Extending the SR 522 Signal Phase and Timing (SPaT) Challenge to Active Transportation Users

FINAL PROJECT REPORT

by

Yinhai Wang
University of Washington

Hao Yang
University of Washington

Yifan Ling
University of Washington

John Ash
University of Washington

Department of Civil and Environmental Engineering
University of Washington, Box 352700
Seattle, Washington 98195

Sponsored by

Washington State Department of Transportation (WSDOT)
310 Maple Park Avenue SE
PO Box 47300
Olympia, WA 98504-7300

Technical Monitor
Justin Belk

for

Pacific Northwest Transportation Consortium (PacTrans)
USDOT University Transportation Center for Federal Region 10
University of Washington
More Hall 112, Box 352700
Seattle, WA 98195-2700

In cooperation with Washington State Department of Transportation

June 2023

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
WA-RD 929.1	01872752	

4. Title and Subtitle	5. Report Date
Extending the SR 522 signal Phase and Timing (SPaT) Challenge to Active Transportation Users	June 2023
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Yinhai Wang, 0000-0002-4180-5628; Hao Yang, Yifan Ling and John Ash	2022-S-UW-2

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Department of Civil and Environmental Engineering University of Washington Seattle, WA 98195-2700	11. Contract or Grant No. 69A3551747110

12. Sponsoring Organization Name and Address	13. Type of Report and Period Covered
Washington State Department of Transportation Transportation Building, MS 47372 Olympia, Washington 98504-7372 14 Doug Brodin, Project Manager, 360-705-7972	Draft research report
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Information and communication technologies offer significant advantages such as enhancing the efficiency, capacity, and reliability of traffic networks. Yet most improvements in signal management and connected vehicle interactions have concentrated on motorized traffic, neglecting non-motorized and vulnerable road users. Issues such as poor perception capabilities, outdated data gathering methods, unequal distribution of resources, and a lack of inclusivity have resulted in a challenging and hazardous environment for non-motorized users, particularly those with disabilities. To address these issues, we propose an innovative signal phase and timing (SPaT) services framework known as the Accessible Crossing Platform for Active Road Users (ACPARU) smart node. Equipped with cutting-edge computer vision algorithms and AI systems, the ACPARU smart node can collect essential data about active users such as location, category, movement direction, and mobility status, and it can create a real-time directional crossing request for each pedestrian and cyclist. The ACPARU smart node also enhances communication systems, serving as a dependable hub from which to distribute SPaT messages and manage interactions among the signal controller, connected vehicles, and users' personal devices (like mobile phones and wearables) using various protocols.

In comprehensive testing with 1,076 users across six intersections, ACPARU achieved 90.24 percent accuracy in generating directional-aware crossing triggers and 89.87 percent accuracy in estimating the mobility status of regular users and four categories of disabled individuals.

The ACPARU smart node is fully compatible with connected vehicle environments and enhances the signal system affordably, primarily because of its flexibility and compatibility with existing infrastructure. The ACPARU smart node represents the first connected infrastructure system that combines traffic sensing, data processing, and information distribution to provide self-operating, unbiased signal services based on edge computing.

17. Key Words	18. Distribution Statement
Signal control, connected infrastructure, active control	No restrictions.

19. Security Classification (of this report)	20. Security Classification (of this page)	21. No. of Pages	22. Price
Unclassified.	Unclassified.	NA	NA

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Disclaimer

The contents of this report reflect the views of the authors, who are responsible for the facts and accuracy of the data presented herein. This document is disseminated through the Washington State Department of Transportation. The contents do not necessarily reflect the views or policies of Washington State Department of Transportation or the Federal Highway Administration. This report does not constitute a standard, specification, or regulation.

SI* (Modern Metric) Conversion Factors

APPROXIMATE CONVERSIONS TO SI UNITS				
Symbol	**When You Know**	**Multiply By**	**To Find**	**Symbol**
		LENGTH		
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km
		AREA		
in^2	square inches	645.2	square millimeters	mm^2
ft^2	square feet	0.093	square meters	m^2
yd^2	square yard	0.836	square meters	m^2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square kilometers	km^2
		VOLUME		
fl oz	fluid ounces	29.57	milliliters	mL
gal	gallons	3.785	liters	L
ft^3	cubic feet	0.028	cubic meters	m^3
yd^3	cubic yards	0.765	cubic meters	m^3
	NOTE: volumes greater than 1000 L shall be shown in m^3			
		MASS		
oz	ounces	28.35	grams	g
lb	pounds	0.454	kilograms	kg
T	short tons (2000 lb)	0.907	megagrams (or "metric ton")	Mg (or "t")
		TEMPERATURE (exact degrees)		
°F	Fahrenheit	5 (F-32)/9 or (F-32)/1.8	Celsius	°C
		ILLUMINATION		
fc	foot-candles	10.76	lux	lx
fl	foot-Lamberts	3.426	$candela/m^2$	cd/m^2
		FORCE and PRESSURE or STRESS		
lbf	poundforce	4.45	newtons	N
lbf/in^2	poundforce per square inch	6.89	kilopascals	kPa

APPROXIMATE CONVERSIONS FROM SI UNITS				
Symbol	**When You Know**	**Multiply By**	**To Find**	**Symbol**
		LENGTH		
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi
		AREA		
mm^2	square millimeters	0.0016	square inches	in^2
m^2	square meters	10.764	square feet	ft^2
m^2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square kilometers	0.386	square miles	mi^2
		VOLUME		
mL	milliliters	0.034	fluid ounces	fl oz
L	liters	0.264	gallons	gal
m^3	cubic meters	35.314	cubic feet	ft^3
m^3	cubic meters	1.307	cubic yards	yd^3
		MASS		
g	grams	0.035	ounces	oz
kg	kilograms	2.202	pounds	lb
Mg (or "t")	megagrams (or "metric ton")	1.103	short tons (2000 lb)	T
		TEMPERATURE (exact degrees)		
°C	Celsius	1.8C+32	Fahrenheit	°F
		ILLUMINATION		
lx	lux	0.0929	foot-candles	fc
cd/m^2	$candela/m^2$	0.2919	foot-Lamberts	fl
		FORCE and PRESSURE or STRESS		
N	newtons	0.225	poundforce	lbf
kPa	kilopascals	0.145	poundforce per square inch	lbf/in^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section 4 of ASTM E380.
(Revised March 2003)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS LIST

AASHTO	American Association of State Highway Transportation Officials
ACPARU	Accessible Crossing Platform for Active Road Users
API	Application programming interface
ATTRI	Accessible Transportation Research Initiative
BSM	Basic Safety Message
CPU	Central processing unit
CV	Connected vehicle
CVC	Connected Vehicle Cloud
DDoS	Distributed denial of service
DoS	Denial of service
DSRC	Dedicated short-range communications
FHWA	Federal Highway Administration
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
IOOs	Infrastructure owners and operators
IoT	Internet of things
ITE	Institute of Traffic Engineers
ITS	Intelligent transportation systems
ITSA	ITS America
MAC	Media access control
MAP	MapData
MUST-II	Mobile Unit for Sensing Traffic Version 2
NHTSA	National Highway Traffic Safety Administration
NOCoE	National Operations Center of Excellence
NTCIP	National Transportation Communication for ITS Protocol
OEM	Original equipment manufacturer
PID	Personal identification device
PII	Personal identifiable information
RSE	Roadside equipment

RSU	Roadside unit
RTCM	Radio Technical Commission for Maritime Services
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SCRT	SPaT Challenge Resource Team
SPaT	Signal Phase and Timing
SSID	Service set identifier
STAR Lab	Smart Transportation Applications and Research Laboratory
TMC	Traffic management center
UDP	User Datagram Protocol
UI	User interface
USDOT	United States Department of Transportation
UW	University of Washington
V2I	Vehicle to infrastructure
V2I DC	Vehicle to Infrastructure Deployment Coalition
V2V	Vehicle to vehicle
V2X	Vehicle to other
WSDOT	Washington State Department of Transportation

1.0 INTRODUCTION AND BACKGROUND

Maintaining traffic safety is a persistent priority for the United States Department of Transportation (USDOT), along with state and local transportation authorities. Until now, the bulk of research has focused on vehicular safety, frequently neglecting the nuanced needs of active road users. These individuals have distinct characteristics that heighten their vulnerability during collisions, notably those involving motor vehicles. The National Highway Traffic Safety Administration (NHTSA) revealed that in 2018, of the 36,560 traffic-related fatalities, pedestrians accounted for 6,283 (17 percent) and bicyclists represented 857 (2 percent) (NHTSA, 2019). Disconcertingly, despite a decline in overall traffic-related fatalities between 2017 and 2018, the number of pedestrian and cyclist fatalities increased (NHTSA, 2019).

Although the issue of traffic safety has yet to be resolved, recent technological breakthroughs offer a slew of promising new solutions. Many of these advancements fall under the expansive umbrella of connected vehicle (CV) applications and Signal Phase and Timing (SPaT) applications. As elucidated in the Model Concept of Operations for the SPaT Challenge (SPaT Challenge Resource Team, 2018), the American Association of State Highway Transportation Officials (AASHTO), the Institute of Traffic Engineers (ITE), and ITS America (ITSA) have jointly initiated the Vehicle to Infrastructure Deployment Coalition (V2I DC). They have challenged public sector transportation infrastructure owners and operators (IOOs) at state and local levels to collaborate in deploying roadside dedicated short-range communications (DSRC) 5.9 GHz broadcast radio infrastructure. This will broadcast SPaT messages in real time at signalized intersections along at least one road corridor or street network, covering roughly 20 signalized intersections, in each of the 50 states by January 2020—an initiative commonly referred to as the SPaT Challenge.

At its core, the SPaT Challenge will equp intersections with DSRC-enabled roadside units (RSUs) that broadcast the SPaT messages and MapData (MAP) messages, as specified by the Society of Automotive Engineers (SAE) J2735-2016 standard. Vehicles and devices capable of receiving these messages will be able to discern current signal phases, each lane's status, and intersection geometry, and will also gain access to location correction information from a Radio Technical Commission for Maritime Services (RTCM) message. Further details are readily available through materials from the National Operations Center of Excellence (NOCoE) and the SR 522 Concept of Operations (NoCoE, 2018; Eghtedari, 2018a). Figure 1 provides an overview of how the key systems and user groups will interface within the scope of the SPaT Challenge.

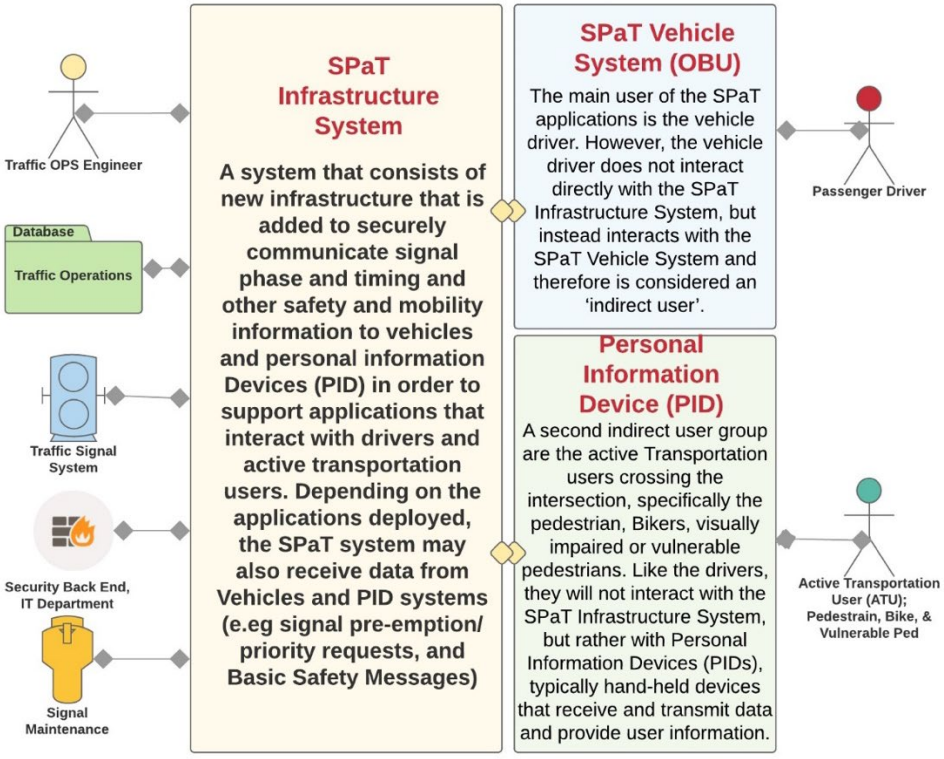

Figure 1: Interaction of key systems and user groups within the SPaT Challenge

In essence, a CV environment allows vehicles and other travelers (e.g., pedestrians, bicyclists, etc.) to communicate with each other, as well as hardware entities such as roadside

equipment (RSE) and RSUs, which is the fundamental environmental to support SPaT services. Such communication is often enabled via DSRC [Radio]. Through this protocol, CVs can send and receive data about vehicle/traveler position, speed, and more that can be used for a variety of control and safety applications (SAE, 2016). In a CV environment, data can be sent between vehicles and other vehicles (V2V communications), between vehicles and infrastructure (V2I communications), and between vehicles and other non-motorized travelers (V2X communications).

At present, the USDOT is funding three main CV 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). The NYCDOT Pilot is focused on testing a variety CV safety application on busy urban corridors (USDOT, NDa). The THEA Pilot is focused on addressing traffic operations and safety in Tampa, Florida (USDOT, NDb). Lastly, the WYDOT Pilot is studying safety and mobility applications that target freight vehicles along a rural freeway corridor (USDOT, NDc). These projects suggest that at a national level, CV project resources have been concentrated in a few main areas, so that states other than New York, Florida, and Wyoming have to find other ways to begin experimenting in the CV domain. To that end, the NOCoE initiated a program called the SPaT Challenge to encourage the study and adoption of CV applications across the country (NOCoE, 2019). Under this program, departments of transportation in all 50 states were encouraged to equip at least 20 signalized intersections with radio equipment capable of broadcasting SPaT information and other CV messages via DSRC (the CV communications standard). While this project has obvious benefits for auto drivers (e.g., eco-driving, route optimization), it and many other projects focusing on CV technologies often ignore pedestrians and other active road users.

It was the goal of this project to use these messages to help non-motorized users with their signal service needs. The Washington State Department of Transportation (WSDOT) worked with the University of Washington (UW) Smart Transportation Applications and Research Laboratory (STAR Lab) to address the signal service needs of pedestrians and bicyclists along the SR 522 corridor. The STAR Lab has successfully worked with WSDOT many times in the past, and at the time of this writing, it is working with WSDOT to install a series of sensors developed internally along SR 522. With regard to the specific needs of non-motorized users, this research initially explored the following applications outlined in the SR 522 Concept of Operations, shown in Figure 2 (Eghtedari, 2018a):

- Pedestrians in Signalized Crosswalk Warning; and
- Mobile Accessible Pedestrian Signal System.

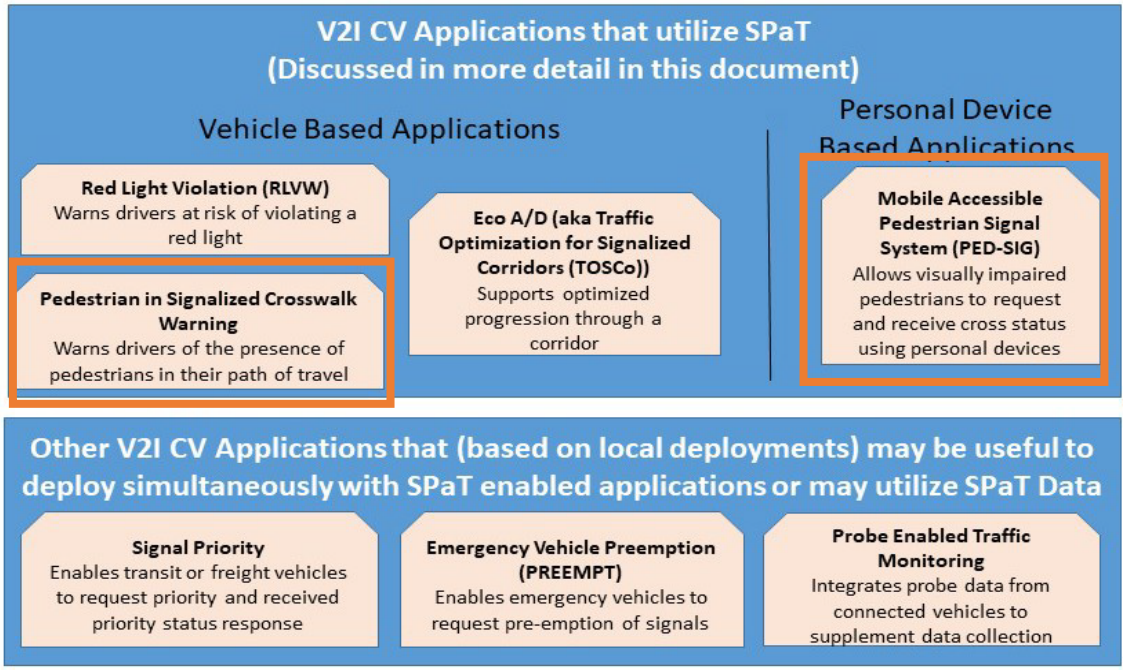

Figure 2: V2I CV Applications from the SR 522 Concept of Operations (Eghtedari, 2018a)

Several challenges that could be addressed with DSRC-enabled communications are as follows. First, vision-impaired users need a simple and consistent way to request right-of-way/walk signals. The process of requesting a call to traverse an intersection could also be improved for bicyclists and other pedestrians with disabilities. Next, beyond simply requesting a call, vision-impaired users may have trouble discerning the status of the current pedestrian signal indication. Finally, both bicyclists and pedestrians are vulnerable road user groups, potentially subject to numerous conflicts during a permitted crossing. With the ability to communicate with the traffic signal controller to receive SPaT data such as intersection geometry, as well as to communicate requests for service, the needs of the aforementioned non-motorized user groups can be addressed, and this was precisely the goal of this project.

At its core, this project involved development of a cell phone application to be used by non-motorized road users through their personal identification devices (PIDs) that will allow communication between them, an RSU, and signal controllers at intersections. An additional app will be developed to share information about signal status with drivers. At a high level, this project will serve as an important milestone in helping WSDOT achieve Goal 6 ("Smart Technology") of the WSDOT Strategic Plan. Connected vehicle research is gaining traction around the world, and WSDOT's choice to accept the SPaT Challenge and fund this project in conjunction with the Challenge will establish a strong base for future connected vehicle-related research work. Additionally, this project has many obvious potential safety benefits, especially with regard to reducing collisions with vulnerable, non-motorized users at signalized intersections. In addition, from an equity standpoint, this project will increase accessibility for non-motorized road users at signalized intersections, especially those with disabilities. Serving all user groups is critical for WSDOT, and this project will help directly address populations that

to date many connected vehicle research projects have ignored. Finally, WSDOT will have increased access to data on non-motorized user travel behavior at signalized intersections via collection through the proposed mobile apps.

2.0 LITERATURE REVIEW

2.1 LITERATURE REVIEW SUMMARY

The Signal Phasing and Timing (SPaT) Challenge will be the first foray into the realm of CVs for many state agencies. Therefore, proper understanding of a variety of components of the CV environment is necessary. At a core level, a CV environment is one in which vehicles and other travelers (e.g., pedestrians, bicyclists, etc.) are able to communicate with each other, as well as with hardware such as roadside equipment (RSE) and roadside units (RSUs). This communication is typically enabled via DSRC and allows the sending and receiving of information on vehicle/ traveler position, speed, etc. Additionally, information in the form of safety alerts and other guidance can be sent and received. To communicate this diverse set of information in an efficient manner, a series of standards has been developed that define, among other things, message type, content, and format. Background information about the primary standard in use today and relevant message types for this project is the first topic covered in the literature review.

Once message content and format are understood, the next logical step is to examine what applications specific message types have. In the context of the SPaT Challenge and this closely related project, messages conveying signal phasing and timing information are of primary importance to help active users with safe and efficient signal service. Additionally, many other applications that promote safety, especially that of active users, are worthy of investigation. These CV safety applications are the second primary component of the literature review.

The third component of the literature review focuses on a more technical aspect, specifically the communications that will enable active users to interface with the signal

controller/RSE to request signal service. Communications between mobile devices and the RSE, as well as associated cyber security issues, are covered.

The fourth and final component of this literature review deviates slightly from published work to focus on providing background information on various sensors developed by the STAR Lab that may have application in this project.

2.2 SAE J2735 STANDARD AND MESSAGES

As mentioned, DSRC has been the communication technology of choice for connected vehicles. With DSRC, various messages can be sent between vehicles and other vehicles (V2V), vehicles and infrastructure (V2I), and vehicles and other non-motorized travelers (V2X). The specific types of messages that can be sent and received have been defined by the Society of Automotive Engineers in its standard entitled "Dedicated Short Range Communications (DSRC) Message Set Dictionary." The standard was most recently updated in March of 2016, and this version is known as the SAE J2735-2016 Standard. According to SAE, "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" (SAE, 2016). Interoperability is a key part of intelligent transportation systems, including ensuring that they properly function as intended over time. With the increasing prominence of CV research, the USDOT has helped highlight the importance of this issue by defining interoperability as one of the key program categories in the "ITS Strategic Plan 2015-2019" (Barbaresso et al., 2014). While interoperability is a broad concept in scope, its main goal is to ensure that communications between devices in intelligent transportation systems (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 (Babaresso et al., 2014; USDOT, NDf). As

the SPaT Challenge is set to bring CV technologies to all 50 states, it is clear that a CV messaging standard that precisely defines the information to be sent between connected entities will be essential for ensuring that CV communications can occur over time and in a variety of locations across the country.

SAE's philosophy regarding 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) (SAE, 2016). At the top level of the hierarchy is the message itself. One level down is the data frame; each message is composed of one or more data frames. Finally, at the lowest level of the hierarchy are data elements. These are the attributes that define each data frame (SAE, 2016). However, it is important to note that while data elements are at the lowest level of the hierarchy, data frames themselves can also be composed of other data frames. Examples of the components of each of the levels of the messaging hierarchy are discussed below.

Perhaps the most ubiquitous CV message defined in the SAE J2735-2016 Standard is the Basic Safety Message (BSM). BSMs are the cornerstone of V2V safety applications, they are often sent at a frequency of 10 Hz, and the information used to define them is obtained from sensors within the vehicle (Hill and Krueger, ND). According to the SAE standard, the BSM message is composed of data frames, the primary one being the BSMcoreData data frame. This data frame comprises the data frames and data elements that are necessary to send with every BSM. 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. (SAE, 2016). To clarify how data frames themselves can be composed of other data frames, note

that vehicle size is a data frame, itself composed of two data elements, vehicle width and vehicle length (SAE, 2016). While BSMs are an integral component of a CV environment and have numerous applications, their application is not the focus of the SPaT Challenge.

According to the NOCoE, the issuer of the SPaT Challenge, the focus of the challenge is to equip intersections with the necessary hardware to enable SPaT broadcasts via DSRC. NOCoE has also noted that additional broadcasts of MapData (MAP) and Radio Technical Commission for Maritime Services (RTCM) messages should occur in conjunction with the SPaT broadcasts (NOCoE, 2019). The grouping of these three messages will allow vehicles to determine their location with respect to the intersection, as well as to obtain status information on signal indications that are relevant to their desired movements (SPaT Challenge Resource Team (SCRT), 2018).

Per the SAE J2735 Standard, "the MapData message is used to convey many types of geographic road information" (SAE, 2016). For detailed information on the exact components and structure of the MAP message, readers are directed to SAE (2016). In the interest of clarity, a higher-level overview of the message contents based on the SPaT Challenge Resource Team (SCRT) Concept of Operations (2018) follows.

Under the MAP message, each intersection is described with a unique integer identifier, and the overall location is based on a point of reference in the middle of the intersection. Lane geometry is then defined on the basis of an offset from this center point to the stop line in each lane. The rest of the lane is then defined as a series of nodes along the centerline of the lane, and locations of nodes can be described as either an offset from the preceding node or strictly in terms of latitude and longitude; crosswalks are defined in a manner similar to that of lanes. Movements permitted from each lane are also described in the message. Vehicle movement paths

can be linked with signal phasing information. Specifically, pairs of inbound and outbound lanes for allowed vehicle movements are defined. These connections are then mapped to corresponding signal groups that define signal phasing (SCRT, 2018).

SPAT messages allow traffic signal infrastructure to communicate data about signal phasing and timing with vehicles. They have a variety of applications, including improvements to safety and operations, and reduction in the environmental impact of fossil-fuel-based vehicular transportation (Hill and Krueger, ND). Again, for complete data on the structure and contents of SPaT messages, please refer to SAE (2016). As with the MAP message, the following provides a more concise summary of the information conveyed in the SPAT message based upon SCRT (2018).

Each SPAT message is able to reference specific intersections on the basis of their unique ID as defined in the MAP message. At a high level, the message can convey status information about the intersection at large, as well as about individual signal groups/phases. For intersection-wide information, the message can indicate whether the intersection is running a fixed-time or actuated control plan, as well as if it is operating under special modes such as preemption, priority, or failure flash mode. With regard to signal groups, the SPaT message can convey the interval (i.e., green, yellow, or red) running at any given time for each phase, along with estimates of when the phase may end, confidence associated with these estimates, and time until said phase will have a green indication again. All times are referenced with respect to when the given interval for a phase will terminate, instead of counting down to the change, as this reduces the number of times that the timing in the message needs to updated. Finally, the SPaT message also provides a feature called “Connection Maneuver Assistance,” which concerns pedestrian crossings. This feature allows the message to include information about pedestrian actuations as

well as actual detection of a pedestrian in the crosswalk (if the supporting detection infrastructure is available) to alert drivers that active users may be in the crosswalk (for applicable conflicting movements) (SCRT, 2018).

The final message of interest for the SPaT Challenge is the RTCM message. The contents of this message indicate a Global Positioning System (GPS) correction factor based on present atmospheric conditions that can be used to help vehicles more accurately determine locations of lanes defined in the MAP message. Correction factors can be computed at the base station at a given intersection or can be obtained remotely (e.g., calculated at a traffic management center (TMC)). The decision of whether or not to apply RTCM messages depends on a variety of factors, including the complexity of the intersection (e.g., are there lanes for protected turning movements?) and whether the intersection is impacted by the urban canyon effect. Note that not all GPS systems within vehicles can apply the information from RTCM messages (SCRT, 2018). As with the preceding two message types, the information presented here is more of a high-level summary of key message features obtained from the SCRT (2018); more detailed information on RTCM messages can be found from SAE (2016). Finally, it is important to mention that researchers are continually trying to address the vehicle localization problem, and the use of RTCM messages is far from the only way to do so. For example, studies including Rohani et al. (2014) and Shen et al. (2018) have presented vehicle localization solutions that do not rely on fixed base stations.

2.3 CV-BASED SAFETY APPLICATIONS

CV-based safety applications primarily fall into one of three categories, depending on the source and receiver of the information: V2V, V2I, or V2X. This section presents an overview of

different safety applications in each of the three categories, as well as studies that have investigated such applications (Harding et al., 2014).

V2V safety applications involve direct communication between vehicles via DSRC. Several possible V2V safety applications, as indicated by USDOT, are as follows (Harding et al., 2014):

- Intersection Movement Assist (IMA): IMA is applicable at both controlled and uncontrolled intersections, where drivers are warned of high-crash risk scenarios and advised not to proceed through the intersection.
- Left Turn Assist (LTA): Upon proceeding into the intersection, the driver is warned not to make a left turn that would lead to an angle crash with an oncoming, through-moving vehicle.
- Forward Collision Warning (FCW): Drivers are warned of potential rear-end crash scenarios with downstream vehicles.
- Emergency Electronic Brake Lights (EEBL): Drivers are warned of rapid deceleration of a downstream vehicle (with V2V capabilities) that has applied its brakes, whether or not the downstream vehicle is in immediate view.
- Blind Spot Warning/Lane Change Warning (BSW/LCW): Drivers are alerted if a vehicle is in or may travel to the location of the driver's blind spot while they initiate a lane change.
- Do Not Pass Warning (DNPW): Drivers are alerted of scenarios in which there is risk of a crash if they attempt to complete a passing maneuver.

While LTA and IMA sound similar in nature, USDOT and NHTSA denote them as separate applications (Harding et al., 2014). 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” (Harding et al., 2014). LTA is intended solely to address crashes where a left-turning vehicle would be hit by a through-moving vehicle in the intersection.

V2I-based safety applications involve scenarios in which drivers of vehicles receive warnings from RSE and other infrastructure components. The following are several common V2I applications according to USDOT (NDb):

- Red Light Violation Warning (RLVW): On the basis of the data in SPaT messages, drivers are warned if they are at risk of running a red light.
- Curve Speed Warning (CSW): Drivers are alerted if they are traveling at an unsafe speed for a curve before reaching it.
- Stop Sign Gap Assist (SSGA): Drivers are warned of scenarios that may lead to crashes at stop-controlled intersections.
- Spot Weather Impact Warning (SWIW): Drivers are warned of adverse weather conditions that are specific to certain locations they are traveling through.
- Reduced Speed/Work Zone Warning (RSWZ): Drivers are alerted of the presence of and regulatory traffic conditions (e.g., speed, etc.) in a work zone;
- Pedestrian in Signalized Crosswalk Warning: Drivers of vehicles are warned of the presence of pedestrians in a crosswalk that they will pass through in a turning maneuver. 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 (CVRIA Team, 2016).

Currently, the USDOT is funding three separate CV 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). Each of the pilot programs focuses on the installation of RSE and instrumentation of vehicles with devices that enable DSRC to test many of the aforementioned V2V and V2I applications, as well as others, in different real-world settings. As of late 2018, the pilot projects were in a phase of operations and maintenance, and applications were continuing to be tested and their performance was being evaluated (USDOT, ND). The main goal of the NYCDOT Pilot is to test a variety of DSRC-enabled safety applications along instrumented corridors in Manhattan and Brooklyn (USDOT, NDa). The THEA Pilot is focusing on improving traffic operations in Downtown Tampa, as well as targeted safety applications such as providing warnings to prevent wrong-way driving (USDOT, NDd). 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. In comparison to the other sites, this site is subject to extremely adverse winter weather, and applications surrounding weather alerts and guidance information are among the central applications (USDOT, NDe). Table 1 shows the CV applications that have been proposed for each of the test sites per USDOT (USDOT, NDc, USDOT, NDd, USDOT, NDe).

Table 1. CV applications for USDOT pilot studies
(table created from a 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

Project	Category	Application
	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 the NYCDOT and THEA pilot studies are implementing CV applications that focus on the safety and mobility needs of pedestrians. Particularly, both projects are studying the Pedestrian in Signalized Crosswalk Warning and the Mobile Accessible Pedestrian Signal applications. The former application was described earlier in this section. The

latter application presents signal status information to pedestrians and allows them to make a call for signal service at intersections with pedestrian actuation (NYCDOT, 2019).

In addition to those working directly on the USDOT CV pilot projects, other research groups have worked to develop CV applications to improve pedestrian safety and mobility. The first such application was developed as a result of the Safe Intersection Crossing Project, funded under the Accessible Transportation Research Initiative (ATTRI). ATTRI is a combined research effort of the USDOT, Federal Highway Administration (FHWA), the Federal Transit Administration (FTA), the ITS Joint Program Office, and the National Institute of Disability, Independent Living, and Rehabilitation Research (NIDILRR) (Giampapa et al., 2017). ATTRI research has sought to address the transportation needs of people with disabilities, veterans with disabilities, and elderly people through projects that focus on technological solutions in the areas of "wayfinding and navigation, assistive technologies, automation and robotics, data integration, and enhanced human service transportation" (Giampapa et al., 2017). For the Safe Intersection Crossing Project, researchers at Carnegie Melon University (CMU) led an effort to develop a mobile application (app) that could enable communication between pedestrians with disabilities and the signal control system at a test site in Pittsburgh, Pennsylvania. The app would allow users to see information on signal phasing and timing and ensure that their needs were understood by the signal system. Given detection of app users, the signal control system was able to estimate the arrival times of pedestrians and add additional green time based on current crossing conditions as a means to improve safety. Under this system, users of the app had to equip their phones with a sleeve-like device that fit over the phone and extended it to have the necessary DSRC capabilities to communicate with an RSE (CMU, 2018). In Minnesota, Liao et al. (2011) developed a Mobile Accessible Pedestrian Signals (MAPS) system with a focus on

improving the crossing experience of pedestrians with vision impairment. As part of their system, they developed a smartphone app that enabled users to obtain intersection geometry data (e.g., street name, direction, number of lanes on a given approach, etc.) and to request the walk indication for a given crossing direction from the signal controller.

Because large-scale CV testbeds are few in number, many studies have focused on the performance of factors associated with DSRC and other means of communication of safety information. Yin et al. (2004) simulated a DSRC vehicular ad hoc network in which vehicles used a collision avoidance algorithm. They noted that DSRC did not seem to suffer from latency issues, but its throughput capacity could be enhanced. Liu et al. (2016) developed a V2X communication system rooted in WiFi 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. Others focused more on applications. Sugimoto et al. (2008) developed a collision risk estimation algorithm for vehicle and pedestrian crashes that relied on cellular communications between vehicles and pedestrians and a vehicle's GPS system. They noted that a test of their application in the field provided drivers with more time to safely respond to pedestrians who were not immediately in their field of view. Hussein et al. (2016) developed a crash prediction algorithm based on communications between vehicles and pedestrians. The algorithm ran on a smartphone and applied the GPS and magnetometer sensors to determine location and direction; then proper location information could be shared among vehicles and pedestrians, and time and location of collisions could be estimated. On the basis of the estimated severity, a warning message could be provided to the pedestrian. Anaya et al. (2014) developed an app and collision prediction algorithm for vehicle-pedestrian crashes that estimated collision risk and warned pedestrians of that risk via the app.

The app relied on WiFi communication, and the study determined that packet delivery ratio (i.e., transmission performance) was adversely impacted by people's bodies blocking the signal.

2.4 COMMUNICATIONS AND CYBERSECURITY ISSUES

Cybersecurity is a significant issue surrounding communication between the RSU/signal controller and personal mobile devices; it has a direct influence on the reliability of a communication system. Currently, an increasing number of smart devices have been the targets of cyberattacks because of their increased connectivity (Ryu et al., 2009; Eiza and Ni, 2017). Generally, cyberattacks may happen when the target is in the communication range of the attackers; this range can vary tremendously, depending on device type and means of communication used. Therefore, cybersecurity is addressed in the connected environment for a variety of applications that include, but are not limited to, V2V communication, V2I communication, and even train control systems (Zheng., 2015; Lopez and Aguado, 2015). No matter the application, secure and uniform practices should be applied to the entire connected environment that encompass vehicles, traffic signals, work zones, and many other parts of the connected vehicle ecosystem (USDOT, NDg). To date, several studies have focused on cybersecurity in the connected vehicle environment (NHTSA, 2016; Ivanov et al., 2018; ETSI, 2014).

In the CV environment, V2V and V2I are two important means of communication that can prevent collisions. The core communication protocol for both applications is DSRC. DSRC uses multiple standards: IEEE 802.11p (IEEE, 2016a) wireless access for the physical layer and medium access control functions, IEEE 1609.2 (IEEE, 2016b) for security services, and IEEE 1609.3 (IEEE, 2016c) for network services. When DSRC is used, a potential threat can occur when a malicious node either hacks into devices with DSRC equipment or sends fake safety

information. In addition, denial of service (DoS) is another possible means of attack. Lyamin et al. (2014) studied jamming DoS attacks related to the IEEE 802.11p standard in which a malicious node corrupts the exchanged safety messages in a platoon. To fend off 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 connected vehicle environment with applications such as the Connected Vehicle Cloud (CVC) system developed by Ericsson (2019). The CVC system builds a new channel between the vehicle and a variety of services and support provided by original equipment manufacturer (OEM) partners. The security layer provided in the CVC ensures that the communication between the vehicle and the system is encrypted. Zhang et al. (2014) built a defense framework for malware and presented a lightweight malware defense function that can operate in vehicles (Zhang et al., 2014).

Smart phones applications in a CV environment, as was the case for this project, also provide more uncertainties for the SPaT system. Phone apps themselves can suffer security vulnerabilities that can lead to personal data leakage and malware infection (Wright et al., 2012). Personal data leakage from mobile phones typically results from unsafe mobile apps that are embedded with specific code to steal and transmit sensitive data (Yang, 2013). Another major and common problem is malware. Among the different variants of malware, botnets are considered to be the biggest challenge. Botnets are used to send email spam, carry out distributed denial of services (DDoS) attacks, and host phishing and malware sites (Arabo and Pranggono, 2013; Bailey, 2009). Currently, Botnets are gradually transferring to smart devices, since those devices have wide distribution and are powerful enough to run a bot and offer additional gains for a bot-master. With PC-based botnets, cybercriminals often use zombies within botnets to

launch DDoS attacks, and they may happen in the near future on mobile platforms (Karim et al., 2014).

2.5 BACKGROUND ON APPLICATIONS OF EXISTING STAR LAB SENSORS

Over the past decade or so, the STAR Lab at UW has worked to develop a variety of different traffic sensors. This development has included both hardware (e.g., circuitry) and software (e.g., development of video image processing algorithms). One such sensor that the lab developed recently and that may be useful for this project is called the Mobile Unit for Sensing Traffic Version 2 (MUST-II). The MUST-II is a small-form factor sensor, developed on top of the Raspberry Pi single-board computer, that is able to detect media access control (MAC) addresses via Bluetooth and WiFi. Recently, a camera was added to allow video detection for applications such as road-surface monitoring. The team has installed the sensor in a variety of real-world testbeds as follows:

- City of Tianjin, China: Sixteen sensors were installed along several urban corridors in downtown Tianjin to monitor travel times, path volumes (of detected devices), and point volumes (i.e., volumes of mobile devices at a given intersection) on campus roadways, as well as to detect volumes of mobile devices.
- Tongji University in Shanghai, China: Forty-four sensors were installed to monitor travel speeds on campus roadways, as well as to detect volumes of mobile devices.
- State Route 522 (SR 522 Lake City/Bothell Way): Five sensors were installed to collect volume data (of detected devices) and travel time data at five intersections that were implemented with RSE for the SPaT Challenge project. These sensors were installed in late 2018 as part of another WSDOT-UW project entitled “Understanding Opportunities with Connected Vehicles in the Smart Cities Context.”

Data collected from the first two testbeds are currently visualized interactively on the STAR Lab's big transportation data platform, the Digital Roadway Interactive Visualization and Evaluation Network (DRIVE Net, www.uwdrive.net).

For this project, it was envisioned that the MUST-II's capabilities could be extended to add two more functions. One would be to perform as the communication base station to connect non-motorized users and the signal control system. A DSRC transmitter could be connected to the MUST-II to send and receive messages. The second new function would be to act as the detector to detect non-motorized users in case they did not use the app or bring a smart phone with them. Three methods of detection could be applied for non-motorized user detection: Wi-Fi, Bluetooth, and video (Kjærgaard et al., 2012; Malinovskiy et al., 2012; Xu et al., 2005; Wang et al., 2014).

2.6 CYBERSECURITY OVERVIEW ON CONNECTED INFRASTRUCTURE

The SAE defines cybersecurity as "measures taken to protect a cyber-physical system against unauthorized access or attack" (SAE, 2016). A cyber-physical system is defined as a system made up of communications and computer devices used for control applications (SAE, 2016). In the context of this project, key components of the cyber-physical system of interest were vehicles with on-board equipment (OBE), the signal controller and associated RSE, and OBEs used by pedestrians. Because this project would enable communications between PIDs and the RSE, as well as the RSE and OBE in vehicles, a variety of potential cybersecurity issues would have to be addressed to ensure the safety of travelers and information. The following discusses common and relevant cybersecurity issues, agency awareness and response to cybersecurity issues, and some potential means to address the issues.

2.6.1 Overview of Cybersecurity Issues

Schlack (2015) described cybersecurity issues facing the network of traffic signals in Washtenaw County, Michigan. He noted that the county's traffic signal controllers were able to communicate via the 900-MHz or 5.8-GHz communication bands and that with a radio and a laptop, a bad actor could easily find the network service set identifier (SSID), connect to the network, and communicate with the traffic controllers. An experiment conducted by Ghena et al. (2014) 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, the authors recommended that agencies use encryption methods, make SSIDs invisible to the general public, use firewalls to prevent access to unused ports, and make sure that firmware was always set to the most recent version (Schlack, 2015; Ghena et al., 2014).

Perrine et al. (2019) provided an overview of the potential vulnerabilities of traffic signal control systems. An extremely common issue they mentioned, albeit simple, is the use of default usernames and passwords for traffic signal controller hardware. They further discussed how conventional security practices for traffic operations applications have a decreasing number of security features, moving from the network security level to the operating system level, to the application level (Perrine et al., 2019). While the focus of this project was not on addressing cybersecurity issues for proprietary traffic signal controllers, it was important to be aware of such issues, as this project involved creation of a mobile app to communicate with the signal controller/RSE. Hence, it was of paramount importance to ensure that the app would allow only the minimal amount of functionality needed to ensure safe and efficient use and would not allow for any unintended means of accessing/manipulating control plans maintained by the controller, as was done by Ghena et al. (2014).

In terms of cybersecurity for CV applications, Zhao et al. (2012) discussed issues directly related to V2X messaging. They noted that the consequences of attacks on V2X messaging could include deleting messages, changing the information in them, and delaying their reception. They further discussed that authenticating messages as a means of security might not always be practical, especially in real-time safety applications because of data transmission and processing limits (Zhao et al., 2012).

Alnasser et al. (2019) provided a comprehensive view of cybersecurity challenges for V2X communications. They broke down threats to the IEEE 802.11p standard and the LTE-V2X communication protocols. In terms of threats to information access, they described the following types of attacks as possibilities: blackhole/greyhole, flooding, jamming, and coalition/platooning. Blackhole and greyhole attacks result from an attacker blocking all or some of the communications from a given device; in some cases, it can be prevented by requiring authentication. Flooding is the opposite of the blackhole attack, in that the attacker sends numerous messages to a device such that it can no longer receive them from other devices. Jamming results when attackers send signals to disrupt communications, and coalition attacks involve coordinated attack efforts by multiple actors (Alnasser et al., 2019).

Threats to message integrity can be grouped into three categories. One such attack involves changing the contents of the message for nefarious purposes, and while it can be hard to address internal attacks, external attacks can often be prevented through encryption and authentication. The other main categories of message integrity attacks include changing the time order in which messages are received and altering the location data via GPS spoofing (Alnasser et al., 2019). Threats to confidentiality and authenticity were also described in Alnasser et al.

(2019), followed by an overview of security solutions classified as either cryptography-based, behavior-based, or identity-based.

2.6.2 Agency Perspective on Cybersecurity

Agencies taking part in the USDOT-sponsored connected pilots are indeed aware of the cybersecurity risks that such projects pose and are taking actions to best ensure the safety of their systems now and into the future. Recall that NYCDOT chose to implement both the Pedestrian in Signalized Crosswalk Warning and Mobile Accessible Pedestrian Signal System (PED-SIG) applications as part of its CV pilot project (NYCDOT, 2019). For the latter application, NCYDOT (2019) noted that the PID/mobile device will allow pedestrians to request signal service at intersections with pedestrian-actuated crossing phases. Therefore, a communication link will be necessarily established between the PID and RSE to enable proper functionality of this application. To address related cybersecurity concerns, NYCDOT (2018) provided language to outline awareness of and the need to address many such concerns in the specification document for pedestrian assistance devices (NYCDOT, 2018). Specifically, in the document, they noted that the app running on the PID must receive credentials from the Security Credential Management System (SCMS), which will in turn make it able to authenticate the various messages (e.g., SPaT and MAP) that it receives from the RSE (NYCDOT, 2018). They further noted issues such as requiring a stringent password policy for users of the app and protecting against attacks of the app by "by inserting a token in every form and rendering the URL as protected by requesting confirmation with the application programming interface (API) or use of the token with the URL that verifies that the token is present and valid on the response handling" (NYCDOT, 2018). For a full list of the security constraints placed on the PED-SIG app run via a PID by NYCDOT, interested readers are referred to NYCDOT (2018).

Before implementation of the Pedestrian in Signalized Crosswalk Warning and PED-SIG apps, NYCDOT was tasked with completing the pilot project's data privacy plan (Van Duren, 2016). One chapter of this plan addressed the issue of personal identifiable information (PII) contained in the SAE J2735 message set. Regarding the Pedestrian in Signalized Crosswalk application, they noted that the application would not involve gathering of any PII. Furthermore, the communication between the RSE and OBE would be unidirectional in that the OBE would not need to send any information to the RSE under the application's implementation. In terms of the PED-SIG app, they noted that data on the precise time and location of pedestrians using the app would be removed when data on usage of the app were sent to the TMC (Van Duren et al., 2016).

In the aforementioned NYCDOT applications, the SCMS in question is part of a broader suite of cybersecurity solutions endorsed by the USDOT and developed by the USDOT in collaboration with the auto industry. According to Gay (2011), the USDOT is following a "security by design" procedure in its implementation of CV technologies and related systems. This means that the systems are to be designed with due consideration given to the cybersecurity issues they may face. Indeed, the SCMS is a key part of the suite of tools intended to ensure cybersecurity in the realm of DSRC. Put simply, the SCMS is a proof-of-concept system that applies encryption and certificate management techniques to allow for "trusted communication" in V2V and V2I applications (USDOT, ND). Approved users of the SCMS can then authenticate messages and evaluate their contents. The certificates used by the SCMS do not contain any PII or other information that could be used to identify a vehicle; they are solely used for authentication purposes (USDOT, ND). To enroll as part of the system, devices must make a request to the USDOT; this allows the USDOT to certify devices and ensure that they follow

predefined requirements (Kreeb and Gay, ND). Once devices have been enrolled in USDOT's system, they get security certificates from certificate authorities (CAs) that serve as a component of a digital signature on messages that the devices send. The SCMS can also collect and evaluate reports of misbehaving devices and determine whether to ban a device as a trusted source to send/receive messages within the system (Kreeb and Gay, ND). Currently, only projects funded by the USDOT are able to request access to the SCMS proof of concept (Kreeb and Gay, ND).

In terms of other agency-level work on cybersecurity, some agencies have focused on the issue from the vehicle perspective. The SAE (2016) published the *Surface Vehicle Recommended Practice J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*. This guidebook focuses on vehicle cybersecurity issues and covers subjects such as determination of cybersecurity threats and how to design proper security measures to manage such threats over a cyber-physical vehicle system's lifecycle (SAE, 2016). NHTSA (2016) also developed a guidebook on cybersecurity best practices for vehicles. The guide serves as a high-level overview and covers issues such as information sharing, vulnerability reporting, risk assessment, and several so-called fundamental protections, some of which are relevant to non-vehicle applications (NHTSA, 2016). Some of the fundamental protections that the NHTSA notes as key takeaways from this document include limiting developer access to devices following the development work, controlling access to keys/passwords, controlling access to and the ability to alter firmware, storing data on events as they can help trace attacks, and controlling communication with servers by applying encryption methods and verifying devices based on certificates (NHTSA, 2016).

2.6.3 Mobile Application Development on Cybersecurity

Mobile applications (apps) are increasingly becoming a necessity in daily life and playing a significant role in all kinds of activities such as navigation. However, apps easily suffer from vulnerability to different types of cyberattacks that need to be addressed with great attention in order to increase the apps' overall robustness. Because this project involved the development of a mobile app, it was critical to make sure that potential vulnerabilities were addressed to increase the app's potential for widespread use and adoption. Five representative cybersecurity challenges that are faced in app development are discussed below.

The first and most important challenge is that of data encryption. After encryption, the data can be converted into a form that is unreadable without decryption. Given that the app may contain users' private information, such as current location, it is important to apply encryption for data security (Martínez-Pérez et al., 2015). This can effectively avoid the illegal use of PII or other sensitive data. Even if the encrypted data leak, it is very hard to decode them directly. Data encryption was necessary for the development of the app in this project because location information of pedestrians would be necessary to properly localize them at a given intersection and allow them to place a call for service. The STAR Lab gained experience in applying encryption in some of its past work on mobile sensing. Notably, the lab worked to develop a sensor known as the Mobile Unit for Sensing Traffic Version Two (MUST-II). The MUST-II can detect mobile devices via their MAC addresses over Bluetooth or WiFi when a given mobile device is within the detection range of the sensor. To provide anonymity and avoid potential security concerns, the MAC address of each detected mobile device is encrypted by using a hashing algorithm. Hashing algorithms are a common cryptographic means of encryption, and they apply a function to map unencrypted data to an encrypted form.

Another key security concern in app development is user authentication. User authentication is important for protecting users' privacy and ensuring that the person using the app is the desired user and has permission to do so. Like data encryption, user authentication aims to ensure data privacy, but the difference between them is that data encryption can protect data security even when data leaks. Furthermore, user authentication prevents others (i.e., non-authorized users) from logging into the account associated with usage of a given app. Common means of user authentication include requiring users to have a username and password combination to log into and access an app. Recently to further improve security, two-factor authentication has been more widely applied (Aloul et al., 2009). In comparison to one-factor authentication, two-factor authentication uses the mobile phone as a software token to generate a one-time passcode for usage of an app. If not used within a certain amount of time, the passcode expires, and the user must request another new code to log into the app. Ensuring strong passwords and changing them and usernames from the default or easily predictable values is critical for restricting access to apps/information to only those who should actually have it.

The third key concern for app development cybersecurity is the avoidance 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 (Siddharth, 2018). By using communication keys, hackers can understand the code and logic used to develop the app, which provides a path for back-office attacks (e.g., attacks of the servers storing information in the databases that are used to power the app). Thus, in some cases, reverse-engineering can allow users' credentials (e.g., app usernames and passwords), as well as any PII that may be stored on the server-side, to be stolen. There are some common methods to prevent reverse engineering. One approach involves saving important code on a server (which

itself must be secured) rather than in the app itself, as this substantially decreases a hacker's ability to access the code. Additionally, and as with the topic of encryption, hashing algorithms can be applied to obscure data and map them into a form that cannot be understood/easily translated without access to and knowledge of the used hashing algorithm.

Although perhaps a bit more general in scope, the fourth key cybersecurity concern in app development is future preparation. In most cases, an app is designed for defending against known cybersecurity problems at a given point in time. Therefore, apps usually do not have the ability to cope with upcoming cybersecurity challenges, which are constantly changing in their ubiquity and complexity. However, by analyzing current development trends, developers can predict some future challenges. For example, the communication between an app and Internet of things (IoT) devices should be addressed (Domenico, 2017). With the popularity of IoT devices, there are more potential access points for apps, which also increases the possibility of their being attacked. Furthermore, a flexible app framework can help simplify future security updates.

The final security issue in app development is having insecure code. Even if all of the aforementioned challenges have been overcome, insecure code can ruin all previously completed work. A lot of cybersecurity problems are caused by insecure code during the development process. For example, some abnormal situations (or corner cases) may be ignored at the beginning of the app development. Additionally, to add new functionality to apps, unstable libraries that provide access to new features may be included in the code, and these may present leaks and means to be hacked. 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 (Ritesh, 2019). The first is to use code scanning strategies and models that can detect and pinpoint common security issues. The second method is to carefully check the third-party

libraries for known issues and security vulnerabilities. While third-party libraries work well in most situations, they may break down as a result of unknown exceptions, providing a chance for someone to hack in. Therefore, understanding the code and vulnerabilities is critical before applying it in the app development process, no matter how great the features may be.

3.0 SYSTEM ARCHITECTURE DESIGN

To make the system work smoothly and efficiently, traffic management centers, traffic lights, signal controllers, the MUST-II device, and cell phones are indispensable. Traffic management centers supervise and arrange the operations of traffic lights. Traffic lights are controlled by their corresponding signal controllers, which can also communicate with non-motorized users' mobile phones through the connection provided by the MUST-II device. Figure 3 shows the overall working flow of the system.

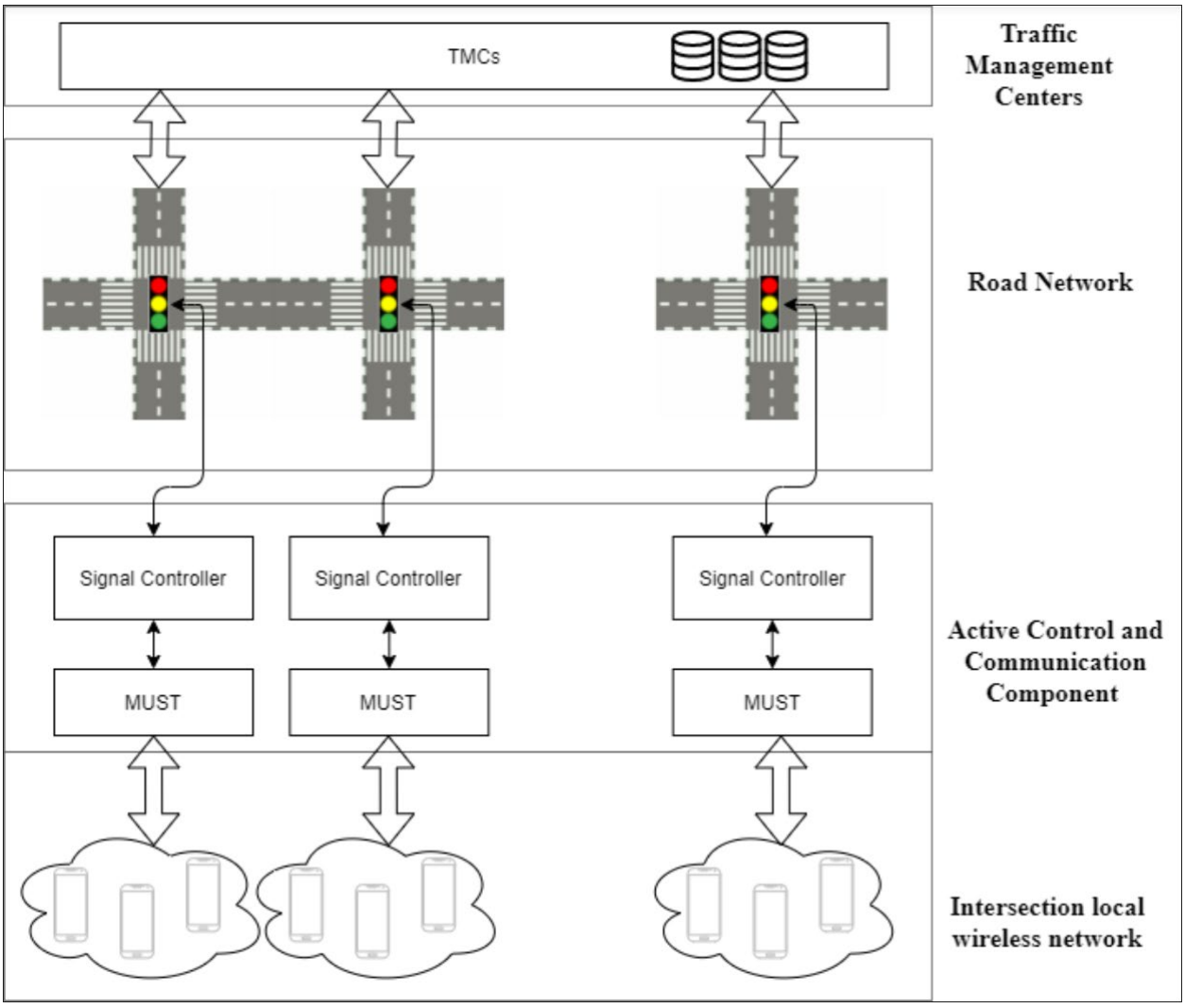

Figure 3: System architecture of the project

3.1 TRAFFIC MANAGEMENT CENTERS

A traffic management center (TMC) is controlled by crew members from the department of transportation, who keep their eyes on roadway traffic 24 hours a day, seven days a week to ensure that necessary operations are conducted, important information is disseminated, and traffic flows at optimal performance.

TMCs are the most important part of the roadway network, playing the role of a nerve center and ensuring the efficiency and safety of roadway traffic. TMCs use traffic cameras to monitor real-time traffic flow and to identify any existing or potential problems. Engineers and radio operators constantly focus on abnormities on the road. Roadway detectors and sensors send essential information to the TMC's database, and TMCs analyze the data to identify problems and solutions. When emergencies occur, TMCs organize law enforcement such as highway patrol police, fire departments, and medical personnel to respond. During emergencies such as traffic incidents, stranded drivers are helped, and damaged or totaled vehicles are removed from the highway to keep traffic flow at its maximum possible efficiency. When adjustable infrastructure such as reversible lanes and ramp meters are applicable, TMCs adjust the operation status of this infrastructure to help traffic flow more safely and faster while preventing or dissipating traffic congestion. When important information about constructions, incidents, and inclement weather needs to be disseminated, TMCs broadcast the information over highway advisory radios with corresponding travel time changes. Some information is also shown on electronic signs on roadways, as well as updated on the Internet. These types of important information are also made available to television and radio news agencies to let them broadcast the latest information of interest. Wherever emergencies or disasters happen, TMCs are the most important components in coordinating a response.

The TMC database needs constant new feedback from the detectors and sensors on the roadway network to keep it up to date and useful. Our innovative transportation project will provide TMC databases with new types of data and will introduce a new way of traffic management. The system and TMC will be mutually beneficial and will improve performance and efficiency together.

3.2 SYSTEM KEY COMPONENTS

The two most important components in the system are the signal controller and the Mobile Unit for Sensing Traffic Version II (MUST-II).

3.2.1 Signal Controller

The signal controller controls the operation of the traffic lights at an intersection. It records the operation history of the traffic lights, stores preloaded phases for different types of operating situations, and uses signal timing plans to change the working status of the traffic lights connected to the controller. Traditionally, the signal controller and lights form an isolated system and do not send information to or and receive it from other devices once the initial setup has been completed. However, this project intended that the signal controller would communicate with other devices to control the intersection operation.

3.2.2 MUST-II

The MUST-II is a modular computer that serves as a terminal to process multiple data from different hardware such as cameras, antennas, light sensors, and more. The MUST-II is a capable device that can be the communication bridge between users and transportation infrastructure, serving as the key to unlock the possibility that non-motorized users and transportation infrastructure can be interactive.

3.3 SYSTEM DESIGN LOGIC

The whole system is intended to serve non-motorized users. When they arrive at an intersection, users can use their smart phone to send a crossing request to the MUST-II device. The MUST-II communicates with the signal controller and asks it to adjust the signal timing plans to better serve the non-motorized users who sent the signal if possible.

The MUST-II device is connected to an antenna that is capable of sending and receiving information to receiving devices within the range of the intersection. The antenna divides the usage of the MUST-II device into two different categories, listening and broadcasting. The MUST-II device is connected to the signal controller with an ethernet cable and is constantly reading and interpreting the signal timing information from the controller and broadcasting to all non-motorized users within the coverage of the intersection via User Datagram Protocol (UDP) over the antenna.

When non-motorized active users send the encrypted crossing request, the antenna is listening and actively searching for such signals. After the antenna captures the signal, it send the signal to the MUST-II device, and the MUST-II starts processing the request. In a real-life situation, within a very short period of time, there could be multiple users sending multiple signals to the antenna and passing them to the MUST-II. In this situation, the MUST-II device should first collect all the requests received by the antenna. Then after collecting the signals received at a single moment, the MUST-II device starts sorting the signals. Because two things cannot happen at exactly the same moment, the MUST-II must sort which one came first and which one followed. When the sorting work has been completed, the MUST-II starts filtering the received information. Some signals may be redundant, some may be suspicious, and others may

be erroneous. All these unideal messages are filtered out and trashed, and only the correct and trustworthy signals are kept.

After the procedures above, the MUST-II analyzes the requests and uses algorithms to calculate the best phase to serve the non-motorized users. With the optimal phase selected, the MUST-II device phase-matches with the signal controller to make sure that the signal controller hears the plan and makes the right movement. The signal controller sends the new (or still old; sometimes changing the timing plan is not ideal) signal timing plan to the MUST-II device through the ethernet cable. After the MUST-II device has read and interpreted the specific signal timing plan, the signal timing plan is broadcast again with the antenna. Non-motorized active road users' phones are constantly listening for this type of information, and once the information has been received, the phones filter out redundant information from the received signal timing information and show the results to the non-motorized active road users. If users send the request again, the system goes through the whole process again.

4.0 HARDWARE SYSTEM OVERVIEW

For this project, two main hardware components were used: a signal controller and a MUST-II unit with various sensing peripherals and an antenna system.

4.1 SIGNAL CONTROLLER AND INTERFACE

Each intersection along the study corridor (SR 522) was equipped with an INTELIGHT 2070-LDX controller, as shown in Figure 4. As the name suggests, these controllers are based on the Type 2070 controller standard. They also have Internet capabilities via WiFi or hardwire (Ethernet). For this project, the STAR Lab was able to obtain one of the subject controllers through a generous donation from the Q-Free company (formerly INTELIGHT). Therefore, we were able to learn about the controller's usage, set up timing plans, and test its communication capabilities.

Figure 4: INTELIGHT 2070-LDX controller

4.2 MUST-II

The second main hardware component for this project was the MUST-II. The MUST-II is a sensor developed in-house by STAR Lab researchers based on the Raspberry Pi single-board Linux computer. The sensor has additional peripherals for sensing MAC addresses over both

Bluetooth and WiFi, as well as a camera and temperature sensor. Applications of the MUST-II to date have included volume trend estimation, travel time estimation, and road-surface detection. The MUST-II can also send data to a remote server via various communication protocols (i.e., Transmission Control Protocol (TCP), File Transfer Protocol (FTP), Secure Copy Protocol (SCP)) and can be remotely accessed/controlled via Secure Shell (SSH) Protocol. The Internet capability of the MUST-II is provided by a data-only SIM card.

In this project, the purpose of the MUST-II was to serve as a communication bridge between the signal controller and the mobile phone application (the latter of which is described in detail in the next section). By establishing a connection between the MUST-II and the signal controller, the MUST-II would be able to obtain real-time information about signal timing and detector status. This information could then be shared to mobile phone users via a mobile application (app). The MUST-II would also allow communication between mobile devices and the signal controller itself, which would be necessary for allowing active users to request service on pedestrian phases. As the communication range of the MUST-II is limited by the communication protocol (e.g., Bluetooth or WiFi), it was expected that multiple sensors might have to be installed at a given intersection, depending on its size. The MUST-II is compact, and all components could be enclosed in a water-proof case that could be mounted on a light pole or signal cabinet.

5.0 SOFTWARE SYSTEM OVERVIEW

5.1 USER APP FUNCTIONS

The software components for this project were three-fold. First and foremost, a mobile application was developed that would allow active road users to access signal timing information, request calls for service on pedestrian phases, and obtain a host of other information. The general requirements for the app were as follows:

1) The app was to be developed for Android devices.

   Here, the STAR Lab team used the appery.io development environment for the initial prototyping of the app. This environment allowed for both the design of the user interface controls within the app and the back-end code to implement core functionality.

2) The app should allow the following five key functionalities:
   a) Allow users to determine their location on a map.
      i) Users should be able to determine their location via an indicator on the map, like the blue circle in Google Maps.
      ii) When the map is zoomed out and users' locations are different than where they are currently viewing on the map, they should be able to click an icon to localize their location.
   b) Allow users to view timing information on pedestrian phases at a given intersection.

      Display information on the time remaining in a given pedestrian phase, as well as the time remaining until a given pedestrian phase begins.
   c) Allow users to request a walk indication on a pedestrian phase.

i) Users should be able to push a button in the app to request a walk indication at a given intersection, assuming they are within a specified distance of said intersection.

ii) Users should also be shown which intersections have the capability to request the walk indication (i.e., which intersections are equipped with INTELIGHT controllers).

d) Allow users to cancel their request for a walk indication on a pedestrian phase.

Users should be able to cancel their request (and only their request) for a walk indication by pushing a button in the app in case they make a mistake.

e) Allow users to perform routing and navigation via the app.

Users should be shown the shortest path between two locations they input into the app with step-by-step directions.

3) The app should also include basic background information such as a link to the STAR Lab website (www.uwstarlab.org).

5.2 CONTROLLER INFORMATION EXTRACTION

The other two software components necessary for use in this project were both developed by Q-Free. These systems were called MAXVIEW and MAXTIME. MAXVIEW allows management of signals in the field via a remote, map-based system that can be run and viewed in a web browser. The platform also allows for remotely changing signal timing, setting up timing schedules, and event monitoring and reporting, among many other tasks. In this project, the main use of MAXVIEW was to gather background information on the signal timing plans in use along SR 522, as well as to collect information on pedestrian detections and usage of various intersections along the corridor.

The MAXTIME software platform exists in two primary forms. The first is installed on the INTELIGHT 2070-LDX controllers as their primary operating system. Once this system has been installed on a given controller, via a USB drive or remotely via the Internet, signal timing plans can be established and modified via the controls on the front panel of the controller or via the MAXTIME PC app (the second main form of MAXTIME), as shown in Figure 5 and Figure 6. MAXTIME also has a REST API that allows accessing data in the MAXTIME software over Hypertext Transfer Protocol (HTTP). An example of data returned in Extensible Markup Language (XML) format from the API is shown in Figure 7 (here, the information shown is time remaining in each pedestrian phase). Through the use of this API, which allows data access for controllers made by INTELIGHT and, more broadly, controllers compliant with National Transportation Communication for ITS Protocol (NTCIP), detailed information on signal timing plans such as the time remaining in a given phase, detector status, etc., could be viewed in real time. This information could then be collected and displayed to users of the app to give them real-time information on signal timing for a given intersection.

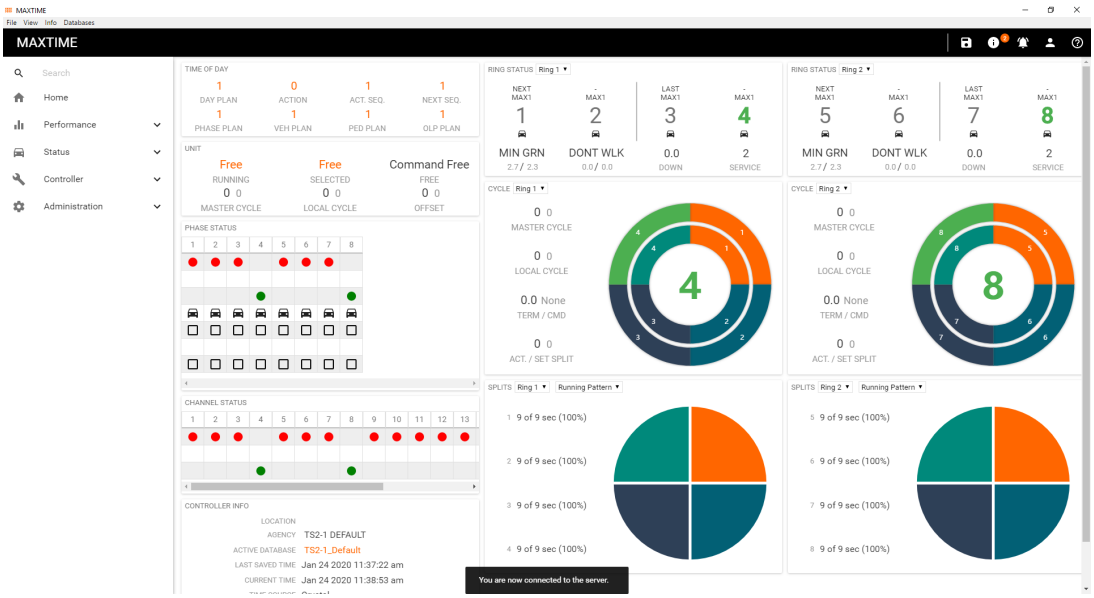

Figure 5: MAXTIME PC app main screen

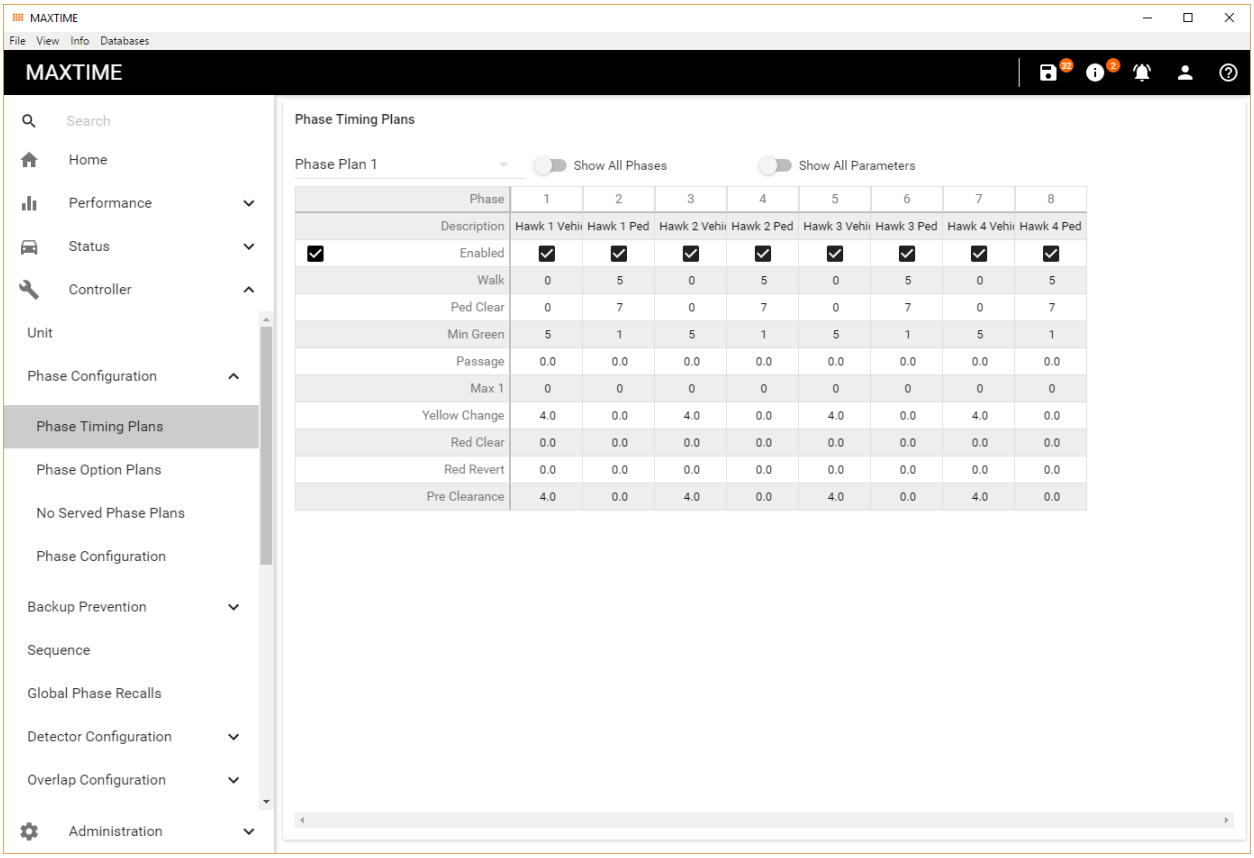

Figure 6: Signal timing plan setup interface in the MAXTIME PC app


```
▼<mibscalar name="PedDnTm" type="readonly" link="http://127.0.0.1/v1/mib/objs/PedDnTm?type=xml">
  ▼<index name="index1">
      <data index="1" value="0.8" counter="0"/>
      <data index="2" value="0.8" counter="0"/>
      <data index="3" value="0.0" counter="0"/>
      <data index="4" value="0.0" counter="0"/>
      <data index="5" value="0.0" counter="0"/>
      <data index="6" value="0.0" counter="0"/>
      <data index="7" value="0.0" counter="0"/>
      <data index="8" value="0.0" counter="0"/>
      <data index="9" value="0.0" counter="0"/>
      <data index="10" value="0.0" counter="0"/>
      <data index="11" value="0.0" counter="0"/>
      <data index="12" value="0.0" counter="0"/>
      <data index="13" value="0.0" counter="0"/>
      <data index="14" value="0.0" counter="0"/>
      <data index="15" value="0.0" counter="0"/>
      <data index="16" value="0.0" counter="0"/>
    </index>
  </mibscalar>
```


Figure 7: MAXTIME API response showing the time remaining in pedestrian phases

5.3 COMMUNICATIONS PROCESS

The communications process was the core task of the project, as it involved development of the systems needed for video-detection of pedestrians, as well as alerting drivers of pedestrian presence via a mobile app. The framework for this task was as follows.

The first goal to accomplish was the video-detection of pedestrians waiting to cross the intersection. Our system is called Accessible Crossing Platform for Active Road Users (ACPARU), which is a preliminary version of the VENUS system (Yang et al., 2022). The ACPARU sensor, which had already been developed, includes a camera and a variety of other sensing peripherals. In this project, we used a pole-mounted ACPARU sensor to surveil the intersection from above and developed video-processing algorithms to detect both pedestrians waiting to cross the intersection and pedestrians currently crossing the intersection in real time based on video footage collected by the MUST-II. Additionally, we investigated how the ACPARU could communicate with the traffic signal controller in order to do the following:

(1) alert it that pedestrians are waiting to cross the intersection, and it should then actuate the pedestrian detector for their signal phase/crossing direction and

(2) determine whether it is possible to extend the green signal for pedestrians lagging in the intersection as the crossing countdown time is diminishing.

In this project, the team developed a means of communication between the MUST and traffic signal controller via the UDP protocol, as shown in Figure 8. Therefore, the main goal involved developing pedestrian detection algorithms and determining how to convey this information to the controller.

The second part of the communication task focused on development of a mobile app to alert drivers of the presence of pedestrians in the intersection (via V2X communication) in an

effort to reduce conflicts between drivers turning through a crosswalk and crossing pedestrians. An initial version of a mobile app that could communicate with the MUST/signal controller had already been developed for this project. Here, the goal was to extend the usage/functionality of the app to receive pedestrian presence information from the MUST sensor and push this information to drivers using the app via a heads-up-display mode (like a mapping app) to minimize distraction. The overall framework of this communication process is shown in Figure 8.

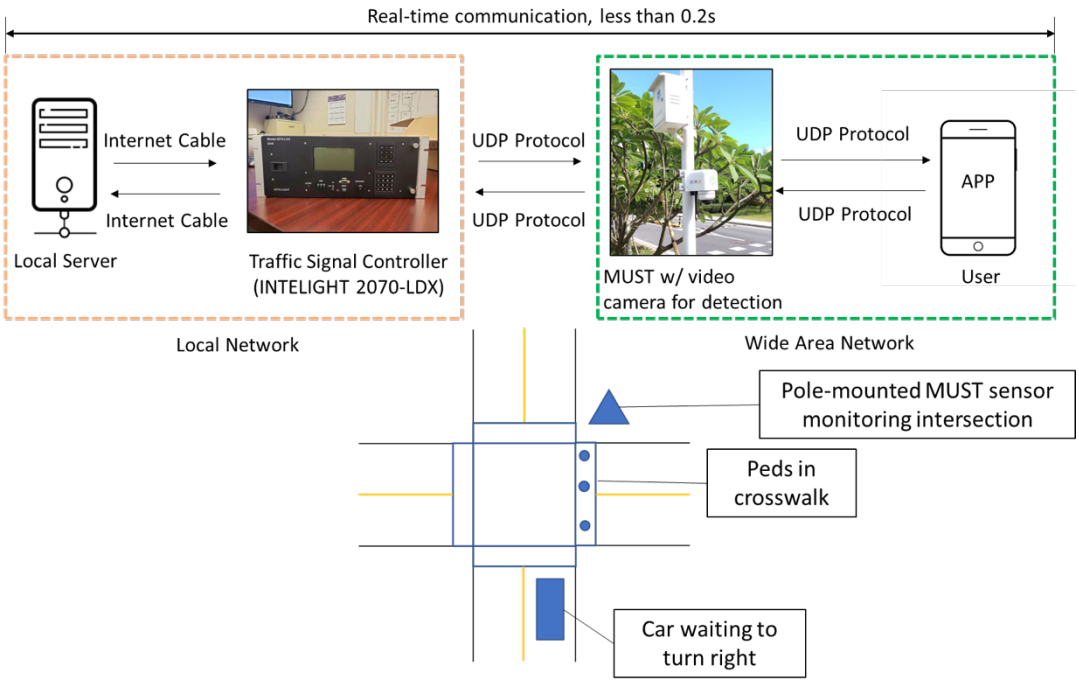

Figure 8: Framework of the communication process for the proposed ACPARU perception and intersection system.

6.0 USER APP DESIGN AND IMPLEMENTATION

6.1 SYSTEM DESIGN AND STRUCTURE SUMMARY

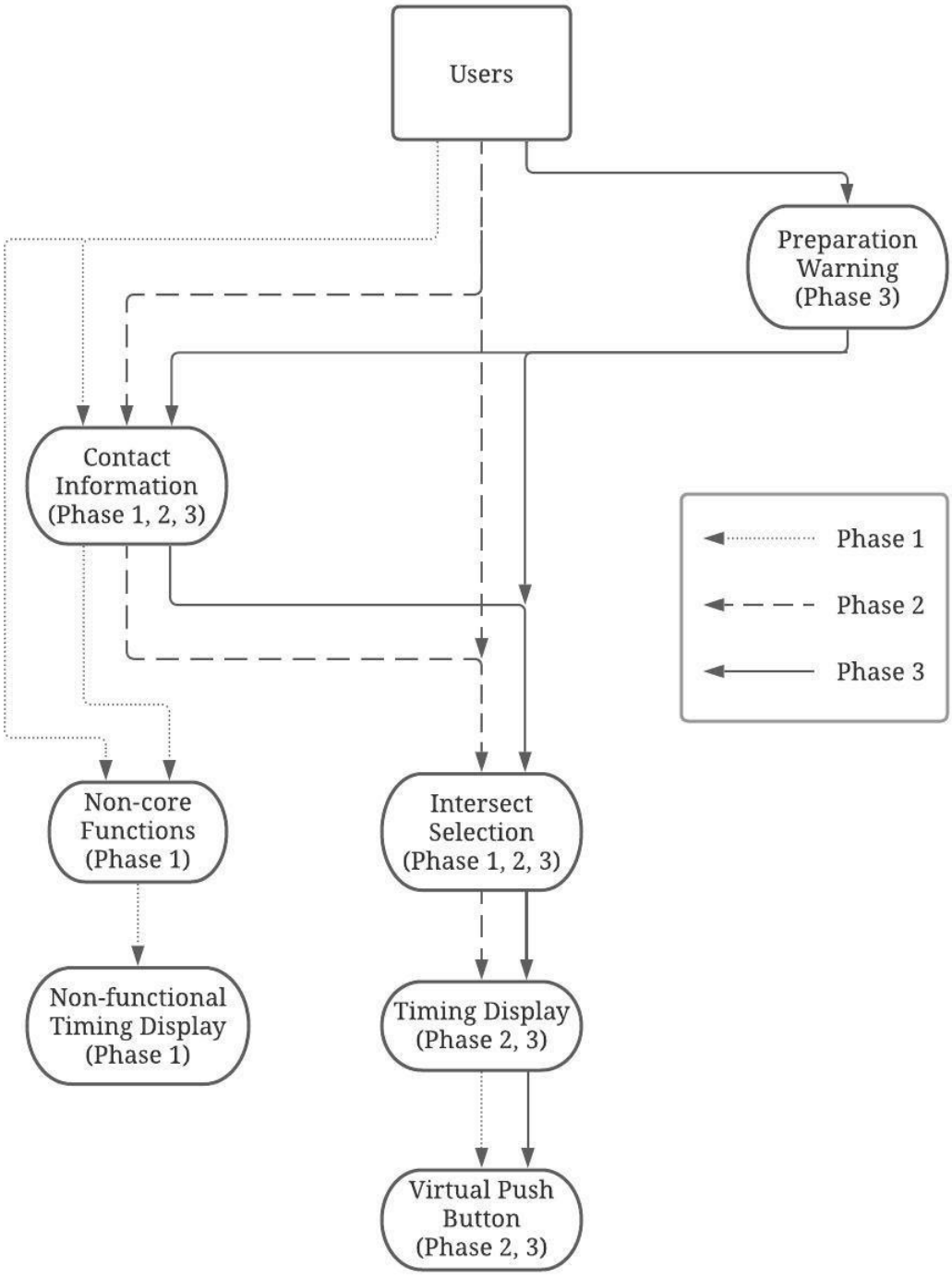

Figure 9: Mobile app design logic

Figure 9 shows the system design logic of the app. The app development was divided into the following three phases; in Figure 9 each is marked with different lines:

- Phase 1: Experimental app, with a feasible structure that could potentially represent the final app design; the core function was only a demo, not included.
- Phase 2: App with usable core function; the overall app was redesigned on the basis of the core function.
- Phase 3: Refined the user interface (UI) design to optimize users' core function experience.

After phase 3, the app would go through a series of tests to prove real-life performance and stability.

6.2 PHASE 1 DEVELOPMENT

The first step of the app development was establishing the basic idea of the functions of the desired app. The core function of the app was secure communication between transportation infrastructure and a cell phone. The whole app had to be developed to serve the core function, and minor functions had to be added to better work with the core function.

Because the IOS platform has way too many regulations, and the development process would have been much more complex as a result of the exclusiveness of the development environment and tools, we decided that Android was a much better platform than IOS. The programming language used in the app was Kotlin, which is a language based on Java and is currently promoted by Google.

During this phase, we did not already have a physical test platform. Therefore, all the development and testing work was based on simulation software on a Windows operating system PC, rather than on a physical mobile phone.

In the first version we developed an experimental UI layout, and the app included a GPS positioning function (Know Your Location), a path directing function (Set Your Path), and a non-functional virtual push button function (Walk Request). After users clicked the Know Your Location button and clicked the Track button, the app showed the users' latitude and longitude and position on the map based on Google Map Service. In the Set Your Path function, it also showed users their location while also providing a simple navigation service that allowed users to set an origin and destination using natural language. It also had a Show Traffic function to allow users to view traffic status. The Walk Request button would send a cross-road request to the transportation infrastructure and lead the user to a page showing the current wait time. However, in this version, this core function was not working because the Intelight 2070-LDX controller had not yet been configured at this phase of the project. It still needed to make connections between some potential hardware that could deliver the information between the cell phone and the controller, and in this phase, we used a QR code to deliver fake timing information.

This version was just a very basic demo of what the app would look like, and it established a basic logic for the app: Home screen – Let users view their location information – Let users make a request. Although later most of the app was deleted or modified, this first version established the overall structure of the app design, and it worked as the skeleton for the whole app development process. However, the core function of the app was still not working in this version. As a substitute, we used alternative technologies such as scanning a bar code and QR code to compensate for the absence of direct communication between a cell phone and the controller. In this phase, the app was still not sufficient to fulfill the basic requirement of the project. Figures 10 and 11 show the user interfaces of the app.

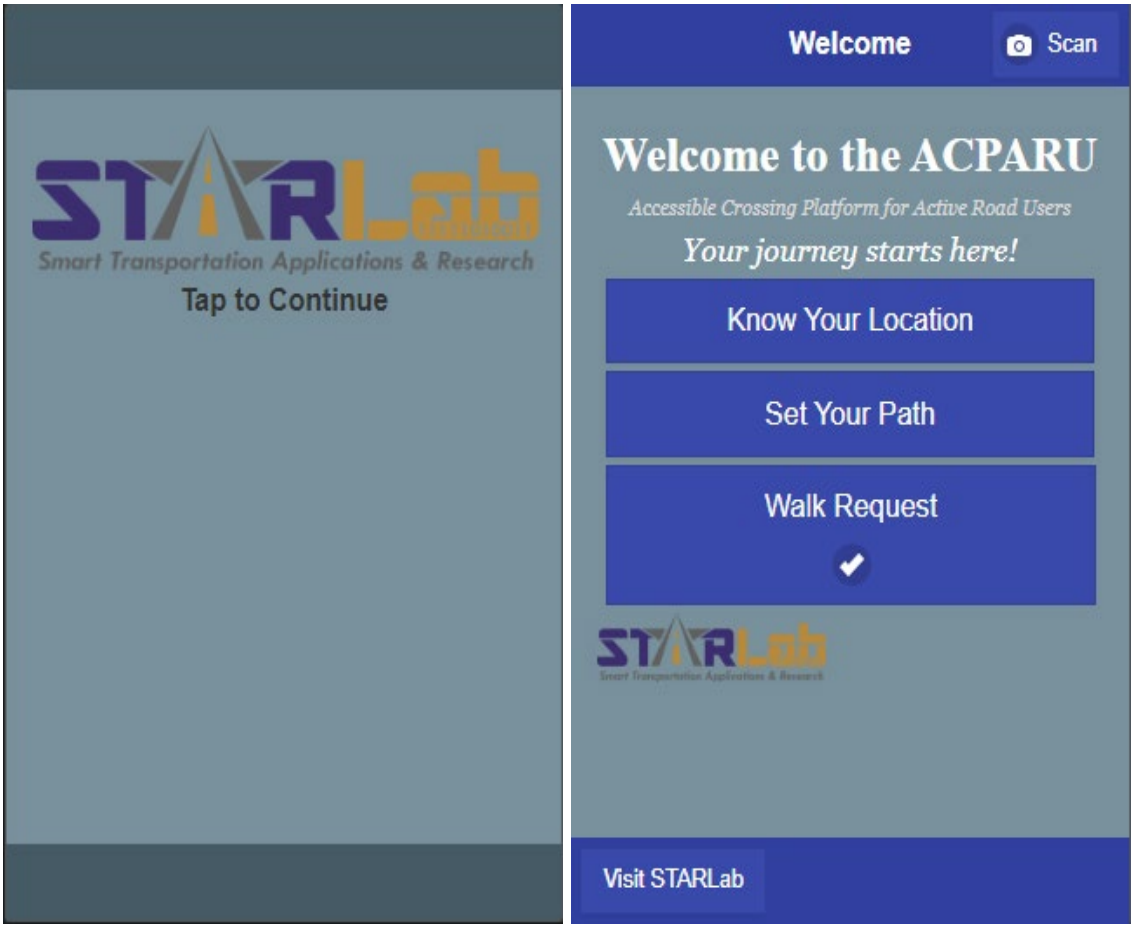

Figure 10: Welcome pages of the mobile app phase 1

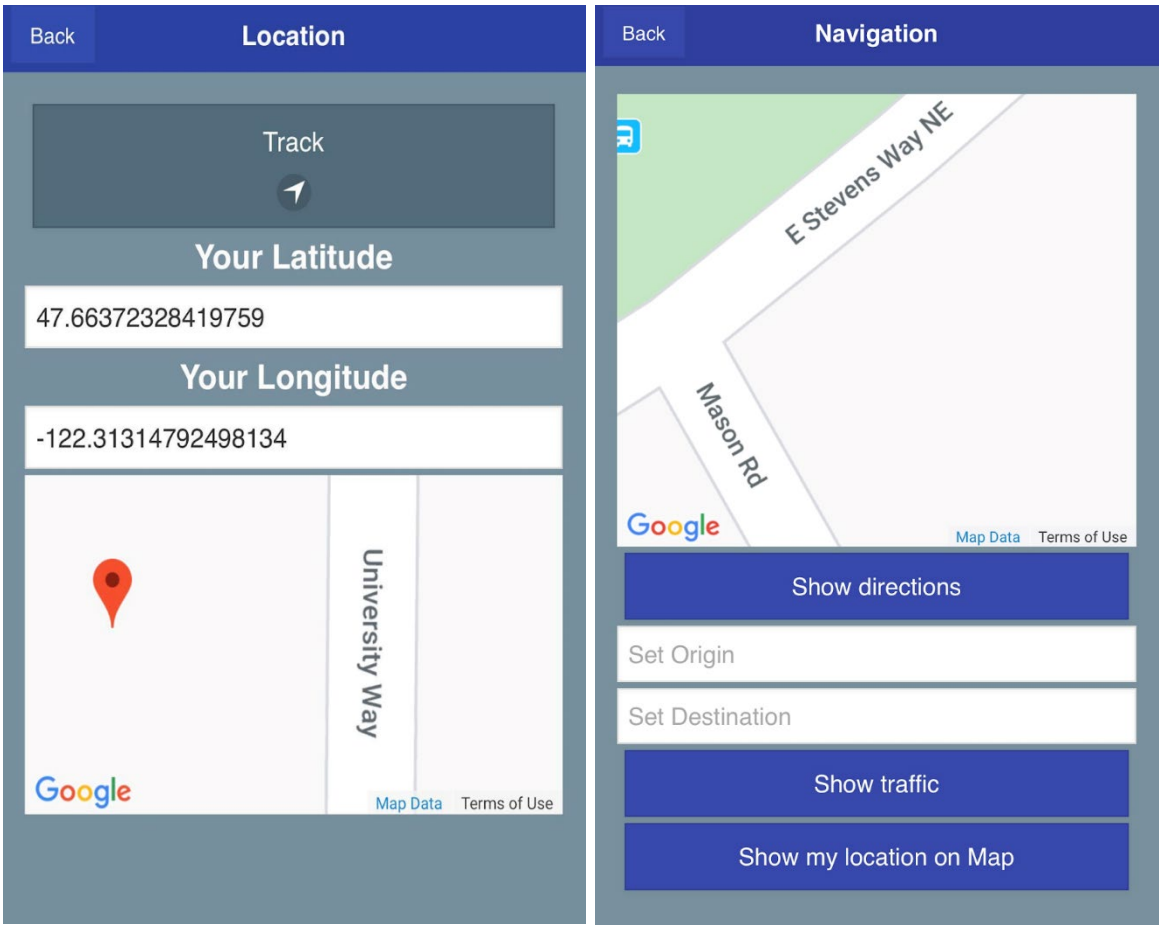

Figure 11: Functional pages of the mobile app phase 1

6.3 PHASE 2 DEVELOPMENT

After the first phase of the app design, our team members worked on the controller's communication function. After figuring out how to establish physical communication between the MUST-II device and the controller, the team refined the communication process:

1) Users select which intersection they are at and the crossing direction.

   After a series of testing, it turned out that GPS was not a reliable option for determining users' locations because GPS tracking accuracy greatly depends on how strong the GPS signal is, and it can frequently cause error. Therefore, our team decided to use a simpler yet more reliable option to check users' location (where in

the intersection a user was). We let users determine the location. Users were provided with two drop-down lists, one to let them choose the intersection, the other to let them choose which direction to cross.

2) Users send a request to the MUST device.

   After determining the intersection and crossing direction, users would click a button that would first send the crossing request to the MUST device, then lead them to the next page, which would include a waiting time display for timing information. This was the main part of the app because it was part of the core function.

3) The MUST-II receives the user's choice.

   This part would be processed inside the MUST device, and the communication was based on a specific data format decided by the team.

4) The MUST-II device communicates with the controller.

   This part required the MUST device to send a virtual push to the controller, and the controller would send back the new timing information.

5) The MUST-II sends back the required information.

   The MUST-II device would send the information from the controller to the app on the mobile phone.

6) Users receive the information.

Because the MUST device would need to deal with multiple mobile phones at the same time, to save processing power we decided to let the MUST device directly deliver only the raw timing information instead of letting it pre-process the raw information. Because raw data have a specific format, after receiving the timing information, the mobile app would fetch and process

the useful part of the information following the message pattern, calculate the timing information and display it on the timing screen.

The user interface of the app was also redesigned as the new communication process was established. The original blue-gray theme was abandoned for a more modern white background, minimalist design. A welcome page was added to the app that included a button to access the core function and the contact information of the developers. Because this version focused more on testing, most of the functions in the first version of the app that were not related to the pedestrian call were removed to reduce the complexity of the test form. The only functions we had in the test version were as follows (see figures 12 through 15):

- Welcome page.
- Contact information.
- Selection of the intersection with the Google Map location moving correspondingly.
- Selection of the crossing direction.
- Wait time display.

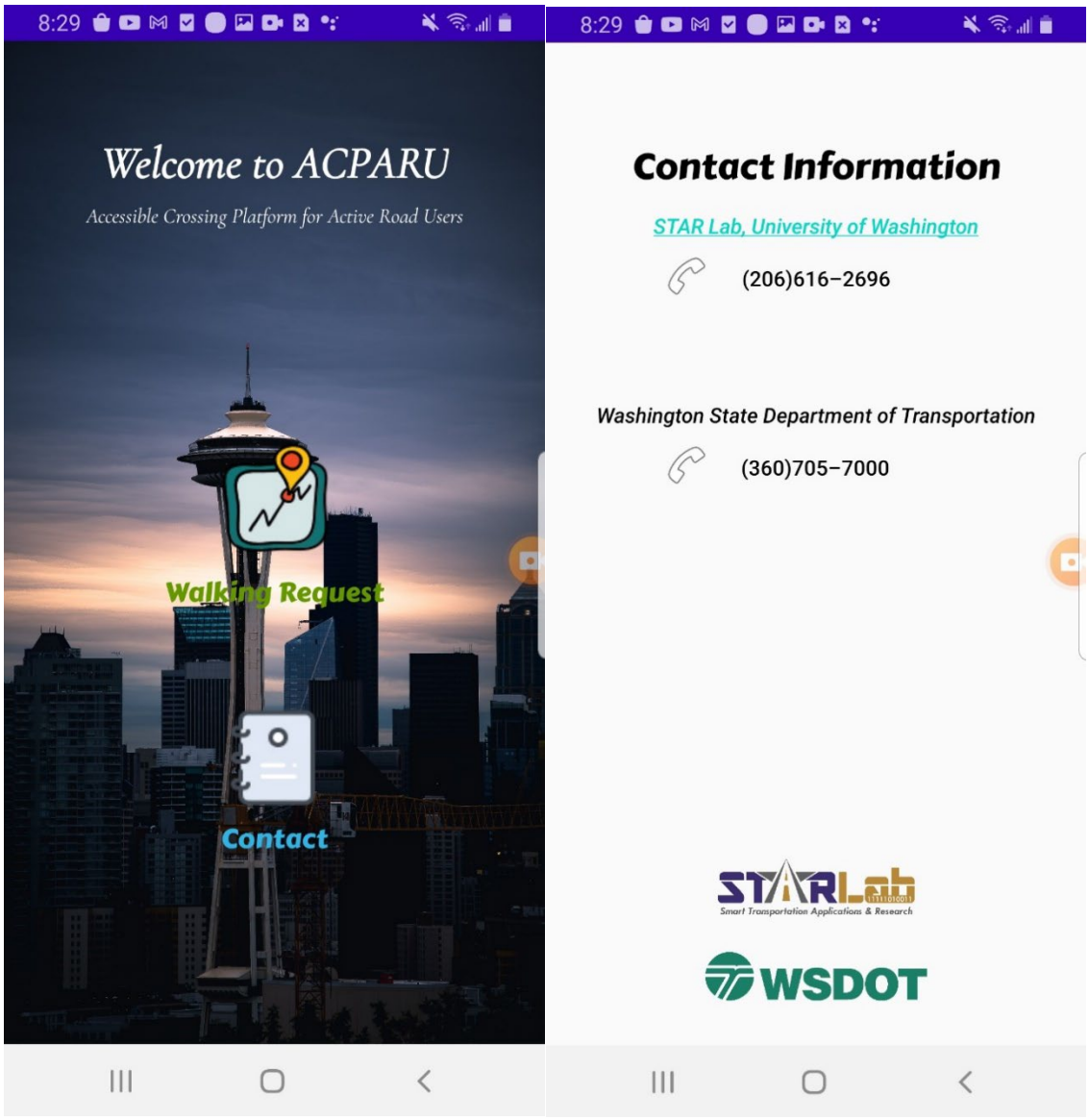

Figure 12: Welcome and contact information pages of the mobile app phase 2

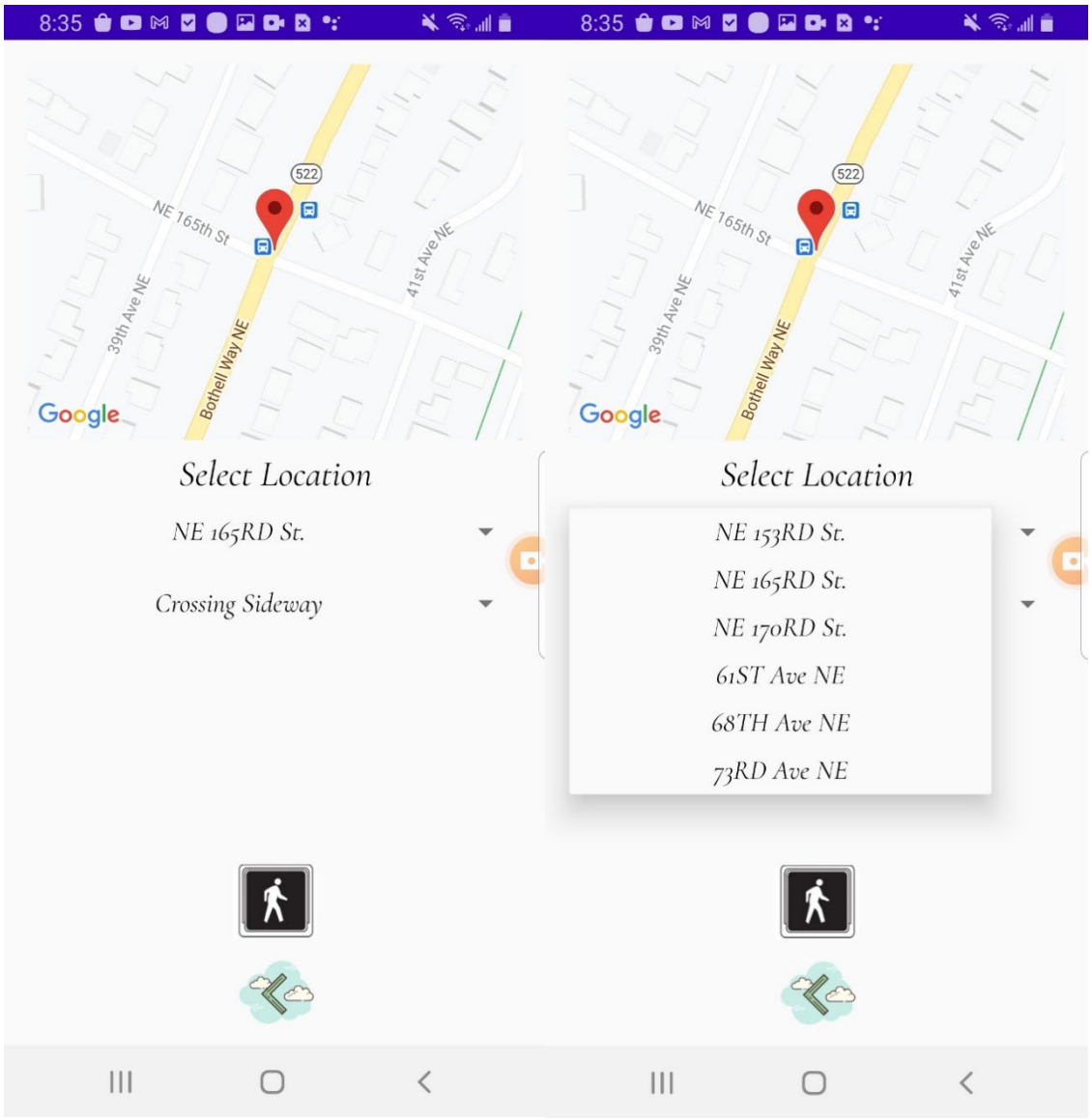

Figure 13: Road crossing selection and waiting pages of the mobile app phase 2

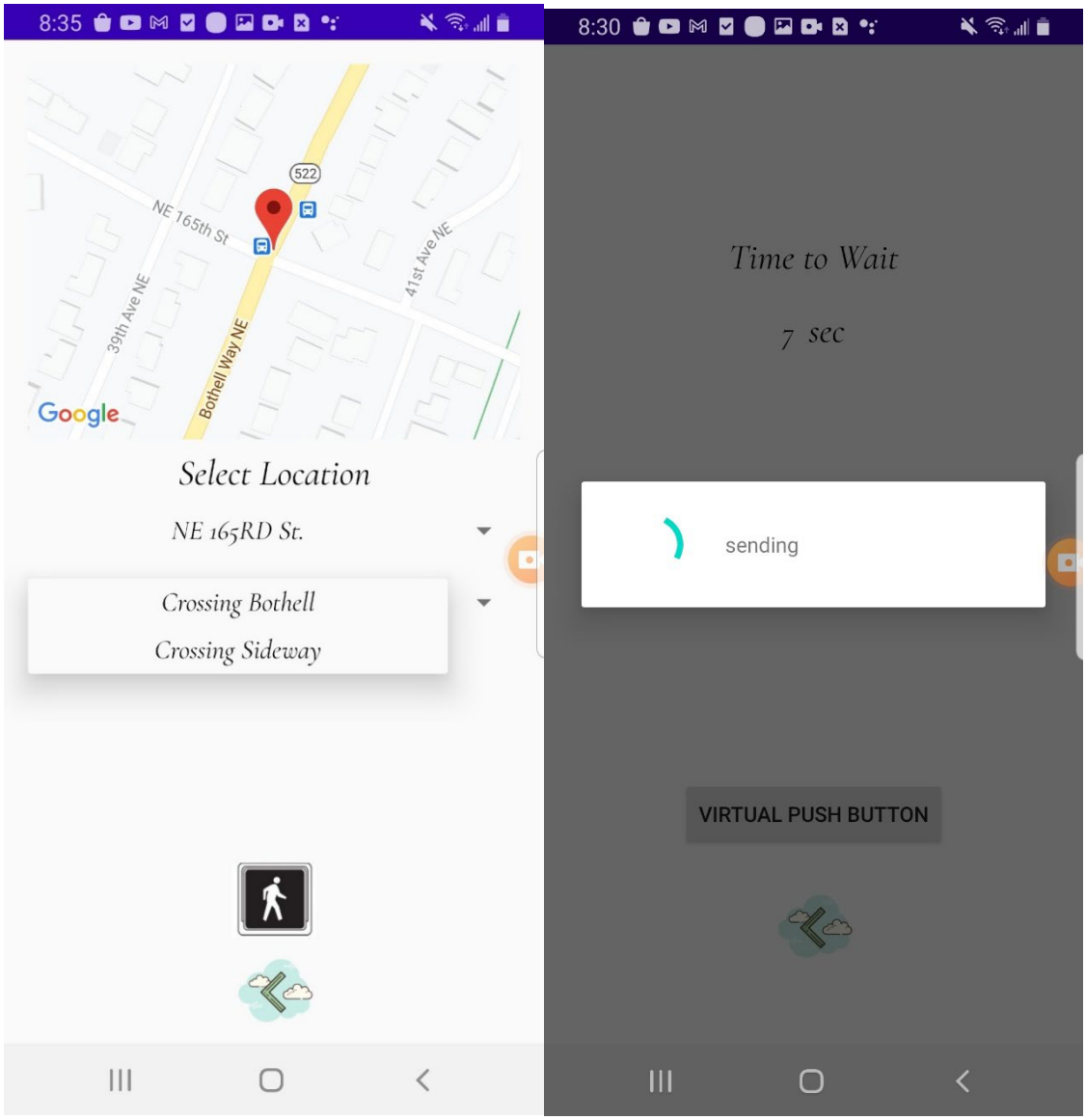

Figure 14: Road crossing selection and waiting pages of the mobile app phase 2

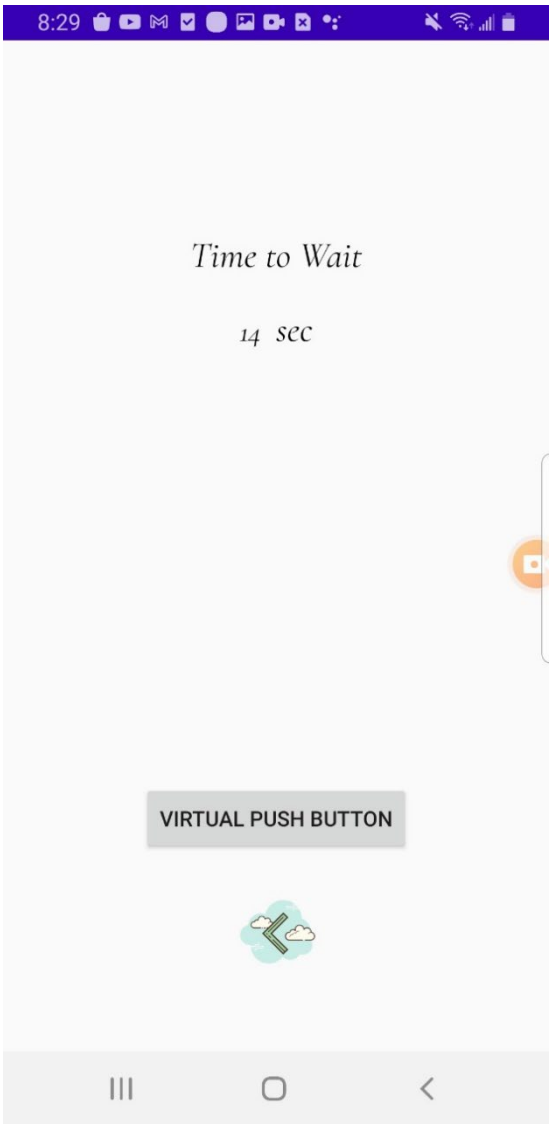

Figure 15: Waiting time display pages of the mobile app phase 2

For communication between the cell phone and MUST device, we first chose HTTP for sending and receiving information. Once the MUST device and mobile phone had been connected to the same network, the MUST device could use the HTTP protocol to send and receive the required information to and from a mobile device. However, although using the HTTP protocol was feasible for communication, it was not stable and secure enough for the

stability and security standard of this project; therefore, it was only used as a protocol during the technology verification phase.

During verification, we set up a virtual working environment that involved only one MUST device and the test mobile phone. Because of the COVID-19 outbreak, it was not safe to hold the experiment in the laboratory, so instead, we set up the experiment in a team member's home, and all other members provided support remotely. It turned out that the HTTP protocol was able to acceptably send and receive data to and from the MUST device. However, test results showed that HTTP protocol had a significant latency issue, and the team never forgot that HTTP is not a very secure protocol. Therefore, a replacement for HTTP protocol was needed to improve latency and enhance cybersecurity.

The new protocol we chose was UDP. In comparison to HTTP, UDP has the following benefits:

1) The UDP does not have retransmission delays, which means it is more suitable for time-sensitive applications such as this project.
2) The UDP has smaller data packets, which gives it a better data transfer speed.
3) The UDP does not need end-to-end communication before sending messages, making it good for information broadcasting while also maintaining good encryption standards.

Because our team was the among the first to use the Kotlin language to develop UDP communications between an Android phone and controller, there were not many helpful cases for the team to learn from. And although Kotlin is based on the Java language, its vocabulary, grammar, and even logic can sometimes be very different from those of Java. These difficulties

took the team a fair amount of time to overcome. Eventually, we figured out how to correctly use the mobile phone's central processing unit (CPU) threads and how to encode the information.

The testing app that used the UDP looked the same as the previous version that used HTTP, but the codes for the core function were completely modified, and the new version app could be considered a completely new app with the same appearance as the old one. This app would work as a basic platform for all later app modifications.

This app version underwent a significant evolution from the first version. This version abandoned the functions in the first version that were not related to the core function. The most important thing was that it proved that both HTTP and UDP could be used as data transferring media. However, the communication latency in this version was still significant, and the UI design of the app was very primitive and only served the basic requirements of the app design. Many details still remained to be improved or added.

6.4 PHASE 3 DEVELOPMENT

Although phase 2 achieved most of the goals specified for the project, there were still details that needed to be addressed.

One problem was communication latency. The nature of UDP does not allow zero latency, but it needed to be shortened to reduce the time difference between the display on a user's mobile phone and the true real-time timing on the controller. In this phase, the data receiving algorithm was improved. The latency was compensated for by adding time, which was fine-tuned on the basis of the real-life measured latency. In the current phase, latency was controlled to a period of 0.5 to 1 second, and this latency would be safe for users and would not cause the app to display an unrealistic time.

Another aspect that needed to be improved was the orientation of the selection menu. The intersection and crossing direction selection part was changed to horizontal rather than vertical. This would prevent one of the drop-down lists from being hidden when users were making a selection on another drop-down list.

Finally, we refined the UI design and consistency. As Washington state is the Evergreen State, and the WSDOT logo is also green, we used green as the theme color. We also regulated all the fonts in the app to ensure both consistency and clarity.

This phase made the app functions usable to the public while it also refined the overall appearance of the app to make it user friendly. Although new features could still be added in the future, this current version of the app already fulfills the ideal project requirements (see figures 16 through 19).

Another important feature that is worth noting is the voice assistance for vulnerable users. For the users who cannot see the screen clearly, we offered a mode that reads out the options for them. In this mode, the workflow is simple: users are asked questions to confirm the choices they make, and to confirm the choice, users tap the screen twice to express “yes” or tap the screen once to express “no.” After entering the timing information screen, the countdown number is played every 5 seconds.

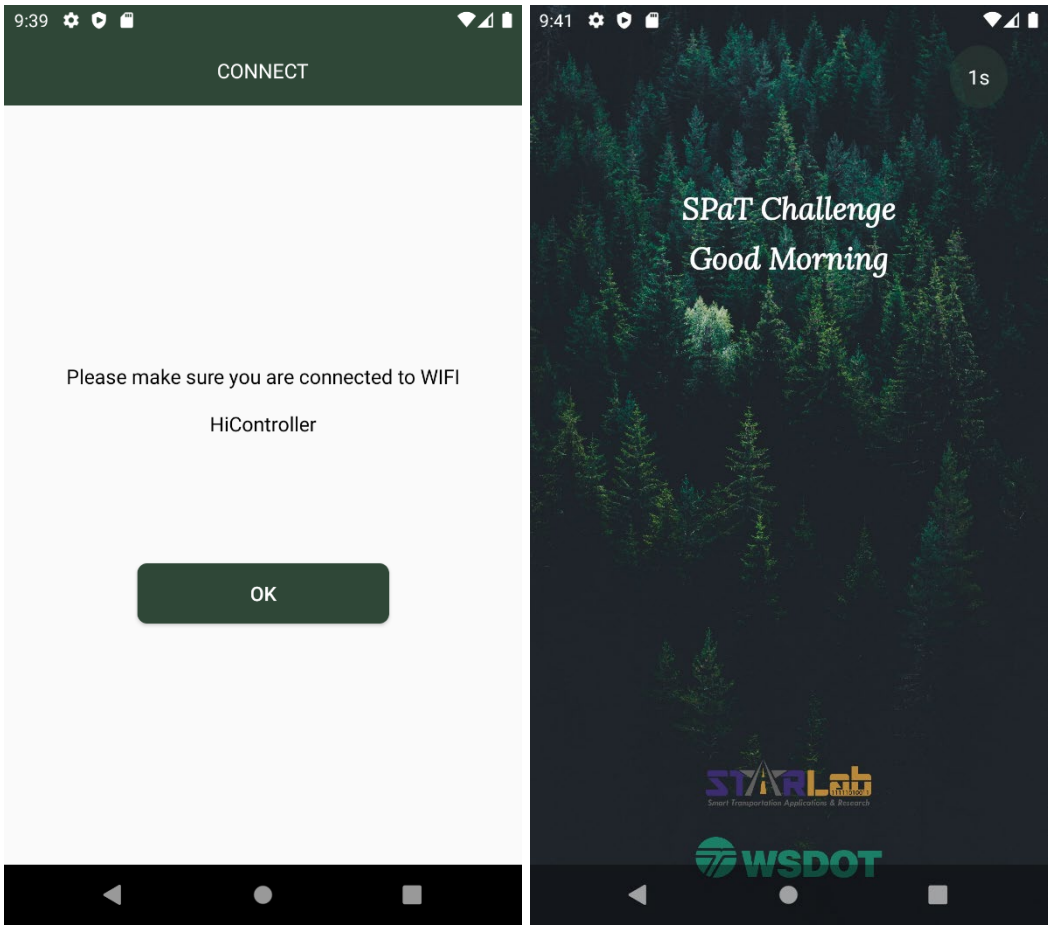

Figure 16: Initialization pages of the mobile app phase 3

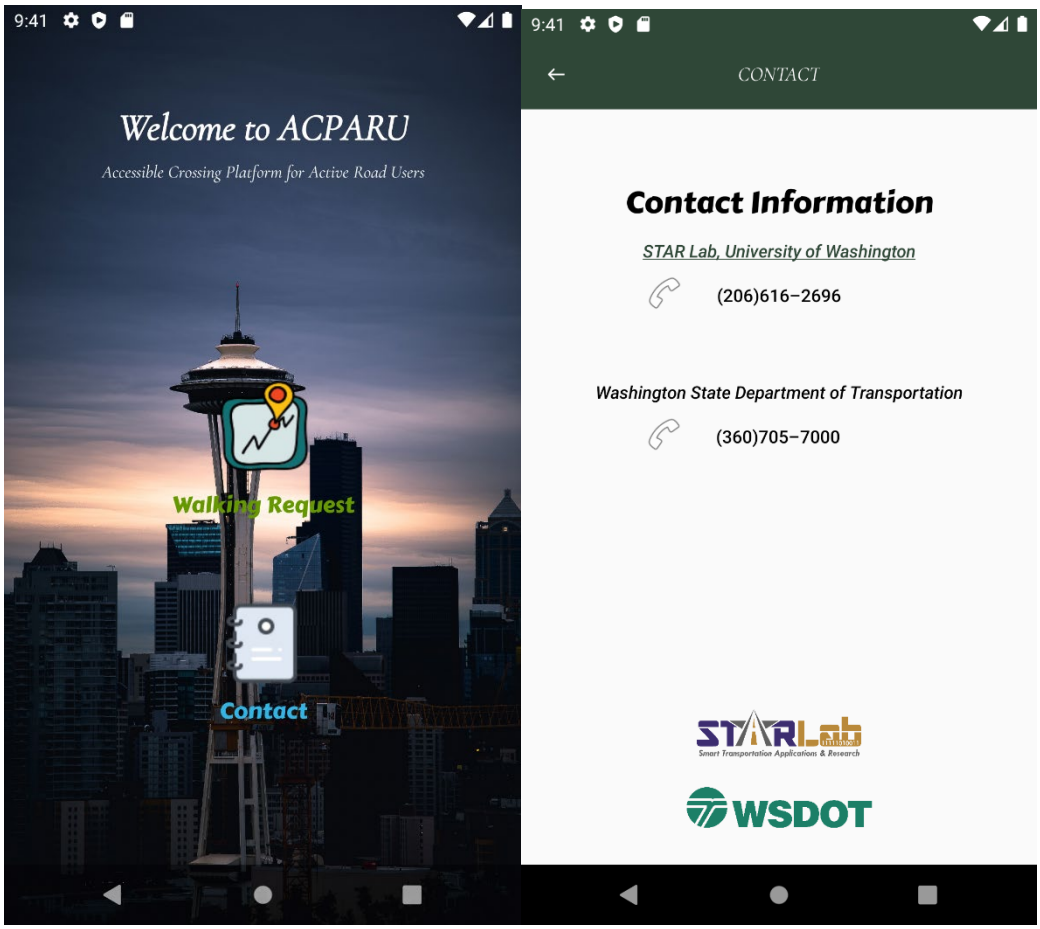

Figure 17: Welcome and contact information pages of the mobile app phase 3

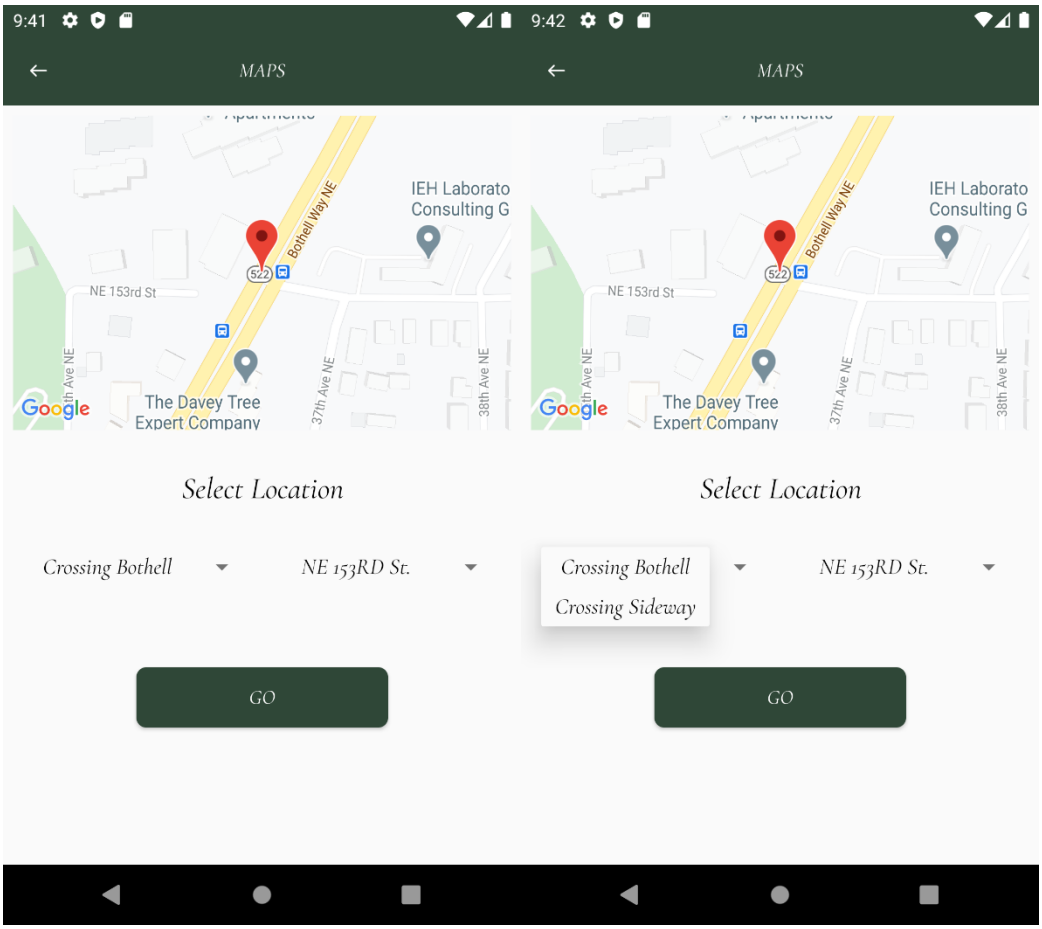

Figure 18: Road crossing selection pages of the mobile app phase 3

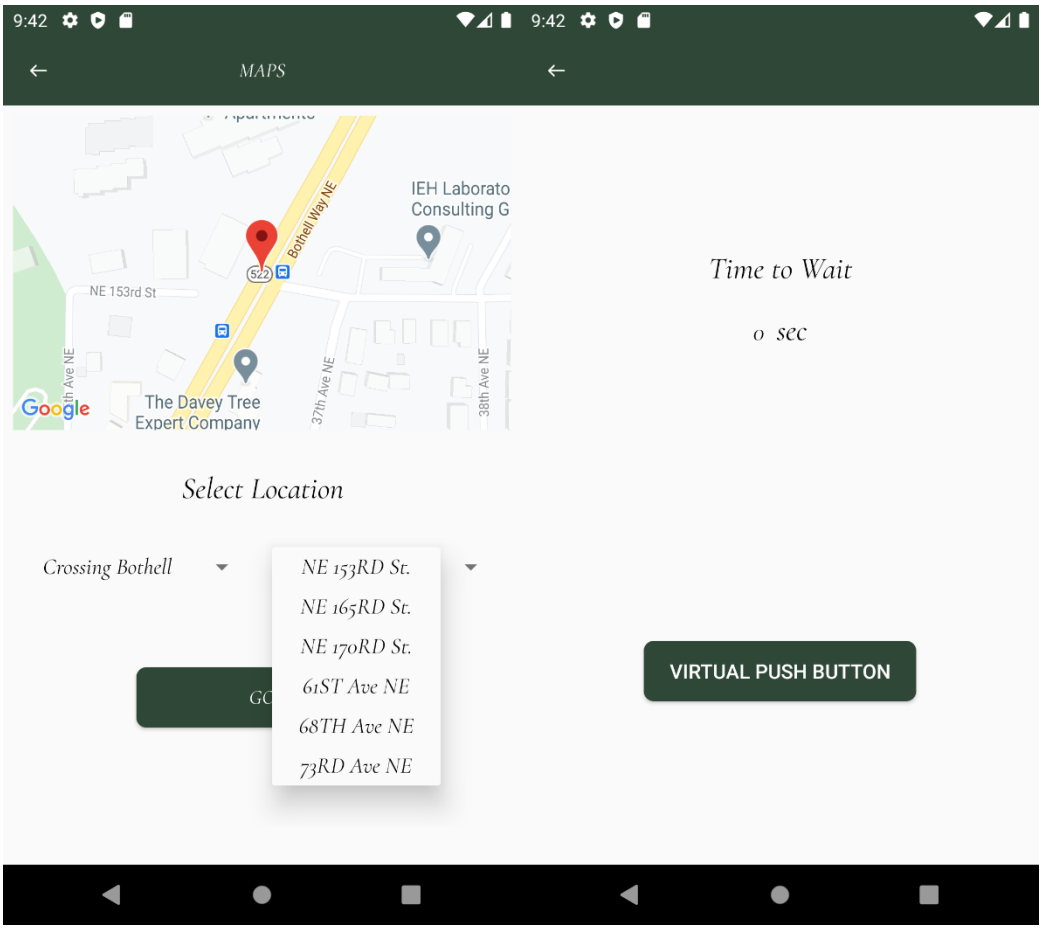

Figure 19: Road crossing selection and waiting time display pages of the mobile app phase 3

7.0 SIMULATION EXPERIMENT

7.1 HARDWARE PREPARATION

The simulation experiment was conducted at the University of Washington's STAR Lab and in close proximity to Civil Engineering's More Hall. Because of the pandemic situation, the simulation experiment was operated by just two lab members. Essential hardware included the following:

- Two mobile phones
- Intelight 2070-LDX controller
- MUST-II
- Windows PC.

The mobile phones for the simulation experiment were smart phones advanced enough to run the latest version of the Android operating system and were equipped with high end mobile CPU and graphics processing unit (GPU) to avoid a performance bottleneck in rare situations. The mobile phone had already been installed with our app in Phase 3, which had already been tested during the development phases 2 and 3. The mobile phone was fully charged and connected to a phone charger, with a Hicontroller Wi-Fi network connected.

The Intelight 2070-LDX controller was pre-programmed to simulate a real-world working environment. The STAR Lab had not only the controller but also a full signal cabinet and demonstration board with red/yellow/green indications for each of the eight movements defined by the National Electrical Manufacturers Association (NEMA), as well as pedestrian indications for each direction of crossing. The controller was connected to the hardware needed to work properly under various conditions, including extra-long-range communications. It was also connected to the power supply and the PC that was involved in the simulation experiment.

The MUST-II device was used as the communication bridge between the mobile app (accessed via a mobile device) and the signal controller. The MUST-II would have Internet access provided by a hardwired Ethernet cable and/or wirelessly via a SIM card and supporting data plan.

The Windows PC was installed with the necessary software to observe and make changes to the operations on the controller setups and hardware setups. It was needed to run the MAXTIME app to verify information provided by the controller against that displayed in the mobile app, as well as for potential adjustment of timing plans and simulation of pedestrian detection. (A call to a pedestrian phase, or any phase for that matter, could be made via the app's user interface.) The PC was connected to the Internet to prepare for any likely errors or emergencies, rather than connected to local network as the mobile phone was. The PC served as surveillance of the overall lab simulation experiment; if anything did not work as expected, the PC would serve as an emergency backup.

7.2 EXPERIMENT

Before testing the following cases, the team ensured that the controller was running a timing plan that included pedestrian crossing phases and was supported by pedestrian detection (virtual via MAXTIME app or otherwise). The team verified the following use cases:

1) Allow users to determine a location on the map.
    a) Verify that when users open the app, the location shown on the map is the location corresponding to the intersection selected.
    b) On the screen showing the map, switch the intersection on the map, and verify that the map switches to the corresponding location.
2) Allow users to view timing information on the pedestrian phases at a given intersection.

a) Select a SPaT-enabled intersection (there was only one in the lab) and verify that for pedestrian phases with demand that is currently being served, time remaining in the walk phase is shown in the app, and that such timing information updates at the specified interval.
b) Compare/validate the timing information in the app in real time against that shown in the MAXTIME app running on the PC.

3) Allow users to request a walk indication on a pedestrian phase.
   a) Verify that if at least one user is within the acceptable usage range of the current intersection (exact threshold to be determined, but the goal is to ensure only users "near" an intersection) then the user is allowed to place a call for service at a given crosswalk/phase and that the phase is served.
   b) Compare/validate information on the detection status in the app in real time against that shown in the MAXTIME app running on the PC.
   c) Verify that if the user is NOT within the acceptable usage range of the current intersection (exact threshold to be determined, but the goal is to ensure only users "near" an intersection) then the user is NOT allowed to place a call for service at a given crosswalk/phase and that the phase is NOT served.
   d) Compare/validate information on the detection status in the app in real time against that shown in the MAXTIME app running on the PC.

8.0 FIELD TESTING

8.1 SYSTEM HARDWARE COMPONENTS

There were three major components in the ACPARU system: (1) the traffic operations component (controllers and TMC server), (2) the ACPARU roadside system (ACPARU smart edge node and on-board camera), and (3) the non-motorized users app (shown in Figure 20). For the traffic controller, the team chose to use the 2070 series (2070LDX) controller made by Q-Free Inc. The reason for the team to choose this specific model to perform the test was that the 2070LDX not only could meet the standards of the Advanced Transportation Controller (ATC), California Department of Transportation (CalTrans), and NTCIP but could also provide an open hardware architecture to allow the client to fully explore more functions and utilize the hardware's potential. The ACPARU roadside system is capable of adapting many other models of signal controller with other well-established architectures, not limited to the 2070LDX model. The Nvidia Jetson AGX Xavier uses an embedded edge platform for real-time sensing over streaming pixels for the smart edge nodes. The Jetson AGX Xavier has an 8-core ARM CPU and a 512-core Volta GPU (Yang et al., 2022). The ACPARU roadside system consumes only part of the Xavier resource to maximize system efficiency, and it does not interfere with Xavier computing power in one cycle. Collie (GL-X300B), made by GL.iNet,. is integrated with the Jeston Xavier AGX and facilitates data transmission for communication functions, and the Collie gateway is based on OpenWrt open-source embedded operating systems, which is compatible with 2.4-GHz WiFi and has full-band 4G communications ability (Yang et al., 2022). The system is agnostic of the brand and type of matching onboard camera. The app is designed to run on mobile phones with Android 8.0 or a newer operating system version.

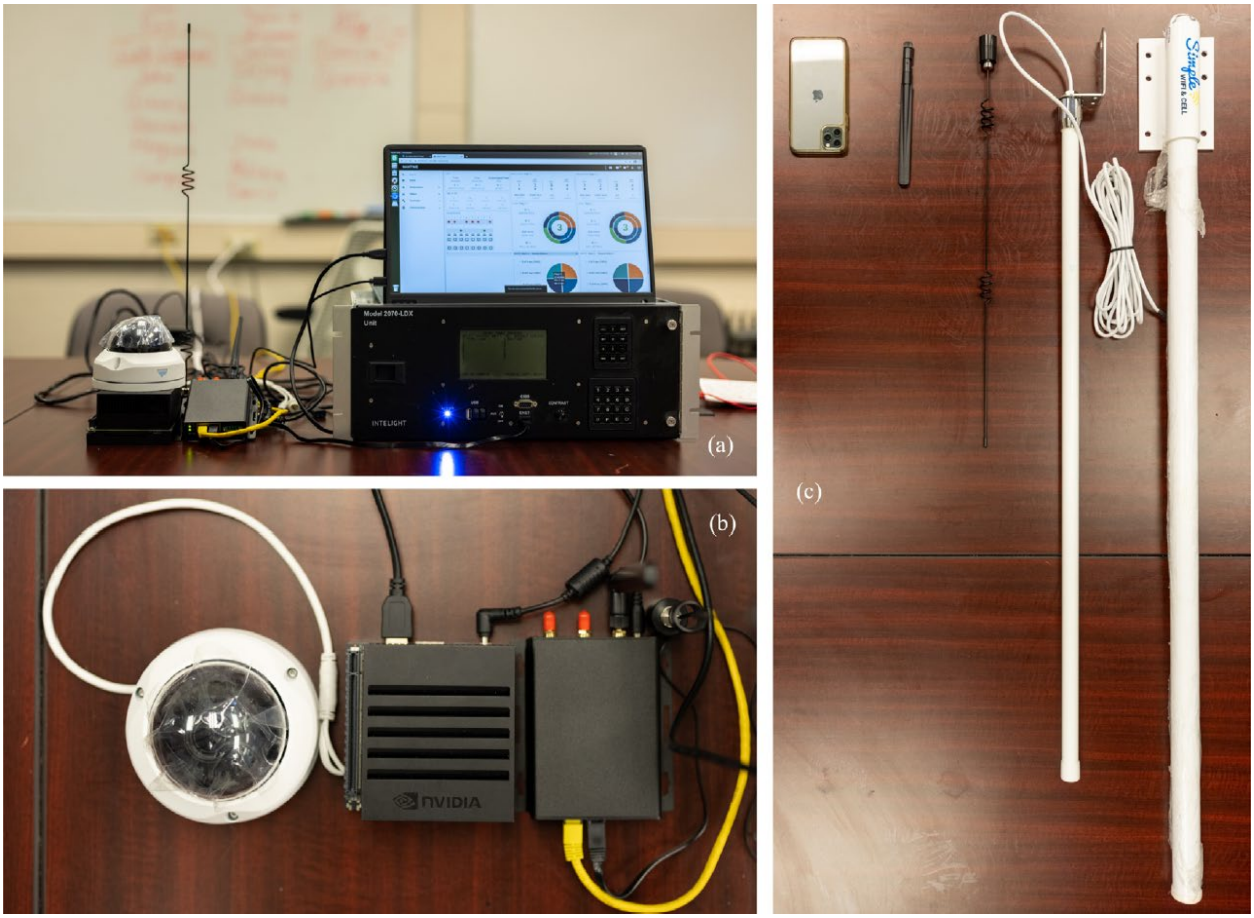

Figure 20: The hardware controllers, ACPARU smart node, and attached external antennas. (a) Overview of the ACPARU smart node system and controllers. The ACPARU-generated signals can be directly visualized by the controller and visualized on the screen. (b) The ACPARU smart node's three key component (streaming camera, Nvidia Jetson AGX Xavier and the connected gateway, from left to right). (c) The various external antennas to cover the range from 50 m to 150 m for information interaction. (Yang et al., 2022)

8.2 SENSING SYSTEM EVALUATION

8.2.1 Mobility Aids Dataset

The Mobility Aids dataset (Kollmitz et al., 2019) was created by faculty of engineering at the University of Freiburg, Germany, and the data were collected from a hospital from Frankfurt. The data contained more than 17,000 annotated red green blue-depth (RGB-D) images, which were categorized into five different types based on the level of mobility aids a person would need:

1. Pedestrian

2. People in wheelchairs
3. People in wheelchairs (with people pushing)
4. People with crutches
5. People using walking frames.

This dataset with five categories helped the team to train the ACPARU system on user classification and user localization.

8.2.2 ACPARU Dataset

To fully evaluate the ACPARU smart node, supplementary data were used. These were gathered through video footage from six intersections situated across three distinct U.S. states, each featuring different designs, camera angles, and standard crossing paths. These recordings were compiled into the ACPARU dataset. The entire span of video sequences amounted to 19.95 hours, with every camera angle covering a minimum of two usual crossing directions. The default, as well as waiting and crossing zones for each camera view, are illustrated in Figure 21. Out of the 35,879 captured images, 4,560 of them were made and categorized into six distinct classes of non-motorized users. These included pedestrians, people in wheelchairs, people pushing wheelchairs, users of crutches, people with walking frames, and bikers. For the sensor detection analysis, 908 out of the 4,560 images were selected to test the detection function, while the remaining images were used for model training and verification. In terms of pose direction estimation, the original video sequence was processed on an ACPARU edge node fitted with the fully trained detector. The chosen testing set of 908 images, containing 1,076 objects from six cameras, was further utilized to assess the accuracy of pose direction and mobility status estimations. More comprehensive data on the quantity of objects and the evaluation outcome are in the subsequent section.

Figure 21: Detailed camera view and pre-defined ROI zones of the collected ACPARU dataset for testing the system. (Yang, 2022)

8.2.3 Edge Computing Optimization

The Nvidia Jetson AGX Xavier served as the embedded edge platform tasked with real-time detection, along with the estimation of user pose direction and mobility status. The CPUs of the Xavier were divided into seven units, each assigned with different roles ranging from

managing the operating system, preparing inputs, processing data for algorithms, preparing outputs, and controlling outputs. The last two units were specifically used for receiving orders from the TMC and the controller, as well as transmitting data to servers or mobile devices. The GPU shouldered the responsibility of running the detection script, while the CPU and GPU mutually exchanged information via the cache for each cycle. To enhance the overall efficiency of the edge framework, the detector and feature extractor utilized the TensorRT deep learning framework and performed communication inference asynchronously. Moreover, all the code was drafted in the Python language and was optimized with Numba for better performance.

8.2.4 Parameters Settings

The algorithms' parameters on the ACPARU smart edge nodes were as follows:

- In the user detection part, the minimum object confidence of Rc was set at 50 percent.
- In BEV view projection, the team used an N value of 8.
- The two sensing threads (user detection, pose direction mobility status estimation) were asynchronous. The default processing speed for the detection was in real time, and the pose direction mobility status estimation was set to 2 fps.
- The pre-defined ideal size frame of the object was 300 pixels.
- The minimum object size (S) was no less than 150 pixels.
- The activation function used in the mobility status estimation neural network was ReLU.

8.2.5 User Detection Evaluation

The detection algorithm of the ACPARU edge node was trained and evaluated with the two datasets: the Mobility Aid dataset and the ACPARU dataset. The real-time, multi-object detection identified six categories: pedestrian, person in a wheelchair (PW), pedestrian pushing a

person in a wheelchair (PPW), person using crutches (PC), person using a walking frame (PWF), and biker. For testing on the Mobility Aid dataset, only the first five categories were included, with the average precision of detection being 82.29 percent for pedestrians, 84.64 percent for PW, 74.56 percent for PPW, 73.11 percent for PC, and 78.59 percent for PWF. For testing with the ACPARU dataset, the average precision of the six categories came out to be 88.31 percent for pedestrians, 85.12 percent for PW, 74.77 percent for PPW, 72.14 percent for PC, 72.32 percent for PWF, and 89.46 percent for bikers. The Intersection over Union (IoU) threshold was set at 50 percent, and the Area-Under-Curve for each unique recall mean average precision (mAP@0.50) for the Mobility Aid dataset was 79.84 percent and for the ACPARU dataset was 88.14 percent. With regard to processing speed, the ACPARU achieved an average of 21.09 frames per second (fps) when the input frame resolution was set at 1080 * 720.

8.3 COMMUNICATION SYSTEM EVALUATION

The ACPARU system's integrated gateway can facilitate communications with controllers and TMCs via both wired and wireless networks. The ACPARU smart edge node prototype was put through a trial in which wired and wireless connections between the controller and ACPARU node were scrutinized. This involved running a script for sending and receiving messages every second over a span of one week. All packets (604,800 in total) were successfully received by the target equipment, with none being lost.

Given the complexity of real-world deployment scenarios, the system incorporated two communication methods between the ACPARU node and user personal identification devices (PIDs). In settings where reliable wireless service is available, the ACPARU node can leverage 4G technology for real-time information sharing. Conversely, in rural areas lacking 4G carrier services, the system can activate an internal self-organized network for data sharing.

To accommodate various intersection sizes, the ACPARU edge node integrates a modular design, programmable transmission power, and customized antenna components, catering to a wide array of real-world conditions. This self-organized network, based on the Wi-Fi protocol, fully complies with the IEEE 802.11ac standard.

Customized communication scripts were created for the ACPARU gateway to effectively support connections between controllers, PIDs, and ACPARU nodes. This communication system is suitable for two-lane, three-lane, and even larger intersections, offering low latency and high sensitivity. The smart gateway of the ACPARU can adapt both its software and hardware to meet varying requirements for sensitivity, communication distance, and cost. Detailed parameters and test results can be found in Table 2.

Table 2. The communication performance of the ACPARU self-organized LAN based on Wi-Fi protocol with customized settings and antennas.

Transmit power	Antenna	50 m RSSI	80 m RSSI	Max range	Cost	Delay
17 dBm (50 mW)	6 dB	−82 dBm	−	59 m	$115	<128 ms
17 dBm (50 mW)	9 dB	−77 dBm	−	64 m	$134	<128 ms
17 dBm (50 mW)	12 dB	−73 dBm	−	75 m	$215	<128 ms
20 dBm (100 mW)	6 dB	−66 dBm	−80 dBm	82 m	$115	<128 ms
20 dBm (100 mW)	9 dB	−62 dBm	−76 dBm	90 m	$134	<128 ms
20 dBm (100 mW)	12 dB	−59 dBm	−71 dBm	104 m	$215	<128 ms

9.0 CONCLUSIONS AND FUTURE WORK

9.1 CONCLUSION

This research introduces the Accessible Crossing Platform for Active Road Users (ACPARU) system, a novel roadside unit designed to not only enhance traffic accessibility but also equity and safety for all non-motorized road users at intersections. A customized approach was developed in this project. The team employed video-based perception algorithms on edge devices to accurately identify and classify non-motorized users at signalized intersections. This system detects their location, crossing direction, and mobility status, enabling the activation of signal requests by non-motorized road users themselves. Additionally, the ACPARU smart node can identify disabled users crossing the road, send alerts to controllers and nearby individuals through a mobile application, and generate triggers to potentially extend the crossing phase as required. Through extensive experimentation using real surveillance videos from six different intersections, the ACPARU system demonstrated reliable non-motorized user detection and perception, effective communication, and touch-free function of road crossing triggers in various intersection configurations. It is planned for installation at nine intersections along Washington State Route 522, aiming to further benefit non-motorized users and improve intersection safety and equality.

9.1.1 Relative Publications and Conference Talks

The following journal article that was derived from the project has been published:

Cooperative traffic signal assistance system for non-motorized users and disabilities empowered by computer vision and edge artificial intelligence.

9.2 FUTURE WORKS

9.2.1 Mobile Application

The app for the project has room for improvement. Although the basic required functions have already been integrated into the app, the app itself is still just one small part of the project, and more technologies can be implemented into the app. In addition, the UI design and data collection function can also be improved in many ways. The following are the aspects of the app that can be either revised or enhanced:

- The UI of the app can be designed to be more user-friendly and modern, and the app should be enhanced for disabled people by including more sound and vibration feedback from the mobile phone. This would allow more users to potentially use the app, thus allowing this new transportation safety technology to benefit a bigger population.
- The user recognition system should be connected to the mobile phone so that the graphical pedestrian detection data can be enhanced by GPS data from the mobile phone, and the system can perform better pedestrian tracking even if there are obstacles present. Also, some detection images and system decision results should be shown in an easy-to-understand way to guide users to cross the road, and in this process, sounds and vibrations may be included.
- Privacy and security should also be considered. Although UDP communication is already quite secure, a cybersecurity system should be integrated into the app's communication to prevent potential malware from harming the system or from using the system to cause chaos and danger.

9.2.2 Hardware and System Improvement

Although we used the best hardware on the market that was suitable for this project at the start of the project, the evolution of the hardware quality, reliability, and performance did not stop from the time that we made those hardware selections. In the future, the team plans to update the Xavier computer to newer versions or replace it with even more powerful computing power. The antenna hardware performance could also be upgraded to a higher level so that the system can be applied to much bigger intersections or even some other scenarios. The cybersecurity part of the project may not be enough in the future, so the team may consider involving another unit to enhance security at the hardware level.

Currently, the system is still at an experimental phase. Although the system can work very well, the aesthetic and hardware integration parts of the project were neglected. The team will need to produce a more compact, modular, and weather/impact resistant shell for the hardware to make the system actually suitable for easy application to real-life situations.

10.0 REFERENCES

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.*

Aloul, F., Zahidi, S., & El-Hajj, W. (2009). Two factor authentication using mobile phones. In 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 641-644). IEEE.

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.

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.

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

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.

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

Chen, X., Henrickson, K., & Wang, Y. (2015). Kinect-based Pedestrian Detection for Crowded Scenes. Computer-Aided Civil and Infrastructure Engineering, 31(3), 229-240.

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).

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

Eghtedari, A. G. (2018a). SR-522 SPaT Challenge Infrastructure System Concept of Operations Draft Version 0.1.

Eghtedari, A. G. (2018b). WSDOT NWR SPaT Challenge, WSDOT, Seattle, WA.

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

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).

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

Gay, K. (2011). “Cyber Security Factsheet.” USDOT ITS JPO, < https://www.its.dot.gov/factsheets/pdf/cybersecurity_factsheet.pdf> (May 1, 2019).

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.

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.

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.

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).

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.

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.

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

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

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.

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.

Kjærgaard, M.-B., et al. (2012). "Mobile sensing of pedestrian flocks in indoor environments using wifi signals." Proc., 2012 IEEE International Conference on Pervasive Computing and Communications, IEEE.

Kollmitz, M., Eitel, A., Vasquez, A., Burgard, W., 2019. Deep 3D perception of people and their mobility aids. Robot. Auton. Syst. (ISSN: 0921-8890) 114, 29–40. http://dx.doi.org/10.1016/j.robot.2019.01.011, URL http://ais.informatik.uni-freiburg.de/publications/papers/kollmitz19ras.pdf.

Kreeb, B., and Gay, K. (ND). "SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS) PROOF OF CONCEPT (POC) Fact Sheet." USDOT ITS JPO, < https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf> (May 1, 2019).

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.

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.

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

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.

Malinovskiy, Y., Saunier, N. and Wang, Y. (2012). "Analysis of pedestrian travel with static bluetooth sensors." Transportation Research Record, 2299, 137-149.

Martínez-Pérez, B., De La Torre-Díez, I., & López-Coronado, M. (2015). Privacy and security in mobile health apps: a review and recommendations. Journal of medical systems, 39(1), 181.

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

National Highway Traffic Safety Administration (NHTSA). (2019). 2018 Fatal Motor Vehicle Crashes: Overview, USDOT, Washington, D.C.

National Operations Center of Excellence (NOCoE). (2018). "SPaT Challenge Overview." NOCoE, <https://transportationops.org/spatchallenge> (Sept. 18, 2018).

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

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).

NYCDOT. (2018). New York City Connected Vehicle Pilot Deployment Project: Pedestrian Assistance Device Specification to support the visually impaired, NYCDOT, New York, NY. https://cvp.nyc/sites/default/files/2018-03/PID_1%200_12162016_1.8-%20addendum%20to%20ASD.pdf#page=43&zoom=100,0,845

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.

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

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.

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.

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

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.

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

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

Society of Automotive Engineers SAE. (2016). Surface Vehicle Recommended Practice J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE, Warrendale, PA.

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.

The SPaT Challenge Resource Team (2018). SPaT Infrastructure System Model Concept of Operations Draft Version 1.6. https://transportationops.org/spat-challenge-infrastructure-system-model-concept-operations

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

USDOT. (NDa). “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> (Oct. 15, 2020).

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

USDOT. (NDb). “Connected Vehicle Pilot Deployment Program: Tampa (THEA) Pilot.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/pilots/pilots_thea.htm> (Oct. 15, 2020).

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).

USDOT. (NDc). “Connected Vehicle Pilot Deployment Program: Wyoming (WY) DOT Pilot.” Intelligent Transportation Systems Joint Program Office, <https://www.its.dot.gov/pilots/pilots_wydot.htm> (Oct. 15, 2020).

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).

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).

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

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).

Van Duren, D., Cadzow, S., Petit, J., Whyte, W., Security Innovation, Rausch, R., and TransCore. (2016). Connected Vehicle Pilot Deployment Program Phase 2, Data Privacy Plan-New York City, USDOT ITS Joint Program Office, Washington, D.C. https://rosap.ntl.bts.gov/view/dot/32311

Wang, X., Wang, M., and Li, W. (2014). "Scene-specific pedestrian detection for static video surveillance." IEEE transactions on pattern analysis and machine intelligence, 36(2), 361-374.

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.

Xu, F., Liu, X., and Fujimura, K. (2005). "Pedestrian detection and tracking with night vision." IEEE Transactions on Intelligent Transportation Systems, 6(1), 63-71.

Yang, H. (Frank), Ling, Y., Kopca, C., Ricord, S., & Wang, Y. (2022). Cooperative Traffic Signal Assistance System for non-motorized users and disabilities empowered by computer vision and Edge Artificial Intelligence. Transportation Research Part C: Emerging Technologies, 145, 103896. https://doi.org/10.1016/j.trc.2022.103896

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.

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.

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.

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

Zhao, M., Walker, J., and Wang, C.-C. (2012). "Security Challenges for the Intelligent Transportation System." Proc., SecurIT '12, ACM, Kollam, Kerala, India.