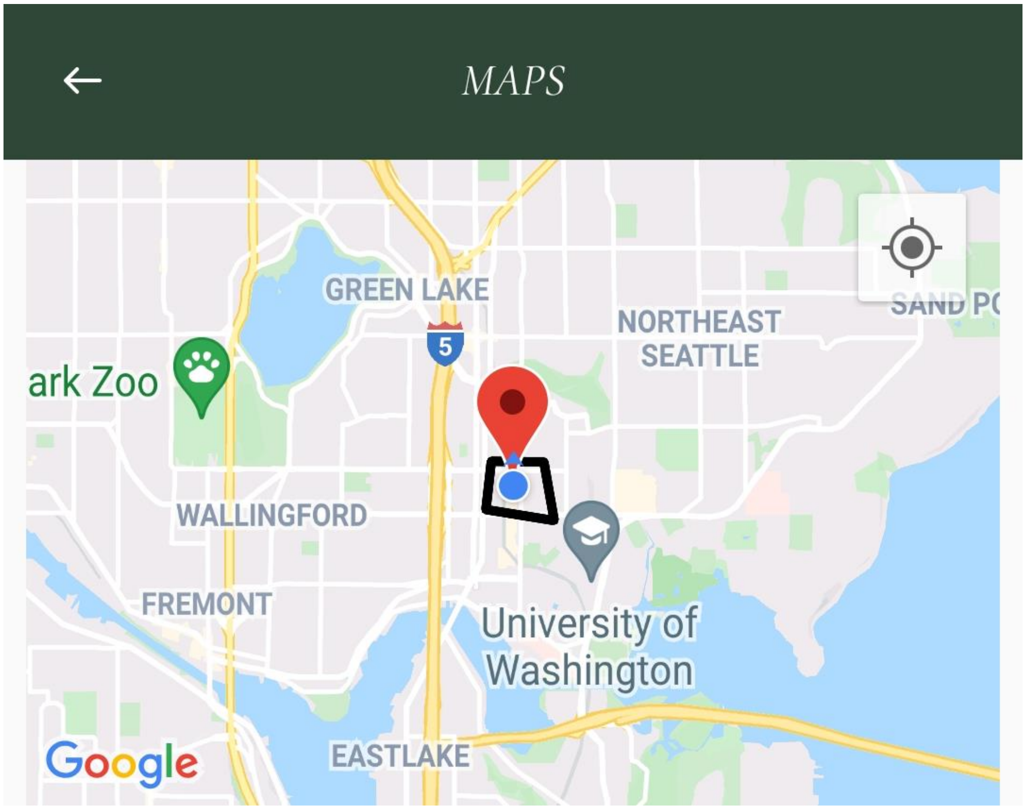


Figure 4-2 Sample preset detection range.

Communication Test (Manual):

The researchers stayed in manual mode (default) to walk into the service area. The monitor on the roadside device showed that the 2 mobile phones were connected to the Wi-Fi. Then, the researchers selected the corresponding intersections and crossing directions on the phone and click the “GO” button. The screens on the mobile phones successfully showed the time remaining. Then, the researchers clicked the “VIRTUAL PUSH BUTTON” button. The roadside device successfully received the requested information including the user ID, user classification result, and crossing direction and activated the corresponding signal timing plan. Then, the roadside device sent the updated signal timing plan to the phone and the waiting time got updated within 1 second after the request was sent. The test was conducted multiple times with researchers walking slowly, walking normally, jogging, and biking. In most of the cases these tests, the mobile phone app got right classification result and the results were sent.

Communication Test (Auto):

The researchers stayed in default manual mode and walked into the service area. The monitor on the roadside device showed that the 2 mobile phones were connected to the Wi-Fi. Then the researchers clicked “AUTO” button, the roadside device successfully received the requested information including the user ID, user classification result, and crossing direction and activated the corresponding signal timing plan. Then, the roadside device sent the updated signal timing plan to the phone and the waiting time got updated within 1 second after the request was sent. The test was conducted multiple times with researchers walking slowly, walking normally, jogging, and biking. In all these tests, the mobile phone app got right classification result and the results were sent.

Range Limit Test:

The researchers stood outside of the targeted service area and inside the Wi-Fi coverage area, then click “AUTO” button. The message “Not In Range” popped should pop up.

4.2 Result

For the connection test, researchers tested the connection condition from 12 different directions, among them, 9 of them were still connected even after reach the mark of 100 meters. 2 of the tests had the mobile phones disconnected right after the 100 meter mark, and 1 test had the mobile phones disconnected right before reaching the 100 meter mark. After examining the result, buildings have significant effects on the connection, and the thicker the building block between the transmitter and receiver is, the more significantly it will block the signal.

For the location verification test, the coordinates turned out to be accurate. The accuracy of the GPS usually stayed unnoticeable when nothing is blocking the signal above the researchers. When at a more building-concentrated area, the outdoor signal accuracy might drop, and show an error of about 2-3 meter, which is also acceptable. However, the result was not very good inside the building, and sometimes the mobile phone can completely lose its signal right after the building. Therefore, it is not recommended to use the system inside the building.

Because once the app, Smart Gateway, and the signal controller were properly set up, within the detection range, the chance of the losing the message during communication is very low. Therefore, it was not surprising to observe a 100% data transmission success rate during the tests. Although the data transmission parts were all successful, it is worth noting that after the user clicked the virtual push-button, it may take up to a few second for the user to receive the updated time due to the broadcast frequency, but the data received was still accurate. However, the user classification function did not work perfectly. Although it reached a success rate of over 65%, it still needs to be improved in the future. The aforementioned AI technology may help to greatly reduce the error rate.

The range limit test was successful, every time the researchers sent requests outside the detection range, the “Not In Range” message popped up.

Chapter 5. Conclusion and Future Work

5.1 Conclusion

In this research, our team designed and produced a new way for different types of non-motorized road users to communicate with the signal controller. The project proposed a system that improved the accessibility, equity, reliability and safety over the traditional push-button switch system and other types of mobile app based alternatives. An Android mobile phone app that could collect and classify users' motion and geographical data was developed, and could help users sending and receiving the necessary information without invading users' privacy. A Wi-Fi based Smart Gateway was also integrated to the RSD that could translate and exchange information between different components in the system, and provided reliable, fast, and safe user experience. The experiments showed that the system could replace the physical push-button switches currently on the street and achieve a touch-free, fast response, and easy access to all types of non-motorized road users.

5.2 Future Work

The technology elaborated in the above sections are not the only technologies we could use to solve the problem. Other projects I worked on also expanded the possibility of the future of this project. This project certain still has its limit, for instance, although users are connected to a Wi-Fi network provided by the antenna system, the network is still a local area network, and because of the designs of most mobile phones on the market force the users to use only either Wi-Fi or cellular network, the user of the app has no option but to cut off his/her connection to the Internet to use the service. Although there is usually no need for a person to use the internet during the process of crossing the intersection, forcing to disconnect the Internet service can potentially cause inconvenience.

Therefore, part of the other project I participated in may help solving the inconvenience. In this project, the edge device collects, processes, and transmits the processed data, including large amounts of images and texts, to the server. A folder in the server is synced with Google Drive so that every little change inside the folder can be reflected in the Google Drive target folder. The server used in the process is strictly protected by the University, and only students and faculty who knows the username and password can have access to it. On the other hand, the Google Drive service has activated the Two-Factor Authentication, which has an adequate level of security. It usually only takes 1-2 seconds for an image of 110 kb to go through the whole transmitting process (edge device – server – Google Drive - user) and plain texts to show short timing information takes no time.

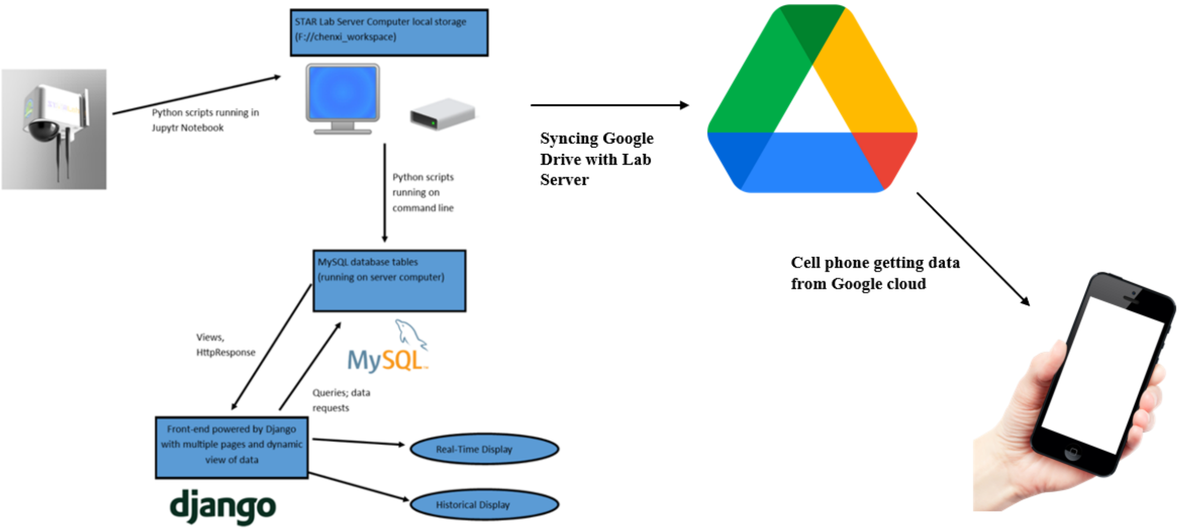


Figure 5-1 The overall logic of the new technic.

Like the current app, this app also has a welcome page and contact information page before entering the main function page. On the main function page, users are allowed to choose either viewing one of the 3 camera views or all 3 camera views together. A warning function is developed for the app, if the camera detects something dangerous happening on the road, it will pop up on the screen, and can potentially pop up at any screen of this app except contract and welcome page.

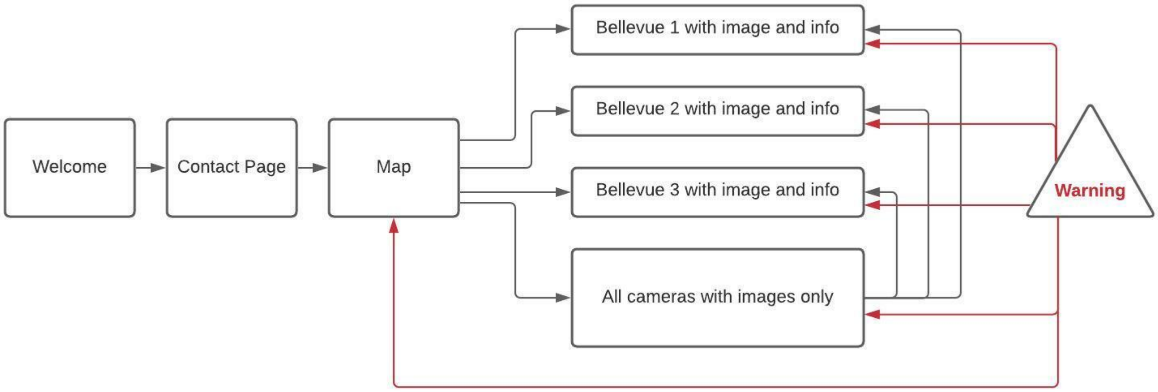


Figure 5-2 Overall app design logic of the app with the new technic.

Figure 5-3 shows the images captured by the cameras onsite and all of them were sent to a server in the UW STAR Lab. Each image was name by the time it was captured and sorted by time. This technique can potentially help this project because it avoided the high data volume of video while also be capable of collecting and broadcast information to road users. However, the data volume can be a potential problem because the edge devices usually do not have large storage space, therefore the data storage strategy needs to be optimized if this project wants to adapt the technology.

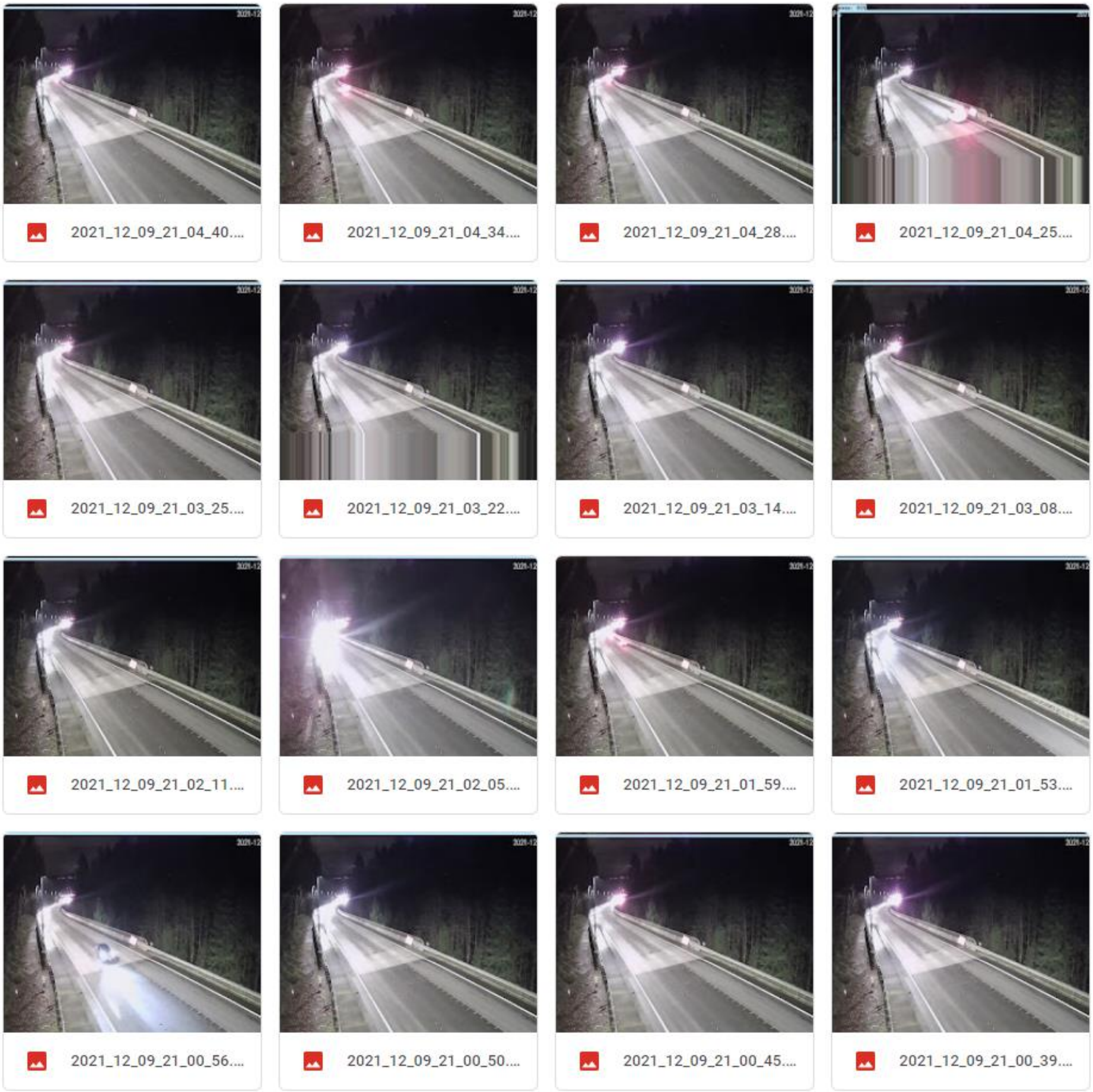
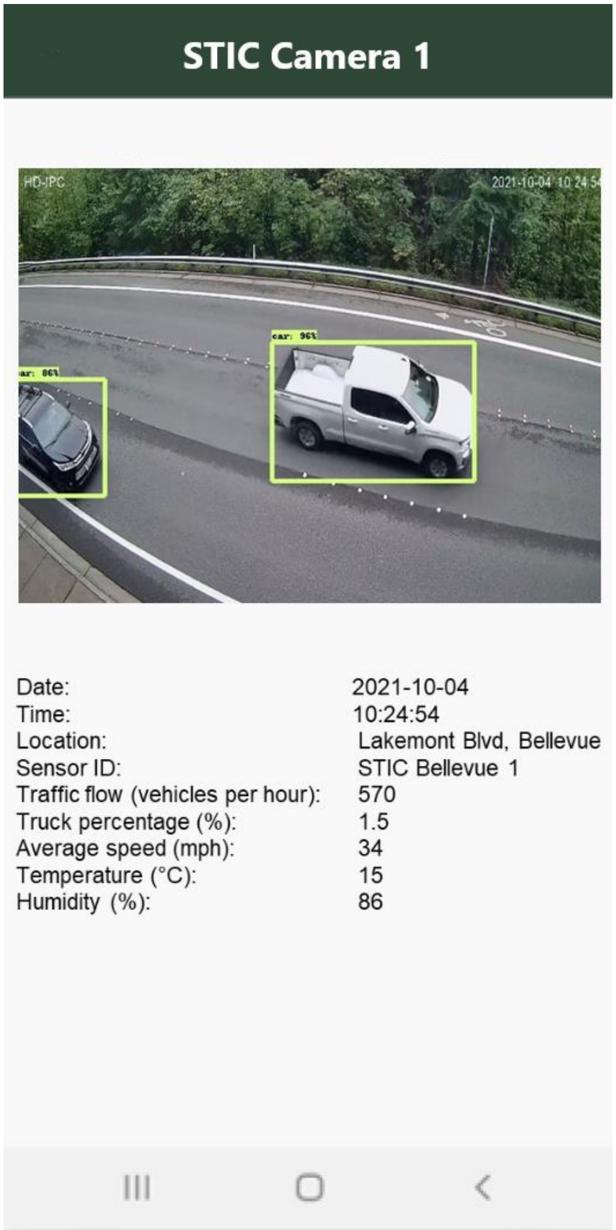


Figure 5-3 Sample image storage interface of the app with the new technic.

For the app design, the new project used a similar them as this project, it also used green as the theme color to represent the Evergreen State. The main page of the app, a satellite map is shown, and will indicate the location of all the cameras installed within the region. When users click on the senser icon, they will be redirected to the corresponding camera view page. And if users click the “See All” button, they will be re directed to the page that can see all the camera views. This page design can improve the main page of the current app. Currently, the map only follow users' selection of locations, but if users can have choice to select specific intersections on the map, the user experience can be improved, especially when some intersections are placed closely together.

Click on locations to view LIVE STATUS

Figure 5-4 The main page of the app that applied the new technic.



STIC Camera 1

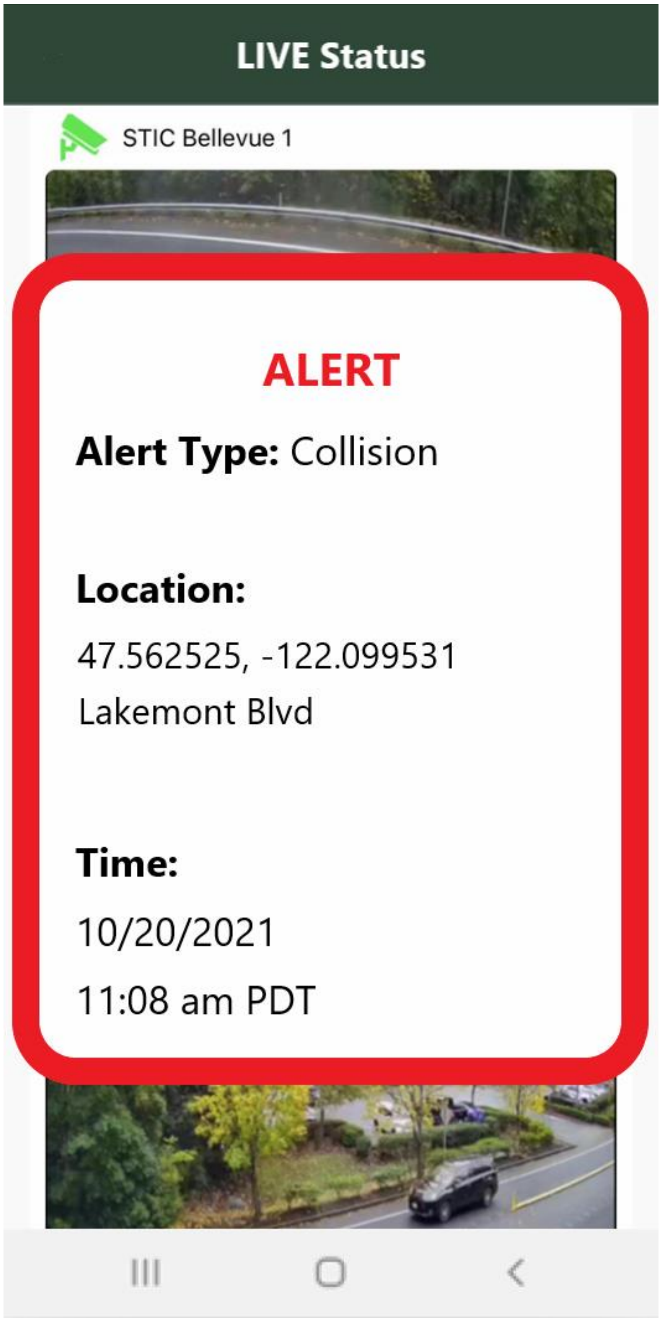
Date: 2021-10-04
Time: 10:24:54
Location: Lakemont Blvd, Bellevue
Sensor ID: STIC Bellevue 1
Traffic flow (vehicles per hour): 570
Truck percentage (%): 1.5
Average speed (mph): 34
Temperature (°C): 15
Humidity (%): 86

Figure 5-5 The text status viewing page of the app that applied the new technic.

On the test status viewing page, users can see the constantly updating camera views. The image will be refreshed every 15-30 seconds. Under the image section, date, time, location, sensor ID, traffic flow, truck percentage, average speed, temperature, and humidity are described. This type of pages may benefit our current app by showing users some information about the intersection, such as surface conditions during winter time.

Figure 5-6 The image status overview page of the app that applied the new technic.

On the image status overview page, the detailed information about the images will be concealed to let users see more pictures. However, the camera IDs are retained to ensure users not to confuse about with camera they are looking at. A page like this may benefit this project to let users know as much about the critical information about the intersections as possible, especially after the intersection-intersection network is established.



ALERT

Alert Type: Collision

Location:
47.562525, -122.099531
Lakemont Blvd

Time:
10/20/2021
11:08 am PDT

Figure 5-7 The image status viewing page of the app that applied the new technic.

The alert function can pop up the alert at any page, telling the user why there is an alert, the location the alert is associated with, and the time when the event happened. The warning function is very useful, especially for the non-motorized road users. Many dangerous events can happen both on the road and on the sidewalk, if the system can capture these events and broadcast them to the users, many fatal accidents may be avoided.

Bibliography

[1] Prisco, J. (2018, September 3). Illusion of control: Why the world is full of buttons that don't work. CNN. https://www.cnn.com/style/article/placebo-buttons-design/index.html.

[2] Society of Automotive Engineers (SAE). (2016). Dedicated Short Range Communications (DSRC) Message Set Dictionary (MAR2016), SAE, Warrendale, PA.

[3] SAE. (2016). Surface Vehicle Recommended Practice J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE, Warrendale, PA.

[4] Barbaresso, J., Cordahi, G., Garcia, D., Hill, C., Jendejec, A., and Wright, K. (2014). USDOT's Intelligent Transportation Systems (ITS) Strategic Plan 2015-2019, USDOT ITS Joint Program Office, Washington, DC.

[5] USDOT. (NDf). "Interoperability White Paper." Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/research_ares/WhitePaper_interoperability.htm> (Jan. 3, 2019).

[6] Hill, C., and Krueger, G. (No date). "Module 13: Connected Vehicles." ITS ePrimer, <https://www.pcb.its.dot.gov/eprimer/module13.aspx#dsrc> (Jan. 3, 2019).

[7] National Operations Center of Excellence [7]. (2019). "SPaT Challenge Overview." NOCoE, <https://transportationops.org/spatchallenge> (Jan. 4, 2019).

[8] SPaT Challenge Resource Team (SCRT). (2018). SPaT Infrastructure System Model Concept of Operations Draft Version 1.6, NOCOE, Washington, DC.

[9] Rohani, M., Gingras, D., and Gruyer, D. (2014). "Dynamic base station DGPS for Cooperative Vehicle Localization." Proc., 2014 International Conference on Connected Vehicles and Expo (ICCVE), IEEE, 781-785.

[10] Shen, M., Sun, J., Peng, H., and Zhao, D. (2018). “Shen, Macheng, et al. "Improving localization accuracy in connected vehicle networks using rao-blackwellized particle filters: Theory, simulations, and experiments.” IEEE Transactions on Intelligent Transportation Systems.

[11] Harding, J., Powell, G., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., and Wang, J. (2014). Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application, National Highway Traffic Safety Administration, Washington, DC.

[12] USDOT. (NDb). “CV Pilot Deployment Program.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/pilots/pilots_v2i.htm> (Jan. 3, 2019).

[13] Connected Vehicle Reference Implementation Architecture Team (CVRIA Team). (2016). “Pedestrian in Signalized Crosswalk Warning.” Connected Vehicle Reference Implementation Architecture, <https://local.iteris.com/cvria/html/applications/app51.html> (Apr. 16, 2019).

[14] USDOT. (ND). “Security Credential Management System (SCMS).” USDOT ITS JPO, < https://www.its.dot.gov/resources/scms.htm> (May 1, 2019).

[15] USDOT. (NDc). “Connected Vehicle Pilot Deployment Program: New York City (NYC) DOT Pilot.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/pilots/pilots_nycdot.htm> (Jan. 3, 2019).

[16] USDOT. (NDd). “Connected Vehicle Pilot Deployment Program: Tampa (THEA) Pilot.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/pilots/pilots_thea.htm> (Jan. 3, 2019).

[17] USDOT. (NDe). “Connected Vehicle Pilot Deployment Program: Wyoming (WY) DOT Pilot.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/pilots/pilots_wydot.htm> (Jan. 3, 2019).

[18] New York City Department of Transportation (NYCDOT). (2019). “CV Safety Apps.” NYC Connected Vehicle Project, <https://www.cvp.nyc/cv-safety-apps> (Jan. 3, 2019).

[19] Giampapa, J. A., Steinfeld, A., Teves, E, Dias, M. B., and Rubinstein, Z. (2017). Accessible Transportation Technologies Research Initiative (ATTRI): State of the Practice Scan, The Robotics Institute at Carnegie Mellon University, Pittsburgh, PA.

[20] Carnegie Mellon University (CMU). (2018). ATTRI Project Update Webinar 4 – Safe Intersection Crossing, CMU, Pittsburgh, PA.

[21] Liao, C.-F., Rakauskas, M., and Rayankula, A. (2011). Development of Mobile Accessible Pedestrian Signals (MAPS) for Blind Pedestrians at Signalized Intersections, Intelligent Transportation Systems Institute Center for Transportation Studies, Minneapolis, MN.

[22] Yin, J., ElBatt, T., Yeung, G., Ryu, B., Habermas, S., Krishnan, H., and Talty, T. (2004). “Performance evaluation of safety applications over DSRC vehicular ad hoc networks.” Proc., VANET ’04 1st ACM international workshop on Vehicular ad hoc networks, ACM, Philadelphia, PA, 1-9.

[23] Liu, Z., Liu, Z., Meng, Z., Yang, X., Pu, L., and Zhang, L. (2016). “Implementation and performance measurement of a V2X system for vehicle and pedestrian safety.” International Journal of Distbiuted Sensor Networks, 12(9), 1-14.

[24] Sugimoto, C., Nakamura, Y., and Hashimoto, T. (2008). "Prototype of pedestrian-to-vehicle communication system for the prevention of pedestrian accidents using both 3G

wireless and WLAN communication." Proc., 3rd International Symposium on Wireless Pervasive Computing 2008, ISWPC, 764–767.

[25] Hussein, A., Garcia, F., Armingol, J.M., and Olaverri-Monreal, C. (2016). "P2V and V2P communication for Pedestrian warning on the basis of Autonomous Vehicles." Proc., IEEE 19th International Conference on Intelligent Transportation Systems (ITSC) 2016, IEEE, 2034–2039.

[26] Anaya, J.J., Merdrignac, P., Shagdar, O., Nashashibi, F., and Naranjo, J.E. (2014). "Vehicle to pedestrian communications for protection of vulnerable road users." Proc., Intelligent Vehicles Symposium Proceedings 2014, IEEE, 1037–1042.

[27] Ryu, D. H., Kim, H.-J., and Um, K. (2009). "Reducing security vulnerabilities for critical infrastructure." Journal of Loss Prevention in the Process Industries, 22(6), 1020-1024.

[28] Eiza, M.-H., and Ni, Q. (2017). "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity." IEEE Vehicular Technology Magazine, 12(2), 45-51.

[29] Zheng, B., et al. (2015). "Design and verification for transportation system security." Proc., 52nd annual design automation conference, ACM.

[30] Lopez, I., and Aguado, M. (2015). "Cyber security analysis of the European train control system." IEEE Communications Magazine, 53(10), 110-116.

[31] USDOT. (NDg). “Connected Vehicles and Cybersecurity Infographic.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/factsheets/pdf/cv_%20cybersecurity.pdf> (Jan. 3, 2019).

[32] National Highway Traffic Safety Administration (NHTSA). (2016). Cybersecurity Best Practices for Modern Vehicles (Report No. DOT HS 812 333), NHTSA, Washington, DC.

[33] Ivanov, I., Maple, C., Watson, T., and Lee, S. (2018). "Cyber security standards and issues in V2X communications for Internet of Vehicles." Proc., Living in the Internet of Things: Cybersecurity of the IoT-2018, IEEE, London, UK.

[34] European Telecommunications Standards Institute (ETSI). (2014). ETSI 3GPP TS 136 213, “Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures.”

[35] IEEE. (2016a). "IEEE Standard 802-11p:20802.11", IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2016.

[36] IEEE. (2016b). "IEEE Standard 1609.2", IEEE Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages.

[37] IEEE. (2016c). "IEEE Standard 1609.3: 221609.3", IEEE Standard for Wireless Access in Vehicular Environments (WAVE)-Networking Services.

[38] Lyamin, N. Vinel, A., Jonsson, M., and Loo, J. (2014). "Real-time detection of denial-of-service attacks in IEEE 802.11p vehicular networks." IEEE Commun. Lett., 18(1), 110-113.

[39] Ericsson. (2019). “Connected Vehicle Cloud.” Ericsson, <https://www.ericsson.com/en/portfolio/iot-and-new-business/iot-solutions/iot-for-automotive/connected-vehicle-cloud>, (Jan. 3, 2019).

[40] Zhang, T., Antunes, H., and Aggarwal, S. (2014). "Defending connected vehicles against malware: Challenges and a solution framework." IEEE Internet of Things journal , 1(1), 10-21.

[41] Wright, J., Dawson Jr., M. E., and Omar, M. (2012). "Cyber security and mobile threats: The need for antivirus applications for smart phones." Journal of Information Systems Technology and Planning, 5(14), 40-60.

[42] Yang, Z., et al. (2013). "Appintent: Analyzing sensitive data transmission in android for privacy leakage detection." *Proc., ACM SIGSAC conference on Computer & communications security*, ACM.

[43] Arabo, A., and Pranggono, B. (2013). "Mobile malware and smart device security: Trends, challenges and solutions." Proc., 19th international conference on control systems and computer science, IEEE.

[44] Bailey, M., et al. (2009). "A survey of botnet technology and defenses." Proc., Cybersecurity Applications & Technology Conference for Homeland Security, IEEE.

[45] Karim, A, Ali Shah, S.-A., and Salleh, R. (2014). "Mobile botnet attacks: a thematic taxonomy." New Perspectives in Information Systems and Technologies, Volume 2. Springer, Cham, 153-164.

[46] Schlack, B. “Cybersecurity Issues in Signal Systems.” ITS California, (May 1, 2019). https://www.itscalifornia.org/Content/AnnualMeetings/2015/Presentations/TS7-2-WCRC-ATMSCyberSecurity.pdf

[47] Ghena, B., Beyer, W., Hillaker, A., Pevarnek, J., and halderman, J. A. (2014). “Green Lights Forever: Analyzing the Security of Traffic Infrastructure.” Proc., 8th USENIX Workshop on Offensive Technologies (WOOT ’14), USENIX, San Diego, CA.

[48] Perrine, K. A., Levin, M. W., Yahia, C. N., Duell, M., and Boyles, S. D. (2019). “implications of traffic signal cybersecurity on potential deliberate traffic disruptions.” Transportation Research Part A: Policy and Practice, 120, 58-70.

[49] Zhao, M., Walker, J., and Wang, C.-C. (2012). “Security Challenges for the Intelligent Transportation System.” Proc., SecurIT ’12, ACM, Kollam, Kerala, India.

[50] Alnasser, A., Sun, H., and Jiang, J. (2019). “Cyber Security Challenges and Solutions for V2X Communications: A Survey.” arXiv:1901.01053, Submitted to Computer Networks.

[51] Siddharth Garg. (2018). Secure Mobile Applications Against Cyber Security Vulnerabilities, Hackernoon. https://hackernoon.com/secure-mobile-applications-against-cyber-security-vulnerabilities-a6d2f6f09063

[52] Domenico Raguseo. (2017). The Future of Cybersecurity, SecurityIntelligence. https://securityintelligence.com/the-future-of-cybersecurity/

[53] Ritesh Patil. (2019). Cybersecurity Issues in Mobile App Development, Security Boulevard. https://securityboulevard.com/2019/02/cybersecurity-issues-in-mobile-app-development/

[54] Li, X., & Wu, Y.-J. (2021). Real-time estimation of pedestrian volume at button-activated midblock crosswalks using traffic controller event-based data. *Transportation Research Part C: Emerging Technologies*, *122*, 102876. https://doi.org/10.1016/j.trc.2020.102876

[55] Vadakpat, G., Smith, S. F., & Rubinstein, Z. B. (2021). Technology to Make Signalized Intersections Safer for Pedestrians with Disabilities. *PUBLIC ROADS*, *84*(4).

[56] Liao, C.-F. (2013). Using a smartphone application to support visually impaired pedestrians AT signalized INTERSECTION CROSSINGS. *Transportation Research Record: Journal of the Transportation Research Board*, *2393*(1), 12–20. https://doi.org/10.3141/2393-02

[57] Wang, T., Cardone, G., Corradi, A., Torresani, L., & Campbell, A. T. (2012). Walksafe. *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications - HotMobile '12*. https://doi.org/10.1145/2162081.2162089

[58] Khosravi, S., Beak, B., Head, K. L., & Saleem, F. (2018). Assistive system to improve pedestrians’ safety and mobility in a connected vehicle technology environment. Transportation Research Record: Journal of the Transportation Research Board, 2672(19), 145–156. https://doi.org/10.1177/0361198118783598

[59] Rahimian, P., & O’Neal, E. E. (2018). Vehicle-to-Pedestrian (V2P) Communications Technology: Do Cell Phone Warnings Improve Road-Crossing Safety for Texting Pedestrians? *Transportation Research Board*.

[60] Attanayake, L., Jayasuriya, H., Mirihana, R., Maduranga, L., & Dampage, U. (n.d.). Real-Time Vision-Based & Optimized Pedestrian Crossing Control System. *INTERNATIONAL RESEARCH CONFERENCE ARTICLES*.

[61] Jang, J. A., & Lee, H. M. (2017). An analysis system of pedestrian-vehicle interaction risk level using drone videos. *2017 International Conference on Information and Communication Technology Convergence (ICTC)*. https://doi.org/10.1109/ictc.2017.8190765

[62] Kothuri, S., Nordback, K., Schrope, A., Phillips, T., & Figliozzi, M. (2017). Bicycle and pedestrian counts AT signalized Intersections using existing infrastructure. *Transportation Research Record: Journal of the Transportation Research Board*, *2644*(1), 11–18. https://doi.org/10.3141/2644-02

[63] Lesani, A., Nateghinia, E., & Miranda-Moreno, L. F. (2020). Development and evaluation of a real-time pedestrian counting system for high-volume conditions based on 2d lidar.

Transportation Research Part C: Emerging Technologies, *114*, 20–35. https://doi.org/10.1016/j.trc.2020.01.018