Vehicle-to-Vehicle (V2V) Communication Implementation

Gunnar Fandrich
Group: Autogators
Electrical and Computer Engineering
University of Florida
Gainesville, Florida
gunnarfandrich@ufl.edu

Mark Lai
Group: Autogators
Electrical and Computer Engineering
University of Florida
Gainesville, Florida
marklai@ufl.edu

Rafael Hernandez-Lopez
Group: Autogators
Electrical and Computer Engineering
University of Florida
Gainesville, Florida
rhernandezlopez1@ufl.edu

Rohan Malik
Group: Autogators
Electrical and Computer Engineering
University of Florida
Gainesville, Florida
rmalik@ufl.edu

***Abstract*—Vehicle-to-vehicle (V2V) allows communication between vehicles, promoting driver awareness and potentially reducing the number of collisions. Existing V2V implementations (cellular vehicle-to-everything, C-V2X) rely on cloud data, whereas the implementation shown in this paper does true V2V between vehicles. A mockup utilizing two ESP32 with a time-of-flight (ToF) sensor and accelerometer communicate using UDP to deliver a proof-of-concept for V2V that can be used as a base for V2V.**

***Index Terms*—V2V, vehicles, driver, awareness, C, ESP32, Wi-Fi, UDP, UDP Broadcast**

I. Introduction

A. Problem Statement

As society moves towards utilizing more autonomous driving systems, vehicles can act as a network to promote efficient and safe driving. This network is referred to as vehicle-to-vehicle (V2V). Automotive vehicles should communicate with each other through V2V to increase driver awareness and reduce the number of collisions [1]. A simple mockup of a V2V system should illustrate the safety increase provided by V2V communication.

B. Background and Related Works

The current state of V2V is nonexistent. The closest thing on the market to V2V is the 2023 Safety Cloud for Chrysler Vehicles, which is implemented through a cellular network to create C-V2X (cellular vehicle-to-everything) [2], [3]. While this is fairly close to V2V, passing through a cloud does not exhibit true V2V. Ideally the cars would communicate directly to each other, which is what is covered by the implementation discussed in this paper. Additionally, Stellantis announced vehicle-to-grid (V2G) testing in 2019 [4].

In 1999, the FCC designated a 75 MHz spectrum in the 5.9 GHz band for dedicated short-range communications (DSRC) [5]. Unfortunately, this band was reallocated in 2020 for unlicensed Wi-Fi [5] use due to the failure of automobile makers to release V2X production cars. Due to the removal of this band, we chose UDP over Wi-Fi as an acceptable simplified protocol for V2V. Ideally, UDP would be replaced with another protocol built on top of UDP – or similar protocol – specifically for V2V and operate on an FCC-designated band for V2V.

In recent years, newer vehicles have been produced with various driver warning systems. One such driver warning system is lane departure warning. Lane departure warning has been observed to reduce single-vehicle, sideswipe, and head-on crash severity by 11 percent and the severity of crash injury by 21 percent [6]. Lane departure warning systems solely alert a driver of a single nearby obstacle on each side of their car. V2V, on the other hand, provides the possibility to reduce common vehicular crashes by communicating warnings and the presence of more than two vehicles or obstacles to the drivers of connected vehicles.

V2V will be illustrated using an ESP32 paired with time-of-flight (ToF) sensor and accelerometer. Each ESP32 represents a simplified car, and communicate with each other using Wi-Fi. UDP Broadcast was chosen as the communication protocol. UDP Broadcast sends a message to every vehicle listening on the network.

II. Security

The proposed implementation of V2V has room to improve. A V2V implementation usable on the market would need to address a few security concerns. Security concerns are outside the scope of the project as we are addressing the lack of implementations covering V2V, but they are still worth mentioning.

A. Packet Security

As our UDP packets are being broadcasted to everyone in the nearby vicinity, an attacker only needs to be located near the network to be considered a "car". This means that anyone could send fake messages or tamper with existing packets. This leaves room for improvement in terms of admitting "cars" on the network, and properly identifying nodes on the network as "car", "adversary", or "miscellaneous" nodes.

Attackers on the network could potentially leverage this limitation to inhibit the flow of traffic by broadcasting that there is some blockade ahead (ToF sensor data shows car ahead, accelerometer data shows there is no/little movement). Attackers could also target individual vehicles with a similar idea. They could send false packets to make the victim vehicle think it has to brake suddenly, potentially crashing with vehicles behind them or causing them to brake too fast. If the victim is carrying a heavy load, such as a large trailer, braking too fast can compromise the stability of their vehicle and potentially swerve out of control or unlatch their trailer.

B. Network Security

A member of the ad-hoc network may be either calibrated to send too many packets or is an attacker. In a case where the packet traffic is too heavy, a denial of service attack (DoS) may occur. This should be addressed as well before V2V is accepted by car manufacturers.

As the network is completely open to new "cars", attackers may be able to probe the network for more vulnerabilities than those discussed. For example, perhaps some UDP misconfiguration could be leveraged to forward UDP packet contents to a CAN bus, or similar idea.

III. V2V Implementation

This section covers our V2V implementation, the features and the mockup.

A. Features

The two vehicles are represented by two ESP32s, see Fig. 1. Although we only implemented two vehicles, our implementation is scalable to allow for more vehicles. Each vehicle possessed a ToF sensor and an accelerometer. The ToF sensor is used to identify whether there is another "vehicle" in front of the ESP32 and the accelerometer is used to know whether the other "vehicle" is moving. On a real vehicle, the CAN bus can be used to monitor and send each vehicle's velocity – and other information as needed, such as GPS for locating where the incoming UDP packet is coming from – in the UDP packet. The ESP32s listen and broadcast messages on UDP port 10000. The current UDP packet we are sending has an ID for the vehicle, the ToF distance, and the accelerometer measurement. On the other vehicle, this information is used to alert the driver via some LEDs. This UDP packet was standardized between vehicles using a defined C struct to contain the relevant information.

Fig. 1. Hardware overview.

B. Hardware

The mockup can be found on Fig. 2. Each breadboard has an ESP32, a power supply, a ToF sensor, and two LEDs. Each could have an accelerometer, but only one "vehicle" had an accelerometer during testing.

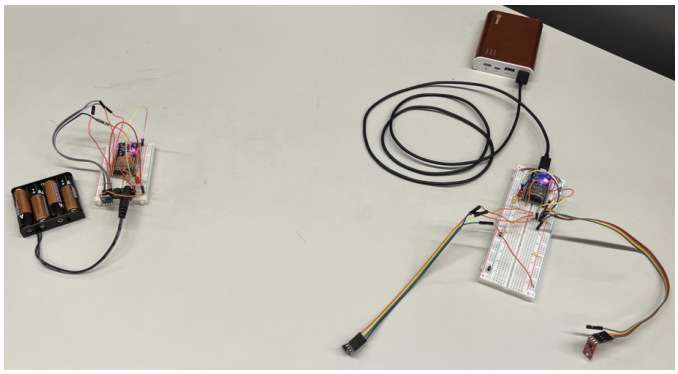

Fig. 2. The mockup used to test V2V, ESP32s are "vehicles".

Close-ups of each "vehicle" can be found in Fig. 3 and Fig. 4. The assembled "vehicles" can be found in Fig. 5 and Fig. 6. They are named "vehicle" B and U, respectively, from now on. B for battery pack and U for USB battery pack.

The driver has two LEDs available in this implementation: a yellow "caution" LED, and a red "warning" LED. The yellow LED turns on when there is a nearby vehicle (less than 100 mm for this experiment) exchanging UDP packets with the driver's vehicle. The red LED turns on in cases where the driver should be more cautious. To simulate this, the red warning LED was turned on in the case that a caution message has been received and the ToF sensor has measured a distance less than or equal to 50 mm.

Two other lights, intended for debugging, were also incorporated into the design. The blue LED onboard the ESP32 was employed to indicate a successful boot and successful Wi-Fi connection between the two ESP32s. The red LED onboard the ESP32 was utilized to monitor the power supply and to ensure the ESP32 was powered on.

Throughout the project's development, several hardware issues were encountered. One of the issues was the original set of ToF sensors not working. This delayed the project and prompted the need for new ToF sensors. Fortunately, this issue was resolved quickly by ordering a new set. The new set did not work perfectly, but this was likely due to the quality

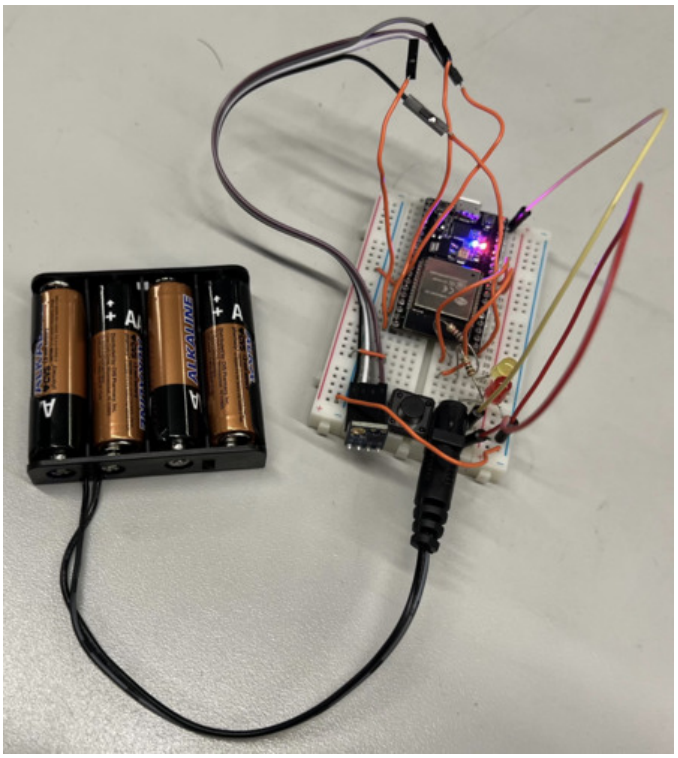

Fig. 3. One of the “vehicles”, vehicle B, used to test our V2V implementation.

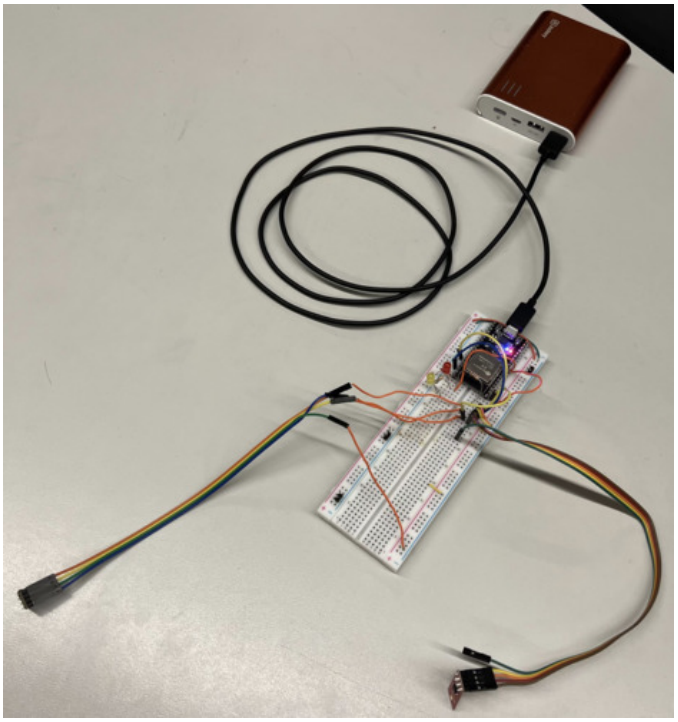

Fig. 4. Another “vehicles”, vehicle U, used to test our V2V implementation.

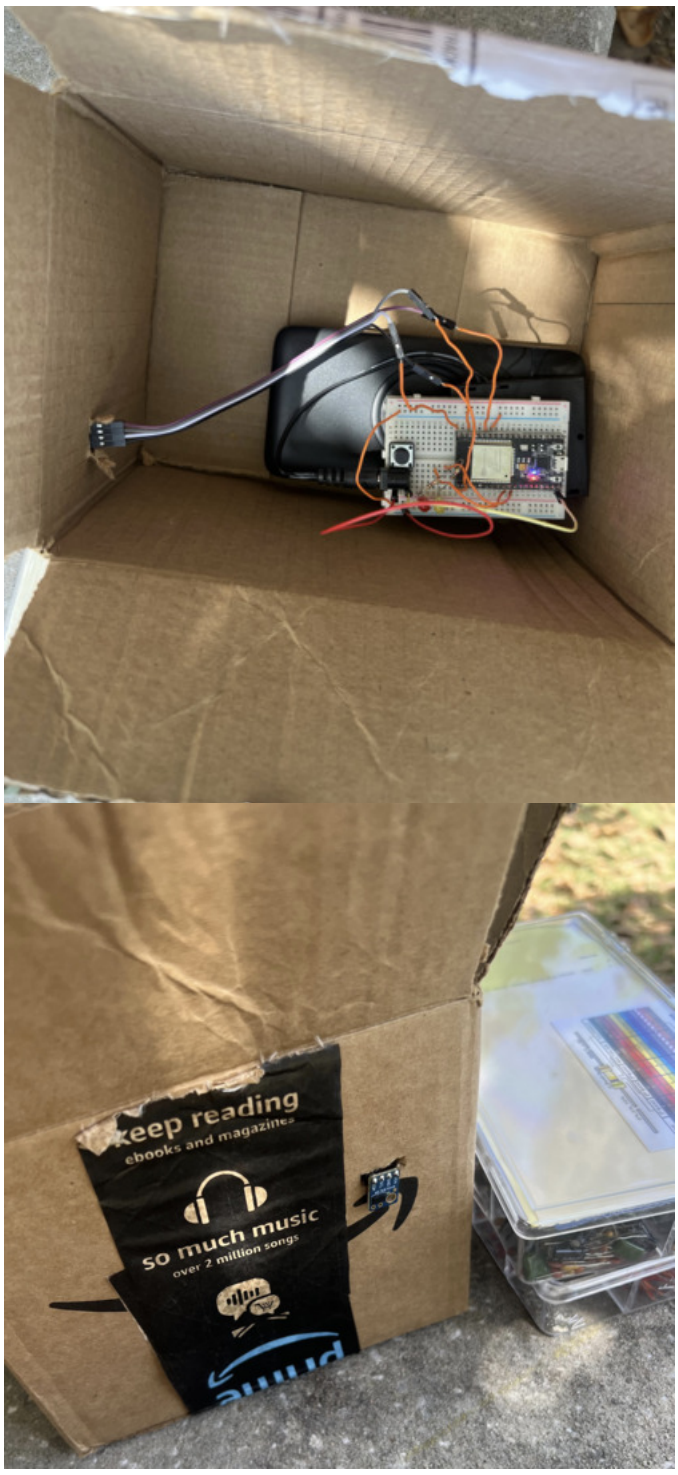

Fig. 5. Assembled “vehicle”, vehicle B, in our testing environment.

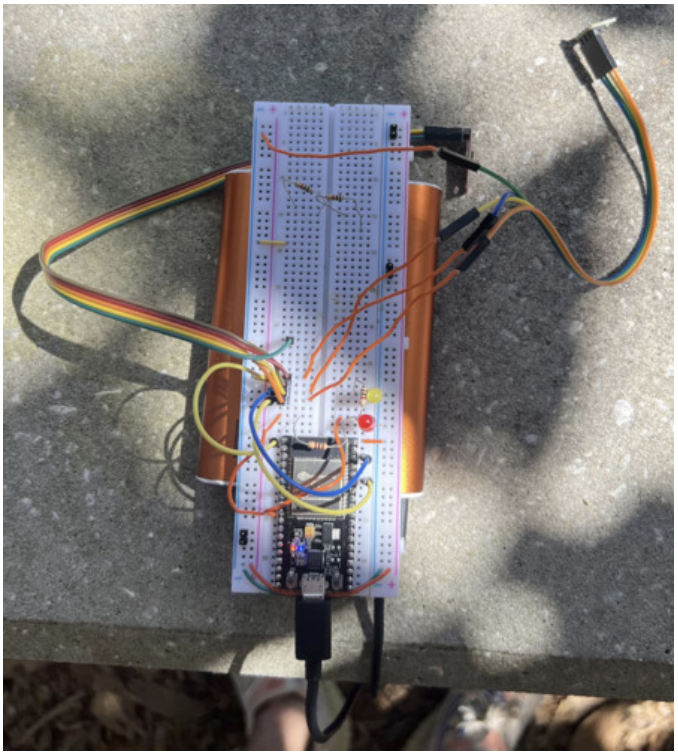

Fig. 6. Another assembled "vehicle", vehicle U, in our testing environment.

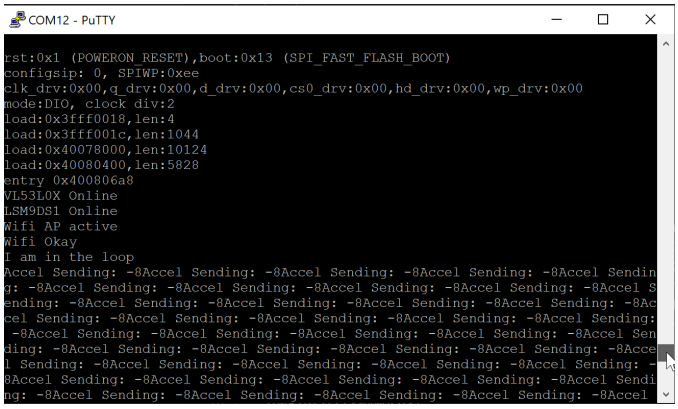

Fig. 7. One "vehicle" is sending a message through UDP.

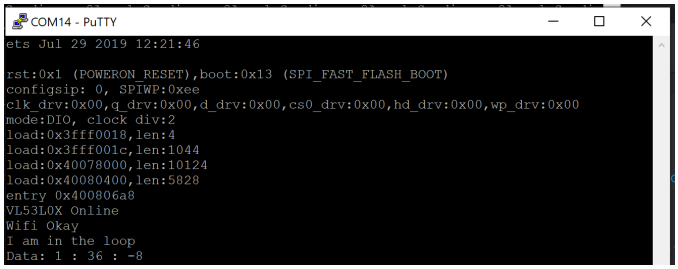

Fig. 8. The other "vehicle" is receiving a message through UDP.

of the components. There were intermittent disconnect issues or sporadic readings, but generally the sensors worked and fulfilled their role in this project. Another issue encountered during testing was power supply issues. Originally, two mobile phone battery banks were to be used to power each ESP32, but the minimal current draw of the ESP32 caused one of the battery banks to switch off. This battery had to be substituted for a battery consisting of four AA batteries in series. This battery provided 6V, and the internal power regulator of the ESP32 was able to step the voltage down to the system's 5V requirement.

IV. Results

The two vehicles were powered independently and in a portable nature. The platoon leader vehicle hosted a Wi-Fi access point, which the subsequent vehicle connected to. ToF data, vehicle status, and accelerometer data was sent between each vehicle and processed accordingly.

The two "vehicles" communicate over UDP with each other. See Fig. 7 to see the "vehicle" sending a UDP packet, and Fig. 8 to see the other "vehicle" receive the UDP packet.

The code for this experiment can be found on GitHub: https://github.com/theriders/V2X_Example

A video demonstration of the experiment can be found on YouTube: https://www.youtube.com/watch?v=WW2k5TiuaQA

V. Conclusion

In this experiment, a V2V network was created using two ESP32 with ToF and accelerometer as a proof-of-concept/base on which car manufacturers may be able to improve and develop on.

While the protocol and protocol security demonstrated in this experiment are to be improved, two "vehicles" successfully communicated and alerted a driver of a possible hazard. Going forward, the protocol can be improved upon and secured to reduce the risk of false messages from adversary cars. In addition, a high-bandwidth band can be selected similar to the 5.9 GHz band previously set aside by the FCC for solely V2X communications. Doing so ensures quick short-range communication, with minimal band crowding.

References

[1] "Vehicle-to-vehicle communication." [Online]. Available: https://www.nhtsa.gov/technology-innovation/vehicle-vehicle-communication

[2] T. Stone, "Haas safety cloud to be enhanced with applied information v2x data," Mar 2023. [Online]. Available: https://www.traffictechnologytoday.com/news/connected-vehicles-infrastructure/haas-safety-cloud-to-be-enhanced-with-applied-information-v2x-data.html

[3] "Safety cloud, cv2x technology that makes roads safer & smarter." [Online]. Available: https://www.haasalert.com/solutions

[4] "The vehicle-to-grid pilot project has been inaugurated at mirafiori," Sep 2020. [Online]. Available: https://www.media.stellantis.com/em-en/e-mobility/press/the-vehicle-to-grid-pilot-project-has-been-inaugurated-at-mirafiori

[5] A. J. Hawkins, "The auto industry lost its spectrum fight with the fcc because v2v was always a fantasy," Aug 2022. [Online]. Available: https://www.theverge.com/2022/8/12/23303191/car-v2v-fcc-spectrum-wifi-court-ruling

[6] J. Young, "Lane departure warning, blind spot detection help drivers avoid trouble." [Online].

Available: https://www.iihs.org/news/detail/stay-within-the-lines-lane-departure-warning-blind-spot-detection-help-drivers-avoid-trouble