Vulnerable Road Users and Cellular Vehicle-to-Everything (C-V2X) Security

Abena G. Achianor
Purdue School of Engineering and Technology.
IUPUI.
Indianapolis,Indiana
agyasiwa@iu.edu

Garvit Agarwal
Purdue School of Engineering and Technology.
IUPUI.
Indianapolis,Indiana
gagarwa@iu.edu

Ismail Bibers
Purdue School of Engineering and Technology.
IUPUI.
Indianapolis,Indiana
ibibers@iu.edu

Benjamin Rader
Purdue School of Engineering and Technology.
IUPUI.
Indianapolis,Indiana
berader@iu.edu

Ericka White
Purdue School of Engineering and Technology.
IUPUI.
Indianapolis,Indiana
whiteerl@iu.edu

***Abstract*—In 2020 alone over 10,000 vulnerable road users (VRUs) died while going through an intersection [14]. VRUs are classified as bicyclists, pedestrians, and motorcyclists, and they play a big role in the future of autonomous driving. VRUs are at a high risk of being hurt when they are on the road; yet, VRUs have not typically been a priority when the automotive manufactures are building cars. That is until recently when C-V2X was introduced to replace DSRC. Multiple industries are now working together to provide a well-rounded experience for the drivers as well as VRUs within C-V2X vehicles. Companies invested in the C-V2X movement are presenting use cases to help researchers uncover areas that may have been overlooked and need more attention. Our group researched a particular use case that was presented named vulnerable roadside collisions warning (VRUCW) that will be implemented into autonomous C-V2X vehicles. While researching VRUCW we found several wireless security issues that need to be addressed. Therefore, in this article we will give you some background surrounding C-V2X and VRUCW, provide research from the risk assessment conducted on VRUCW, and provide solutions that should be implemented to prevent them.**

***Index Terms*—VRUCW, VRUs, C-V2X, Wireless Security**

I. Introduction

Cellular Vehicle to Everything is the next step in improving transportation efficiency, safety, and understanding. Stats from the World Health Organization show that road traffic injuries are a problem and that the core issues are not going to fix themselves. Road traffic injuries are still the leading cause of death, the world over, for people ages 5 through 29. Over a million people die each year from road traffic crashes, half of all road traffic deaths are among those who are not in a "metal shell", most road traffic deaths occur in low and middle-income countries, and these crashes cost most countries around 3% of their gross domestic product [33]. C-V2X may not be immediately feasible for most countries. However, such a statement assumes that C-V2X cannot be cheap enough for such countries. When it comes to intelligent transportation systems (ITS), governments and the transportation industry need smart minds and problem solvers to leap into the fray and innovate new techniques, methods, and technologies. The journey towards C-V2X arguably began in 1999 when the FCC allocated 75MHz of the spectrum to Dedicated Short Range Communication (DSRC). This was introduced as a part of the Institute of Electrical and Electronics Engineers (IEEE)'s 802.11p standard and was intended to be a vehicular communication protocol for wireless access in vehicular environments (WAVE). One of the defining parts of DSRC, WAVE, or WLAN-based V2X (all the same thing) was the fact that it is WLAN or Wi-Fi. It was approved in 2010 and many vehicle manufacturers started supporting it. Companies like Toyota in 2015, Cadillac in 2017, and Volkswagen in 2019 with the Golf 8 model were a few of the corporations pushing for its integration into vehicles. DSRC was gaining popularity in Europe and Japan the most. However, C-V2X was introduced soon after DSRC and it used cellular instead. Adoption was pretty even for both until 5G was introduced. Although most companies had engineering problems and dilemmas due to the availability of OEM components for DSRC or C-V2X, 5G was a future-facing development that was quite promised, and 3GPP's work in C-V2X was thorough and extensive in accounting for various integration and implementation problems for C-V2X. Surprisingly in 2020 after Covid-19 exploded all over the

planet, the FCC split up the spectrum that had been preserved for V2V with DSRC to unlicensed wi-fi applications. People who are devoted to DSRC still fight on and have slowed down efforts to switch OEMs over to C-V2X. The takeaways and reasons for C-V2X winning were that it was easier to integrate into society because of existing cellular infrastructure, and C-V2X was more oriented toward future innovation with 5G development which is marketable and future-facing in terms of technologal enablement. All in all, C-V2X was just as performant with latency as DSRC was, it was future-facing with 5G applications, and it was cost effective in terms of deployment of infrastructure because LTE and 5G systems could be used with it [22] [23] [17] [11] [10] [15].

C-V2X development originates from 3GPP (3rd Generation Partnership Program). 3GPP is a decentralized entity that includes tons of experts from various companies who have volunteered to work on technical specifications for various wireless technologies. 3GPP develops technical specifications, then standard-setting organizations in countries and international regions develop standards which are then used by the manufacturers and product makers. The most notable aspects of 3GPP's development with C-V2X are the creation of direct and indirect communications for C-V2X through LTE in Releases 14 and 15, and then further developments in 5G with Releases 16 and 17. Most developments in 5G are also backward compatible with the Release 14 and 15-based communications in V2X.

II. Cellular V2X

Cellular V2X communication is crucial in transferring safe, dependable, and adept transportation services that may be considered in both the short and enduring and fulfill today's and time to come's expectations. Cellular V2X (C-V2X) is a tertiary-generation participation project (3GPP) technology that is created to function in both vehicle-to-vehicle and vehicle-to-network modes. It is a bigger developing technology that can conclude V2X requirements while also preparing the most methodical approach to connected and autonomous driving. vehicle-to-everything (V2X) communication is critical for creating real-time and well reliable information for implementing cautious, efficient, and environmentally conscious transportation duties [24].

Cellular Vehicle-to-Everything (C-V2X) has monstrous potential to bring significant life-changing improvements in worldwide vehicular traffic administration [24] [5]. It aids in the reduction of troubles such as enhancing vehicle and pedestrian safety with capabilities such as vehicle notification and control for approaching emergency vehicles with distance/direction information, pedestrians crossing in a crosswalk (traffic lights/signals will be controlled or extended for safety and during unexpected events, allowing the identification and avoidance of a pedestrian darting into traffic, traffic congestion, when an accident is near, a notification of its location and distance will be sent. Things such as school bus notifications, including unloading/loading school children in the area, raised fuel consumption, road security, and road capacity. It organizes a framework for cars to communicate with one another and with the entirety around them, developing all-around non-line-of-sight knowledge and a better level of predictability for increased driver safety and autonomous forcefulness.

Cellular V2X is a 3GPP standard used in vehicle-to-vehicle (V2V) applications like self-driving automobiles. IEEE 802.11p, the standard for V2V and other sorts of V2X means, is an alternative. Cellular V2X uses 3GPP standards 4G LTE or 5G traveling cellular connectedness to transmit messages betwixt automobiles, pedestrians, and roadside traffic control equipment in the way that traffic lights. It commonly makes use of the 5.9 GHz commonness range, which is in an official manner designated as the intelligent conveyance system (ITS) frequency in the vast most countries. C-V2X is network-free and has a 25% higher range than DSRC. [4].

The types of transfer communications capabilities include :

- vehicle-to-infrastructure (V2I)
- vehicle-to-network (V2N)
- vehicle-to-vehicle (V2V)
- vehicle-to-pedestrian (V2P)

A. C-V2X Communication Transmission Modes

C-V2X supports basic road safety features by exchanging messages regarding the position, speed, and direction with the surrounding vehicles, and infrastructure. C-V2X defines two complementary transmission modes [34]

- Short-range/sideline: The mechanisms that allow direct Safety vehicular communications via PC5 interface and it is operating in ITS bands (e.g. 5.9 GHz) under the out-of-coverage/independent of the cellular network such as Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to pedestrian(V2P). Figure 2.

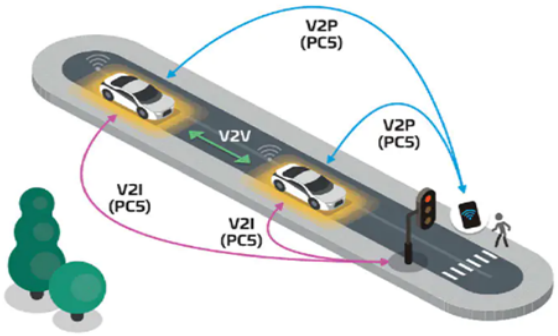

Fig. 1. Direct communications Mode / Designed to Work Without Network Assistance

- Long-range/cellular network communications: The mechanisms that allow direct vehicular communications while the cellular network base station allocates radio resources to the vehicle by the (Uu) interface operates in traditional mobile broadband licensed spectrum such as Vehicle to Network V2N. Figure 3.

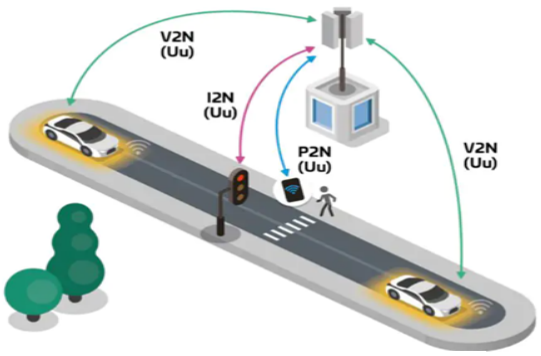

Fig. 2. Network Base communications/ Designed to Work with Network Assistance

B. RSU and OBU Communicate

Since PC5-based C-V2X does not necessitate a cellular network [25], typically there are two types of wireless devices RSU (Road Side Unit) and OBU (On Board Unit) are required to implement C-V2X V2I/V2V/V2P application scenarios:

- RSU: Without the need for cellular networks, a wireless transmitting device can allow direct sildelink communication through a PC5 interface. Road signs, traffic lights, and IP camera information can be broadcasted in real-time to the vehicle via RSU in the predefined area. Another useful scenario is that RSU can be equipped with a SIM card to transfer road information via cellular networks to create additional applications for public safety.
- OBU: Equipped in a vehicle as a wireless communication device to improve the sensor function of autonomous driving buses by direct communication with RSU and other OBUs. OBU is responsible for broadcasting the vehicle's location, direction, and speed information to other defined devices while receiving other vehicles' data as input for its internal algorithms to avoid possible accidents.

C. C-V2X Application Scenarios

RSU/OBU designs must be equipped with 3GPP C-V2X agreeable chipsets in order to use C-V2X applications. Such chipsets are commercially available from Qualcomm, Intel, Huawei, Datang, and Autotalks. Currently, Taiwan uses Qualcomm 9150 for PC5-based C-V2X field testing and commercial deployments [32] [19]. Many interesting applications have come to achievement. The following are some examples of scenarios:

- VRUCW (Vulnerable Road User Collision Warning): a V2P service that warns the driver or independent driving control whole when a vehicle detects a potential pedestrian collision hazard on the roadside through IP Camera and RSU.
- ICW (Intersection Collision Warning): a V2V help that informs the host vehicle driving towards an intersection if an accident is imminent.
- EBW (Emergency Brake Warning): another V2V service, which warns the host vehicle if the front remote vehicle is making a sudden brake. The host vehicle receives an alert from the front vehicle and determines if a collision will happen.
- DNPW (Do Not Pass Warning): a V2V service used when a host vehicle intends to pass the front vehicle in the opposite direction lane. The adjacent car moving in the added direction will be informed by the host vehicle. The OBU of the host vehicle will receive a DNPW message to decide if it is safe to pass.
- TSP (Traffic Signal Preemption): a V2I service that admits high-priority vehicles nearing the signal control junction, such as ambulances, fire engines, and police cars, to transmit a priority signal so that the vehicles can pass through.

III. VRUCW

Vulnerable Road User Collision Warning (VRUCW) [5] can be defined as a V2P (Vehicle To Pedestrian) service that alerts the driver or autonomous driving control unit when a vehicle is sensing a potential pedestrian collision threat via IP Camera and RSU on the roadside. VRUCW is perhaps the most important implementation of CV2X as it directly impacts roadside accidents and can help us save hundreds of thousands of lives.

A. Vulnerable Road Users

So in order to implement the Vulnerable Road User Collision Warning, we first need to define what these Vulnerable Road Users are. The term vulnerable road user [2] (VRU) is used mainly to describe those unprotected by an outside shield, as they sustain a greater risk of injury in any collision with a vehicle and are therefore highly in need of protection against such collisions.

Various VRU categories are :

- Pedestrians
- Cyclists (including eBikes)
- Motorcyclists
- Road workers
- Wheelchair users
- Scooter, skateboard and Segway users

B. How VRUCW Works?

The architecture of VRUCW is extremely similar to the general architecture of CV2X. Since we could not create an actual implementation of CV2X, and consequently VRUCW, we had to take an existing model which is present at [1]. This paper included a small-scale prototype of VRUCW that we inherited for all of our research work. The multi-steps that includes in the typical functioning of VRUCW are:

- **RSU**, as a roadside equipment, receives information from outside sources, such as AI servers, and 4G/5G telecommunication networks. Then, it broadcasts this information by PC5 interface using a unified message format in its coverage field, the maximum reachable radius can be one

kilometer if there are no obstacles such as buildings or trees.

- **OBU** is connected with the Industrial PC (IPC) of the autonomous driving system via Transmission Control Protocol (TCP)/Internet Protocol (IP) protocol. The OBU with 12V power is provided by the vehicle, and antennas of OBU should be installed outside of vehicle for better messages receiving. After a successful 3-way TCP/IP handshake connection between OBU and control unit of autonomous vehicle, OBU can receive Global Navigation System Satellite (GNSS) and Controller Area Network (CAN) messages from the vehicle's control unit.
- Combining vulnerable road user information from RSU, OBU can instantly judge the status of road safety and notify the autonomous driving control unit.

A visual representation of these steps is given in the figure below:

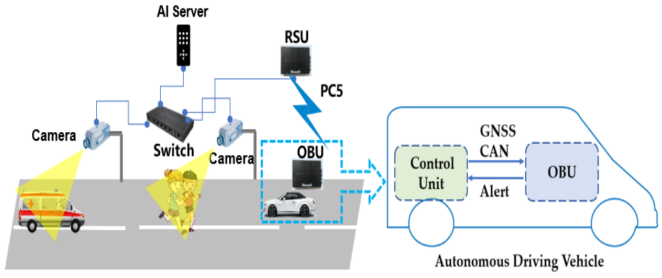

Fig. 3. VRUCW Architecture

C. VRUCW Components

1) AI Server: The AI Server in this modeled VRUCW architecture is from [1], which had the following specifications:

- CPU I7-8700K
- GPU 2 × GTX1080Ti
- RAM 256 G
- Hardisk 1 TB
- OS Windows 10

We understand that these specs are not ideal for a full-scale AI Server, and consequently, this shows in the latency within Camera-RSU Communication. The experiments that the authors did can be shown in the following table:

Item	Step	Latency (ms)
Detect Program	Preprocess	1.3697
	Detect	165.0450
	Convert result	0.0071
	Save result	0.0403
	Total	**166.4621**

Fig. 4. Latency Table

Artificial Intelligence (AI) detection, object recognition and movement prediction for collision warning are used in this model. In the AI server, SSD and ResNet-18 [24] were implemented as network framework. SSD, which stands for Single Shot Detection, means that AI server only needs to take one single shot to detect multiple objects within the image. Compared with the two-stage image detection, the inference and error rate are greatly reduced. The deep residual network (ResNet) is one of the most commonly convolution neural networks (CNNs) for the image feature extraction. ResNet-18 consists of 17 convolution layers and a fully connected layer as shown in Figure 7. This neutral network reduces the amount of calculation by using a 3 × 3 small convolution kernel, so that the time consumption of handling process can meet the low latency required by C-V2X in 3GPP Rel-14 [27].

2) Algorithm of Information Flow: The flow of information followed simple processes which were directed by an algorithm. This algorithm takes into account the distance between the Vehicle and the Vulnerable Road User (S), and it also takes in the speed of the vehicle (V). This algorithm is shown in Fig 5:

Algorithm 1 Threshold for VRUCW Trigger in OBU

1: **if** $S > 50$ m **then**
2: the target pedestrian is keeping a safe distance with the host vehicle, no collision warning is sent.
3: **else if** $V < 10$ km/h **then**
4: the host vehicle speed is not fast so that pedestrian can walk away from danger situation, no collision warning is sent.
5: **else if** $S \leqslant 50$ m and $V \geqslant 10$ km/h **then**
6: the target pedestrian is keeping a danger situation with the host vehicle, collision warning is sent.
7: **end if**

Fig. 5. Algorithm for VRUCW Trigger in OBU

D. Information Flow process

Initially, the image size that the camera sends to the AI Server is 2592 × 1944 and an image extraction speed of 10 frames per second are used in this VRUCW model [26]. The AI server equipped with the target classification algorithm is utilized to determine the pedestrian's category results, which include a person, car, motorcycle, a person with an umbrella, baby carriage, and a person at night. If a pedestrian passes this area under camera coverage, AI server will detect this object and transfer object recognition, position information, and movement prediction analysis results to RSU. RSU encapsulates these messages into broadcast packages and broadcasts this information to all the OBUs within the coverage area of RSU. Meanwhile, the autonomous driving vehicle's control unit sends GNSS and CAN messages to OBU by 50 Hz or 100 Hz frequency. OBU is responsible for combining all the information to determine if a collision is approaching. We use below Algorithm 1 for collision warning trigger threshold after detecting an object. S is the distance between the host vehicle and the pedestrian. V is the speed of the host vehicle. When all the trigger points are met for the alert threshold, a VRU warning message will be sent out from OBU to the autonomous vehicle control unit. Autonomous vehicle own control policy for slowing down or stopping is out of the scope of VRUCW.

SCENARIOS

E. Scenario One: Urban Intersection Implementation

THE PERFORMANCE REQUIREMENTS FOR THE BASIC ROAD SAFETY AND ADVANCED V2X SERVICES

Use case group	Transmission mode	Latency (ms)	Reliability	Maximum Data Rate (Mbps)	Communication Range (m)
Basic road safety services supported by 3GPP Rel-14/Rel-15	Broadcast	10-100	90%	31.7	100-300
Vehicles Platooning	Broadcast, groupcast and unicast	10-25	90% - [99.99%]	[65]	less than 100m; [5-10] sec * max relative speed
Advanced driving	Broadcast	[3-100]	[99.99%]-[99.999%]	[50]	[5-10] sec * max relative speed
Extended sensor	Broadcast	3-100	[90%-99.999%]	1000	[50-1000]
Remote driving	Unicast	[5-20]	[99.999%]	UL: 25 DL: 1	Same as cellular uplink and downlink

Fig. 6. The Basic Road Safety services which are relevant to VRUCW are highlighted in Red to show important metric requirements for the PC5 connection. These requirements are defined in the 3GPP technical specification (TS) 22.185 "Service Requirements for V2X Services V14.4.0" from 2018 [12].

Perhaps one of the most problematic situations for vulnerable road user collision warnings is city intersections. Between the potentially dense populations and the high number of large objects, there is a lot of room for error. Not to mention, it is hard to defend against attacks in a densely populated area and the larger amount of devices can leave more room os denial of service attacks against RSUs.Stats and research on urban area VRU accidents undeniably show that using VRUCW could save tons of lives. For instance, cyclist crashes with cars account for a large percentage of accidents in urban settings. This is especially relevant to developed countries where the fatalities of cyclists have quickly increased with growing cycling habits. Most of these crashes seem to occur in intersection scenarios or places where the car cannot have line-of-sight with the cyclist from things like buildings or backing out of parking lots [31] [1]. The characteristics of VRU accidents are also deeply intertwined with the number of vehicles and the speed. Most accidents occur during the late afternoon hours in high-density areas. Research also suggests that intersections have the highest risk and accidents with VRUs are 10.6 times more likely. High vehicle speed also correlates to worse injuries and much more fatalities [38].

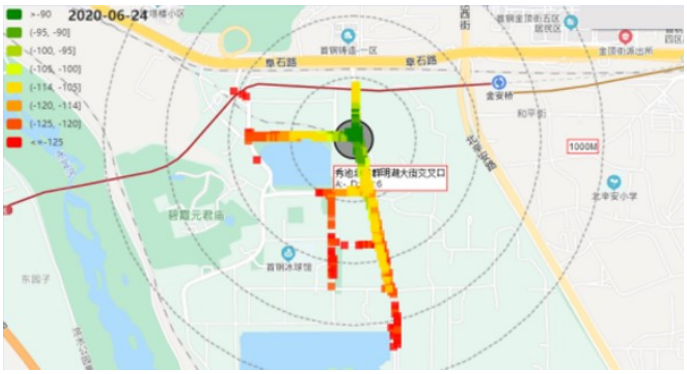

Fig. 7. RSU performance in an intersection in China. The red indicates poor performance from path loss and shadowing due to distance and objects causing interference [2].

1) RSU Interference (NLOS): Cities are home to all sorts of in-ground objects, architectural wonders, and large metal shapes that make up the over-the-air mediums for all sorts of signals. In the case of PC5, these objects cause all sorts of interference, and this interference comes in the form of path loss and shadowing. These are two types of "large scale fading" which are dependent on the medium of a signal and the distance the signal must travel. Shadowing is more related to obstructions and the signal frequency and path loss is also similar. What is important to note is that all signals and their ability to transmit in their environments depends on their frequency, power, and the nature of the objects between the transmitters and the receivers [39].

In cities, it is very important to understand the various components of the signals, potential obstructions, and the general medium for those signals. In order to predict where transmitters will work best, mathematical methods for determining the performance of a signal called "channel models" are used. The problem with these models is that some may not be accurate to the environment the user is intending for. If the right channel model is not used before deploying an RSU, then signals may not propagate well enough to meet the 3GPP basic road safety standards [12]. Most researchers define these as non-line-of-sight (NLOS) cases.

The sidelink interface (PC5) uses the decentralized scheduling of mode 4 instead of the centralized scheduling of mode 3. Mode 4 uses "sensing-based SPS" which is short for semi-persistent scheduling. The semi-persistent scheduling part means that any communicating nodes on the channel which have a conversation going will use the channel in a semi-persistent manner. In other words, "each node successively uses the same frequency resource at specific times." The sensing part is based on two things: the history of past resource slot utilization and the estimation of the interference of future slots. In layman's terms, PC5 communication between devices (RSUs and OBUs) is not decided by a base station and it depends on interference of the signals [12] [19].

Research simulating PC5 and DSRC with NS-3 and SUMO showed that C-V2X (even compared to DSRC) is not as great in NLOS scenarios. However, the other benefits outweigh the costs (reliability, latency) and it still has less Package Error Rate (PER) as path loss increases [28]. Additionally, CV2X was shown to outperform in NLOS and congestion cases [20]. However, this testing was quite limited, especially in channel model usage.

Research from Beijing with actual RSU devices in Urban scenarios showed that intersections specifically create plenty of shadowing and "shielding" for RSU signals. It was mentioned that this is most applicable to intersection collision warnings which can be thought of as more specific applications of VRUCWs. Due to increased package loss rate and power-related parameters, it was determined RSU devices can feasibly cover only one intersection at a time in urban settings. This is most true for dense downtown intersections, and multiple RSUs should be placed to make up for shadowing and path loss [2].

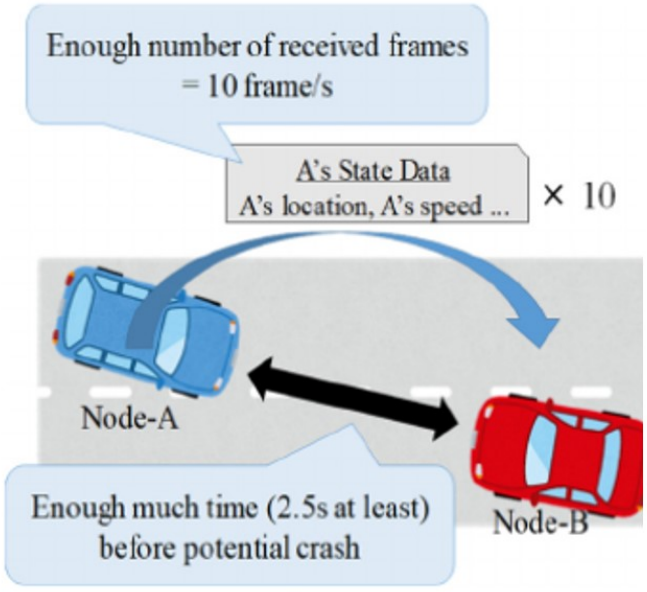

Fig. 8. Quality of service requirements for an intersection collision warning (ICW) [19].

Crash Scenario Parameters.	Values
NTS	10–30 frames/s
Node distribution model	Uniform, Realistic
Relative speed	120 km/h–240 km/h
Wireless Settings	**Values**
Carrier frequency	5.9 GHz
Bandwidth	10 MHz
Frame size	190 bytes
Radio propagation model	WINNER+ (LOS) B1
Shadowing deviation	3 dB (i.i.d)
Noise power	−110 dBm

Fig. 9. Flawed simulation configurations are highlighted in RED from research that tries to prove PC5 cannot feasibly do VRUCW in intersections. Other research suggests that these configurations drastically affect PC5 performance in simulations and that better channel models such as the one proposed in Rel 15 from 3GPP should instead be used [19] [6].

2) Vehicle Congestion: For VRUCWs to work properly, they need to be timely. This is why 3GPP has such high-standard requirements for basic road safety messages. Basic road safety messages, by default, are sent out ten times per second or every 100ms [29]. The core function of C-V2X is to allow various entities to understand the position of other entities at all times. For this to happen, as was mentioned in the architecture section, computation, AI, and other intelligent systems are required to understand and process the locations of these entities. This can lead to the question of how many entities such a system can handle at once. If any piece of the system fails to meet the basic road safety latency and availability requirements, then there could be a catastrophic loss of life.

There are two factors to account for when simulating PC5 performance in a congested scenario: the number of vehicles or OBUs and the channel model being used to simulate the signal interference and path loss. Using a few channel models with PC5 in a highway scenario, simulations indicated that the performance of PC5 in simulations greatly depends on the channel model being used. The packet reception ratio (PRR) was calculated for three channel models along with different bandwidths. It was shown that the newly defined 3GPP channel model from Release 15 performed at 100% PRR while the popular WINNER II channel model performed at 54.85%. Using the correct channel model can drastically affect studies [6]. Research using the ”Manhattan Scenario” also backed supported this conclusion [7].

Some research claims that PC5 mode 5 performs only a percentage of the VRUCW quality of service (QoS) requirements. As shown in Figure 8, it is claimed that VRUCW, ICW, or any sort of collision warning requires basic road safety messages to be transmitted between the VRU and vehicle parties at least times and 2.5 seconds before a collision occurs. This gives the vehicle the average required time to slow down. The research suggests that RSUs cannot perform well enough in small, medium, or large intersections and that the RSUs can only accommodate a small number of entities [19]. However, as stated in other research the channel model and doppler effect can greatly reduce the proposed performance of PC5 depending on what is used during simulation. In this case, the WINNER II models with LOS and NLOS are used. It was shown in previous research that these perform poorly [6]. Additionally, the research from [19] includes vehicles that are going anywhere from 120km/h - 240 km/h which equates to at least 74mph through an intersection! These two findings which are shown in Figure 9 prove that such research is deeply flawed.

Qualcomm and 5GAA studies show that extensive lab simulations with large numbers of actual RSU devices perform well in congested scenarios. They perform even better with congestion mechanisms too [8] [28]. In other words, there is conflicting research that suggests simulations need to use more accurate channel models and that comparisons are not as simple as running NS-3 and SUMO with some generic channel model.

3) Resource Block Attacks: As explained in previous sections, the decentralized PC5 mode 4 does not use a base station but instead uses sensing-based semi-persistent scheduling to decide which parts of the 5.9GHz channel to use and when. During this process between RSUs and/or OBUs, vehicles decide specifically based on the Received Signal Strength Indicator (RSSI). After the vehicle chooses, then Basic Safety Messages (BSMs), which are the same as the ones explained in the congestion scenario, are transmitted continuously ten times per second. Assuming resource blocks are ”orthogonal”,

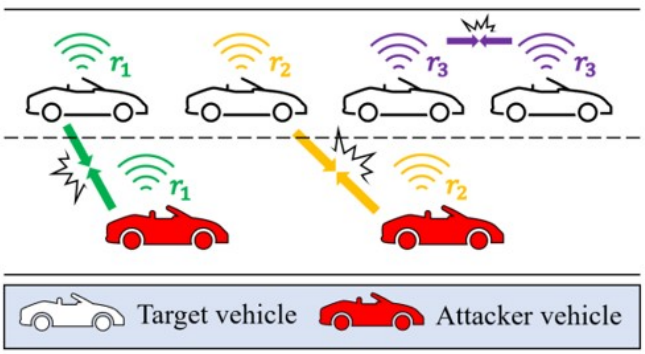

Fig. 10. Example of a cooperative attack scenario where there are just as many malicious OBU vehicles are there are normal vehicles [37]

every once in a while, these vehicles may choose the same resource block as another vehicle and there may be packet collisions. This is very rare with a small number of vehicles and still quite rare with hundreds of vehicles. However, due to the decentralized nature of mode 4, it is possible to proactively jump into resource block allocations and cause packet collisions. Research on DoS attacks against PC5 mode 4 shows that there is high risk for easy interruption of BSMs and total failure of VRUCW functionality. There are two ways for attackers to successfully create a denial of service on PC5 mode 4. In an urban scenario, attackers could set up enough malicious OBUs that are modified. When attacker OBUs cooperate and there are enough of them, then there can be total deniability of RSU resources. In the "oblivious" attack method where attackers are not cooperating or "aiming" for particular target vehicles, they can have just as much success with high vehicle densities or congestion scenarios [37].

F. Scenario Two: The Camera Coverage Area is Limited

In this scenario, the inability to detect road users is because of the: hidden angle/ blind spot. In this case, the camera cannot see the road user, which may endanger road users.

G. Scenario Three: RSU Failure and Cost Effectiveness

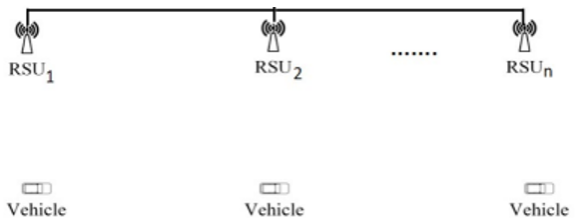

Fig. 11. Example of redundant RSUs which could be connected by fiber or a 5G connection. If one fails, then the others take its place.

When installing RSUs on structures, installers should be mindful that other signs and devices on the structure may impact the RSU [3]. Since the system has been known to experience failures due to inclement weather such as high winds whipping around signage on a pole, taking out RSU antennas, and causing damage [3].

RSUs that are not properly grounded can cause lightning strikes to target the ungrounded metal structures. With structures not grounded this introduces a voltage surge that enters the RSU at the Ethernet connector [3]. The Ethernet connector is attached directly to a Power over Ethernet (PoE) Splitter electronic subassembly mounted inside the RSU. When this piece is damaged, the PoE Splitter ceases communications with the Control Unit. The PoE splitter for RSU must be replaced – RSU will return to normal functionality again [3].

For the cost-effectiveness of RSUs, if they are widely deployed around a city, coverage will be expanded, but the RSU setup cost may be too high [18]. This creates a major challenge in figuring out how to accurately deploy a small number of RSUs while ensuring excellent coverage since the cost could range between 13,000 and 15,000 per unit capital cost, and up to 2,400 per unit per year for operation and maintenance [18]. Due to the high cost of implementing RSUs many large deployments of the system may fail [18].

SCENARIOS SOLUTIONS

H. Solution for Scenario One: Urban Intersection Implementation

There are various ways to approach designing solutions for the urban intersection implementations of VRUCW. Through the conducted research, it has been determined that C-V2X product manufacturers and enablers must be smart about where RSUs are placed, how congestion is handled in PC5 mode 4, and what sorts of security should be used to mitigate resource block weaknesses.

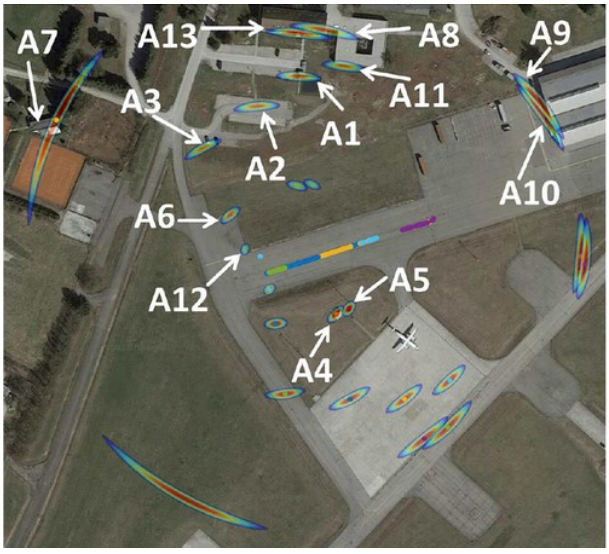

Fig. 12. Example of tracking reflections over time in an environment using the KEST algorithm. "Tracked path over time in urban environment as a results of the proposed tracking algorithm [36]."

1) RSU Interference (NLOS) - Create Channel Models for Each Situation: NLOS can be a huge issue for intersection

collisions involving VRUs. This involves cases where there is interference with the RSU signal to vehicles or VRUs, and the result is more latency, packet loss, or increased power usage. However, research suggests that there is hope for NLOS issues. The channel model is perhaps the most important piece of mitigating NLOS problems and being cost-effective about where to install RSUs in an urban setting or any setting where there exists a potential for signal path loss and shadowing. The solution is rather simple - use better channel models before setting up C-V2X network topologies in cities. There are multiple approaches to creating channel models: "deterministic, stochastic, and geometry-based stochastic channel models (GSCMs) [36]." Channel model studies have been conducted using the GSCM approach. They used a "super resolution estimation and tracking algorithm", named KEST, to estimate specular multipath components of an environment. In an NLOS situation, they used their method to recognize scattering from various objects and in turn develop a more accurate channel model. Such techniques should be refined a bit more before use in actual cities, but the research shows promise for creating better processes in city C-V2X planning [36].

2) Vehicle Congestion - Congestion Mechanisms: The solution to congestion affecting latency and the application of VRUCW (not including malicious actors) involves using programmatic mechanisms. Just as with any other communication channel handling, there will be some slowdown as more entities fill up the channel. However, this can be done more elegantly with a programmatic approach. The Society of Automotive Engineers actually developed a "muting" mechanism defined as J3161/1 (On-Board System Requirements for LTE V2X V2V Safety Communications) to mitigate congestion problems. Extensive research from Qualcomm refutes opposing claims with strong evidence that this mechanism works to defeat congestion latency in situations where basic safety messages (BSMs) are a priority. This includes the VRUCW situation [8] [28]. However, the problem with any congestion mechanism is that it still relies on the goodwill of users. If malicious users decide to go against these requirements, then they can be selfish and use up resources for themselves. In other words, some sort of security is still necessary to prevent the potentially deadly possibility.

3) Resource Block Attacks - TESLA Hash Chains & PKI: Most research suggests the use of PKI (public key infrastructure) to handle PC5 communication integrity and secrecy. However, it is well-known that such an approach would cost vehicle manufacturers and OEMs a large amount of money. Manufacturers would need a hardware security module (HSM), license for certificates, certificates for pseudonymization, expenses for PKI integration, deployment, and even maintenance. A conservative estimate puts this at 30 euros per vehicle and results in an estimated 88 billion euros worth of authorization tickets in just the 1st year [16]. PKC would utilize ECDSA (Elliptic Curve Digital Signature Algorithm) along with some servers at the "edge" (multi-edge computing/MEC). Research suggests that TESLA (Timed Efficient

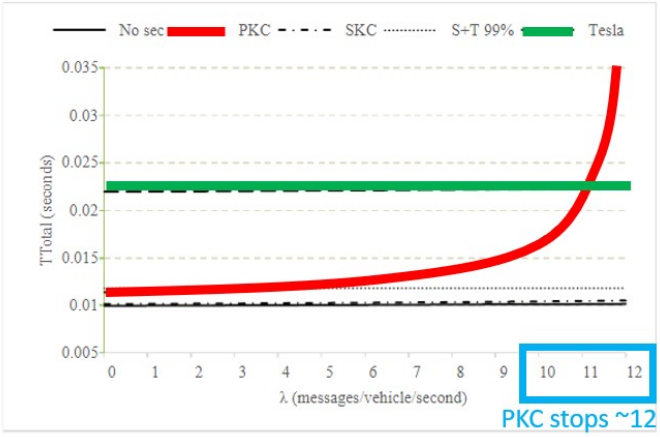

Fig. 13. Comparison of performance of PKI (public key infrastructure) with pseudonym use vs. TESLA SKC (symmetric key cryptography) and hash chaining [29]

Stream Loss-tolerant Authentication) is a "viable alternative" to PKC. Most researchers did not consider TESLA because of the overhead needed to establish hash chains during the process. Based on specification sheets of HSMs, the signature generation and verification times for PKC are estimated to be 0.125ms and 0.5ms. These are not costly when there is a low number of vehicles. However, as shown in Figure 13, a larger number of vehicles results in a latency singularity where generation and verification cannot be done fast enough. TESLA uses SKC MAC to protect the integirty of messages. "A sequence of keys used by a given sender is generated such that the Nth key used is the result of applying a hash function to the N+1th key. Thus, the hash function can be used to verify a sequence of keys used by a given sender, and hence the sequence of messages it sent, provided that the first key in the sequence can reliably be attributed to that sender. The main benefits of TESLA are low computation overhead, low communication overhead, and robustness to packet loss [29]." Further research from the same researchers show how a V2X Application Server can be used to proactively and reliably give out hash chain key committments based on the locations of vehicles. This shows how TESLA could be pragmatically applied in a cheap manner for realistic VRUCW scenarios [30].

I. Solution for Scenario Two: Limited Coverage Area

We need to consider these limitations of the camera coverage area.

- The first solution is to add more cameras for full coverage, But this depends on the cost of the investment because adding more cameras causes the budget to increase.
- The second solution, Relying on the sensor data of the embedded vehicles is the first solution by communicating and sending alert messages to each other V2V and V2I via the PC5 interface to ensure the safety of VRUs who are visible from the vehicles.

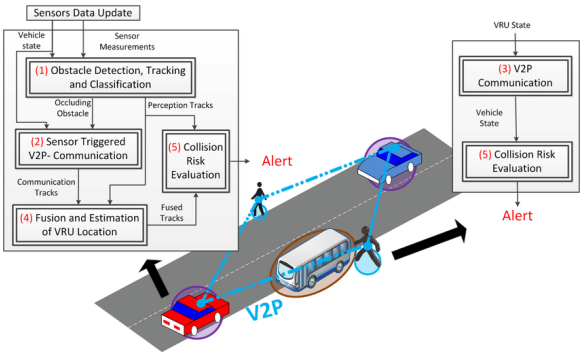

Fig. 14. Safety messages include Cooperative Awareness Messages, Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), Vehicle-to-Infrastructure (V2I)

J. Solution for Scenario Three: Information Re-distribution and Redundancy

The solution of re-distribution and redundancy of information from the OBUs to the active RSUs would be the most effective route.

If you have 3 RSUs within a communication range connected by fiber or 5G connection, and one fails, the remaining systems will continue to gather information. The OBUs will accumulate and collect data from the vehicle(s) until the RSU regains power. The Remaining RSUs will also continue to collect data from the OBUs simultaneously until the out-of-service RSU is fixed or replaced. The cycle of information being transmitted back and forth between the two systems assures round-the-clock safety for vulnerable road users. [3].

IV. Related Works

A. 5GAA

5G Automotive Association (5GAA) is a cross-industry organization focused on bridging the gap between companies in the automotive, technology, and telecommunication industries [9]. Their goal is to use wireless technology to create vehicle-to-vehicle and vehicle-to-infrastructure communications [9]. Currently they are working on several cross-border projects to ensure reliable access to 5G network. One of their most recent projects was a case study done in China to see how C-V2X direct PC5 communication could be used as a tolling application on highways and in highway scenarios [21]. It provided an investment analysis for necessary infrastructure, study on what C-V2X development would be beneficial, and information how the PC5 C-V2X would differ from traditional tolling China uses now [21]. In addition to case studies, 5GAA also hosts numerous conferences that allow various companies to introduce projects they are working on to make C-V2X a reality.

B. Qualcomm

Qualcomm is one of the numerous companies that 5GAA is in cahoots with. They provide cloud connected autonomous platforms for telecommunication, computing, and driver assistance and autonomy [35]. Snapdragon is their most recent project that is providing customers with a cloud connected autonomous platform. Snapdragon is compliant with Release 15 of 3GPP making it capable of working with 5G-NR, having access to vehicle-to-everything communications, etc. [35]. Therefore, it allows car manufacturers with the opportunity to provide a safer and immersive experience to their customers with the new technological features that Snapdragon has [35].

Fig. 15. Qualcomm Snapdragon

V. Conclusion

Cellular vehicle-to-everything (C-V2X) has proven to be the future of autonomous driving. Electronically extending a vehicle's line of sight by providing danger alerts, road awareness, and traffic cooperation. Providing a higher capacity of data for receiving and transmitting information securely. Housing the vulnerable road user collision warning component that allows the safe passage of vulnerable road users who are left unprotected in the event of an accident. And a redistribution and redundancy mechanism in the event of system failure.

References

[1] *Cyclist-car accidents: their consequences for cyclists and typical accident scenarios*, 2015.

[2] *Research on wireless coverage performance of LTE-V2X in urban scenario*, 2021.

[3] J.D. Schneeberger . Connected vehicle deployment technical assistance, roadside unit (rsu) lessons learned and best practice, 05 2020.

[4] Ralph . The technical writer's handbook, by matt young, university science books, mill valley, california, 1989, 232 pp. *Mol. Reprod. Dev.*, 25:97–97, 1990.

[5] 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR). *Deep Residual Learning for Image Recognition*, 0.

[6] 2018 10th International Conference on Communications, Circuits and Systems (ICCCAS). *Performances of CV2X Communication on Highway under Varying Channel Propagation Models*, 0.

[7] 2019 IEEE 90th Vehicular Technology Conference (VTC2019Fall). *Performance Analysis of CV2X Mode 4 Communication Introducing an OpenSource CV2X Simulator*, 0.

[8] Hamza Abbasi and Ralph Gholmieh. C-v2x performance in highly congested highway scenarios, 01 2021.

[9] 5G Automotive Association. 5gaa discusses how c-v2x turns connected and safe mobility into reality at mobile world congress 2022 in barcelona – 5g automotive association, 03 2022.

[10] AUTOCRYPT. Dsrc vs. c-v2x: A detailed comparison of the 2 types of v2x technologies, 01 2021.

[11] Autotalks. C-v2x vs dsrc — get your facts straight on cellular v2x, lte-v lte-v2x, 08 2021.

[12] S Chen, J Hu, Y Shi, L Zhao, and W Li. A vision of cv2x: Technologies, field testing, and challenges with chinese development. *IEEE Internet of Things Journal*, 7:3872–3881, 0.

[13] NATIONAL SAFETY COUNCIL. Position/policy statement - vulnerable road users, 2018.

[14] Transportation Department. Enhancing the safety of vulnerable road users at intersections; request for information, 09 2022.

[15] Gary Elinoff. Is c-v2x overtaking dsrc in vehicle-to-vehicle communications? - news, 03 2019.

[16] Mikael Fallgren, Markus Dillinger, Toktam Mahmoodi, and Tommy Svensson. *Cellular V2X for Connected Automated Driving*. Wiley 2021, 2021.

[17] Jonathan M. Gitlin. Court rules fcc is allowed to reassign 5.9 ghz bandwidth, killing v2x, 08 2022.

[18] Abderrahim Guerna, Salim Bitam, and Carlos Calafate. Roadside unit deployment in internet of vehicles systems: A survey. *Sensors*, 22:3190, 04 2022.

[19] Takeshi Hirai and Tutomu Murase. Performance evaluations of pc5based cellularv2x mode 4 for feasibility analysis of driver assistance systems with crash warning. *Sensors*, 20:2950, 05 2020.

[20] Mouna Karoui, Vincent Berg, and Sylvie Mayrargue. *Assessment of V2X Communications For Enhanced Vulnerable Road Users Safety*. 06 2022.

[21] Tongji University Cooperative Automated Transportation (CAT) Lab. C-v2x direct communications-based tolling: China case study, 08 2022.

[22] Roger Lanctot. A funny thing happened on the way to 5g cars, 03 2021.

[23] Roger Lanctot. C-v2x: Talking cars: Toil trouble, 08 2022.

[24] John Meredith, Patrick Merias, Hanbyul Seo, Deping Liu, and Ying Peng. Study on lte-based v2x services - ts 36.885, 2015.

[25] Patrick Merias. Evolved universal terrestrial radio access (e-utra); physical layer procedures - ts 36.213, 12 2021.

[26] Lili Miao, ShangFu Chen, YuLing Hsu, and KaiLung Hua. How does cv2x help autonomous driving to avoid accidents? *Sensors*, 22, 2022.

[27] Lili Miao, John Virtusio, and KaiLung Hua. Pc5based cellularv2x evolution and deployment. *Sensors*, 21:843, 01 2021.

[28] Jim Misener. C-v2x delivers outstanding performance for automotive safety, 11 2020.

[29] Mujahid Muhammad, Paul Kearney, Adel Aneiba, and Andreas Kunz. *Analysis of Security Overhead in Broadcast V2V Communications*, pages 251–263. 08 2019.

[30] Mujahid Muhammad, Paul Kearney, Adel Aneiba, and Andreas Kunz. *Efficient Distribution of Key Chain Commitments for Broadcast Authentication in V2V Communications*. 11 2020.

[31] Husam Muslim and Jacobo AntonaMakoshi. A review of vehicletovulnerable road user collisions on limitedaccess highways to support the development of automated vehicle safety assessments. *Safety*, 8, 2022.

[32] Society of Automotive Engineers. J3016b: Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles - sae international, 2018.

[33] World Health Organization. Road traffic injuries, 06 2022.

[34] Apostolos Papathanassiou, Alexey Khoryaev, Next Generation, Intel Client Standards, Internet of Things Businesses, Systems Architecture Group (CISA), and Intel Corporation. Cellular v2x as the essential enabler of superior global connected transportation services — cellular v2x - ieee future networks, 06 2017.

[35] Qualcomm. Snapdragon auto 5g modem-rf — qualcomm.

[36] Ibrahim Rashdan, Fabian , Stephan Sand, Thomas Jost, and Giuseppe Caire. Measurementbased geometrical characterisation of the vehicletovulnerableroaduser communication channel. *IET Microw. Antennas Propag.*, 14:1700–1710, 2020.

[37] Natasa Trkulja, David Starobinski, and Randall A Berry. Denial-of-service attacks on c-v2x networks. *CoRR*, abs/2010.13725, 2020.

[38] Mariana Vilaça, Nélia Silva, and Margarida C Coelho. Statistical analysis of the occurrence and severity of crashes involving vulnerable road users. *20th EURO Working Group on Transportation Meeting, EWGT 2017, 46 September 2017, Budapest, Hungary*, 27:1113–1120, 2017.

[39] Wireless World. Difference between small scale fading and large scale fading.

[40] T. Yorozu, M Hirano, K Oka, and Y Tagawa. Electron spectroscopy studies on magnetooptical media and plastic substrate interface. *IEEE Translation Journal on Magnetics in Japan*, 2:740–741, 0.