2022 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN) | 978-1-6654-7334-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/NFV-SDN56302.2022.9974904

Enabling Cross-Technology Communication to Protect Vulnerable Road Users

Xhulio Limani*, Henrique Cesar Carvalho De Resende†,
Vincent Charpentier†, Johann Marquez-Barja†, and Roberto Riggio*
*Universitá Politecnica delle Marche, Italy;
Email: s1094086@studenti.univpm.it, r.riggio@univpm.it
†University of Antwerp - IMEC, Belgium;
Email: {johann.marquez-barja, henrique.carvalhoderesende, vincent.charpentier}@uantwerpen.be}

***Abstract*—Current research in Cooperative Intelligent Transport System (C-ITS) is focusing mostly on improving the performance of the link layer technology utilized to enable communication between cars or on methods to make traffic more efficient and, most important, safer. Less attention is instead devoted to non-motorized road users such as pedestrians or cyclists which are often addressed as Vulnerable Road Users, or VRUs. In fact, while today it is fair to assume that the vast majority of VRUs are equipped with a smartphones or in general with devices with wireless connectivity, we cannot also assume that such devices are compatible with the variant of the 802.11 standard employed in C-ITS applications known as 802.11p. This is a significant gap in that it prevents critical safety services available to vehicular road users to be extended also to VRUs. In this paper we propose an edge computing-based approach capable of enabling interoperability between 802.11p networks and standard Wi-Fi networks. A technique known as *Beacon stuffing* is utilized to forward such messages to the VRU's mobile devices without requiring them to be associated to any network. The proposed system can be easily integrated into off-the-shelf mobile phones and tablets without requiring any root access to the device. We prototype and test the proposed system over the Smart-highway Testbed deployed in Antwerp, Belgium.**

***Index Terms*—Vulnerable Road User, ITS-G5, Wi-Fi, Interoperability, Beacon stuffing**

I. Introduction

Nowadays most urban and suburban areas are being equipped with Cooperative Intelligent Transport Systems and Services (C-ITS) technologies with the aim of providing different types of road users with a wide range of safety-related applications. Typical examples include emergency brake light, slow of stationary vehicle, in-vehicle speed limits and many more. The most popular communication technology is the 802.11p standard and its successor 802.11bd. The use of cellular technologies (like 5G) is also envisioned as a way to extend service coverage and reliability. Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), or in general Vehicle to Everything (V2X) are just a few examples of models that enable vehicular intercommunication. ITS-G5 [1] is the protocol stack for supporting V2X in an ad-hoc network based on the IEEE 802.11p technology and it is currently the main option for vehicular connectivity.

Within the set of C-ITS applications one of particular social relevance falls into the category generally referred to as Vulnerable Road Users (VRUs). The term VRU is used to refer to *non-motorized road users, such as pedestrians and cyclists as well as motor-cyclists and persons with disabilities or reduced mobility and orientation*. Unfortunately, while cars and road infrastructure are being updated to support the ITS-G5 standard the same cannot been said for the smartphones typically used by most pedestrians and/or cyclists. As a result, while possible in theory, many VRUs equipped with regular smart phone cannot benefits from the safety-related features delivered by an ITS-G5 system.

Edge computing has been envisioned by both the automotive and communications industries as an effective option to offload computational intensive and latency sensitive tasks to servers located in close proximity of the end-users devices. In this paper we leverage edge computing to enable interoperability between ITS-G5 and the standard Wi-Fi technology which equips most end-user devices like phones and tablets. A technique known as *Beacon Stuffing* is used to allow ITS-G5 messages to be dispatched to VRUs. Wi-Fi networks periodically advertise their presence to clients using beacons. The term *Beacon Stuffing* refers to the practice of adding additional information to such beacons with the purpose of making information available to any mobile device, even those that are not associated to any network (the only requirement is that the Wi-Fi interface of the mobile device is active). This approach can be used for providing location based services, e.g., for advertising commercial opportunities, for public safety announcements, or for delivering emergency information. Software-defined networking (SDN) techniques are used to enable selective dispatch of ITS-G5 messages to the Wi-Fi Access Points (AP) in a given area.

The contribution of this work is three fold. First, we present an architecture capable of enabling interoperability between ITS-G5 and Wi-Fi. The proposed design leverage the *Beacon Stuffing* technique to allow timely delivery of ITS-G5 messages to VRUs using standard Wi-Fi APs. Second, we implement a prototype of the envisioned system using off-the-shelf components and widely available open source toolkits. Third, we perform an experimental evaluation showing the capability of out system to deliver in a timely manner the ITS-G5 messages to VRUs without requiring them to be associated to any Wi-Fi network. The tests have been performed over the Smarthighway Testbed deployed in Antwerp, Belgium [2].

The rest of the paper is outlined as follows. Section II discusses the related work. Section III describes the platform

and the proposed message relaying mode. Section IV analyses the system performance. Finally, Sec. V draws the conclusions.

II. Related Work

Over the last decade, many researchers have tried to address the unique communications challenges posed by VRUs. Such attempts can be classified into two broad categories: direct communications and indirect communications.

In the case of direct communications [3], [4], [5], [6], the devices involved in the exchange are smartphones for both pedestrians and vehicles. Communication is often implemented using a technique known as Wi-Fi Beacon Stuffing [7]. This technique allows piggy-back arbitrary information inside Wi-Fi beacons effectively allowing communications between Wi-Fi devices without the need of association. Wi-Fi beacon stuffing can be a valid technique because, as opposed to [5], there is no need for a pre-connection between the devices involved in the communication thus reducing the overall latency. In [3], [4] messages are created starting from data obtained from the smartphone sensors (including GPS) but without following the Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Message (DENM) format prescribed in [8]. In [6] the vehicle and the smartphone communicate using the 802.11p protocol as the smartphone has implemented a Qualcom processor capable of communicating using Dedicated Short-Range Communications (DSRC). However, this technology is not available in today's modern smartphones, and the market trend does not appear to be moving in the direction of supporting it.

In the case of indirect communication, different technologies such as cellular communication (4G or 5G) and ITS-G5 are used. The most commonly used device by VRUs remains the smartphone while inside vehicles dedicated On Board Units (OBU) are used. In [9] the OBUs send CAM and DENM messages to the cellular base station which forwards them to the VRUs. Although the data is processed by an edge server, the communication latency can be very variable and can reach 200ms which can be too high for safety-related use cases. The same considerations apply to [10], where the OBUs sends data to an Road Side Unit (RSU) equipped with an 802.11g Wi-Fi interface and working as a bridge to communicate with the VRU's smartphones. However, in this case association to the AP is required.

In this work we focus on a indirect communication scheme involving an intermediate edge server acting as bridge between ITS-G5 and Wi-Fi. However, as opposed to the aforementioned works, we allow seamless delivery of *standard* CAM/DENM messages from vehicles to VRUs with low latency (below 10ms) and without requiring the end-user to be associated to a particular network. For a more comprehensive coverage on the most recent advances in the field of Software-Defined Vehicular Networks we point the reader to [11].

III. System Design

The reference system architecture of the proposed solution which we name *PowerCam* is depicted in Fig. 1. In this case, vehicular road user such as cars and motorcycles generate CAM and DENM messages in order to signal a road hazard

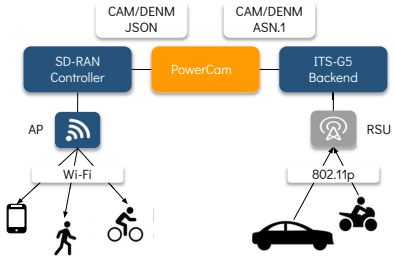


Fig. 1. The *PowerCam* architecture.

or in general an abnormal road condition. Such messages are collected by an 802.11p RSU and dispatched to an ITS-G5 back-end. From here the messages are forwarded to our *PowerCam* module which is executed by nearby edge server. The *PowerCam* translates the CAM/DENM messages received in ASN.1 format into a JSON message and dispatches them to the SD-RAN controller which is in charge of managing the APs in the dispatch area. The SD-RAN controller then triggers one or more beacons stuffed with the CAM/DENM message every time a probe request frame is received by an AP located within a certain distance from the originating RSU. In the rest of this section we will describe in detail the various modules of the *PowerCam* architecture. An overview of the interplay between the various components is reported in Fig. 2. More details will be discussed in Sec. III-E.

A. ITS-G5 Backend, RSU, and OBUs

The *PowerCam* system has been integrated and tested over the Smart Highway [2] testbed in Antwerp, Belgium. The Smart Highway testbed leverages ITS-G5 and C-V2X technologies and supports vehicular communications in real environments enhanced by edge/cloud technologies. The Smart Highway testbed consists of several RSUs deployed along the E313 highway in Belgium and a number of OBU-equipped vehicles. In addition to this, an outdoor lab equipped with development OBUs and RSUs and a test vehicle (a BMW X5) is also available. The outdoor lab has been used for the experimentation reported in this paper.

An OBU is an on-board 802.11p transceiver mounted on a vehicle. It allows for communication with other OBUs or with RSUs. The computer inside a car that collects driving and traffic information can be connected with the OBUs for the purpose of exchanging information with other vehicles or with the road infrastructure. In this study we used a combination of real-world and emulated OBUs. As emulated OBUs we used a software process in order to periodically trigger real CAM messages as if they were generated by a real vehicle. This allowed us to test *PowerCam* in a controlled fashion.

The RSUs are in charge of collecting and sending data from/to vehicles and roadside-infrastructure on the one hand and the backend on the other hand. The utilized RSUs support both ITS-G5 (802.11p) and C-V2X (PC5) interfaces for communication with the vehicles. For this work only the ITS-G5 interface has been utilized. The RSU are also equipped with the Uu interface and can thus support also V2N

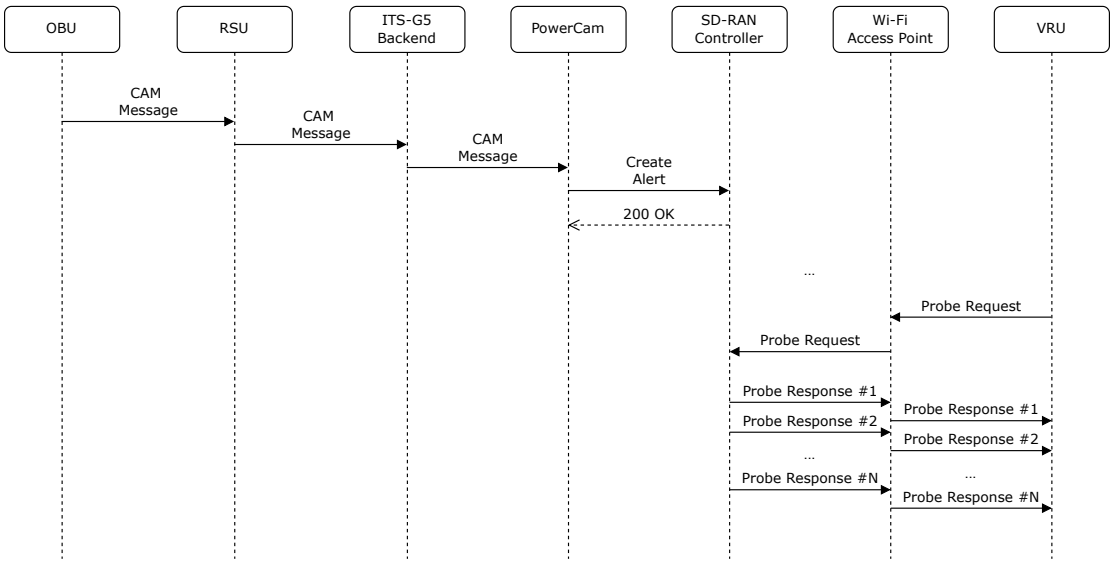


Fig. 2. *PowerCam* message exchanges.

communications. Notice how in the case of emulated OBU also the RSU has been emulated.

The ITS-G5 back-end is in charge of receiving the messages propagated by the RSUs and of storing them effectively making the messages available for secure retrieval by other services (e.g. dashboards, distributed intelligence, etc.) and/or other traffic management platforms. The platform also allows for configurable data propagation from the back-end towards selected (in a geo-aware manner) roadside-infrastructure (e.g., in the case of an accident, the RSU informed of the accident sends this data to the back-end, which in turn deliver it to the RSUs nearby which then notify the vehicles).

CAMINO [12] has been used as ITS-G5 back-end. CAMINO is a vehicular communication management framework incorporating flexible support for both short-range direct and long-range cellular technologies and offers built-in C-ITS services for experimental validation in real-life settings. As for RSUs and OBUs we have used Cohda Wireless [13] products and in particular the MK5 RSU and the MK5 OBU. Both operate in the 5.9 GHz band and support the 802.11p protocol.

B. SD-RAN Controller, Wi-Fi AP, and mobile application

In this work we target a Wi-Fi network implemented following the SD-RAN design principles. As a result a logically centralized controller is in charge of managing a set of Wi-Fi APs. The 5G-EmPOWER platform [14] has been used as SD-RAN controller. 5G-EmPOWER is a flexible, programmable, and open-source SDN platform for heterogeneous RANs (cellular and Wi-Fi).

The 5G-EmPOWER platform builds on an open protocol that abstracts the technology-dependent aspects of the radio access elements, allowing network programmers to deploy complex management tasks as policies on top of a programmable logically centralized controller. The 5G-EmPOWER platform implements a split-MAC architecture where all management frames received by an AP are forwarded to the controller for further processing. The controller has been extended in order to support the concept of *alerts*. The full source code is available under a permissive APACHE 2.0 license[1].

5G-EmPOWER has been extended in order to support the *alert message* concept. An alert message is defined by the following properties:

- A unique identified, a universally unique identifier (UUID) is used for this purpose.
- A message, an arbitrary textual payload to be delivered to VRUs using the Beacon stuffing technique.
- A Time-to-Live (TTL) field, defining for how long (in ms) the message should be broadcasted to VRUs.
- The list of APs to which this message should be broadcasted, this parameter is specified by the *PowerCam*.
- The list of VRU to which this message should be broadcasted, this parameter is essentially the list of VRU that subscribed to the services provided by *PowerCam*.
- A replication factor, the system allows to duplicate the each fragment in order to improve reliability.

Alerts messages are created by the *PowerCam* module using the SD-RAN controller' REST interface. The SD-RAN controller keeps track of the defined alert messages in a dedicated database.

[1]On line resources available at: 5g-empower.github.io

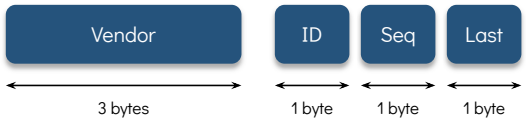


Fig. 3. Message fragment structure.

C. PowerCam

The *PowerCam* sits between the ITS-G5 back-end and the standard Wi-Fi network controlled by an SD-RAN controller. CAM/DENM messages are dispatched by the ITS-G5 back-end to the *PowerCam* module and are translated from their ASN.1 representation to an JSON representation by DUST [15] an embedded proprietary message bus. Once CAM/DENM messages are received their geographical location is checked against the position of the various Wi-Fi APs available in the system. The *PowerCam* then exploits the REST interface of the SD-RAN controller in order to create a series of alert messages. Messages generated by the OBU are to be disseminated only by the AP in close proximity to the RSU that received them. This is due to the fact that, CAM messages are in general meaningful only to VRUs that are near their source. In order to support such use cases our system allows to limit the dissemination of CAM messages only to the Wi-Fi AP that are within a certain distance from the RSU that received the CAM message itself. The dissemination distance is a configurable parameter of the *PowerCam* module. There could be exceptions to this rule for example in the case of emergency vehicles whose arrival should be notified also to VRU that are far away from the vehicle itself.

D. Beacon Stuffing

The Wi-Fi standard defines three main types of frames: control, management, and data. Wi-Fi beacons and probe response frames belongs to the category of management frames and are composed of several fixed and variable length fields. The variable length fields are called information elements (IEs). The 802.11 standard defines a long series of IE some mandatory other are instead vendor specific. One of these is an IE carrying the human readable name of the network called service set identifier (SSID). This IE is capable of transporting 32 bytes of payload. In this paper we broadcast the CAM/DENM data embedded in the SSID IE.

We treat the information carried in the CAM/DENM message as a string of bytes or arbitrary length. However since the maximum length of an SSID is 32 bytes the AP must split the message in smaller chunks and broadcast each chunk inside a separated beacon or probe response message. The CAM/DENM messages encoded in this way need to carry the necessary information to allow proper reconstruction at the VRU's side. For this purpose we use the Basic Service Set ID (BSSID) field present in every Wi-Fi frame. The BSSID is typically the MAC address of the Wi-Fi AP and is encoded as a 6 bytes Ethernet address.

In this work we use a simple way to encode each CAM/DENM fragment. In particular we use the first 3 bytes of the BSSID a special vendor address code which can allow mobile phones to filter out SSIDs that carry a CAM/DENM fragment. Such vendor code should be defined by a suitable standardization agency. Then, as depicted in Fig. 3, we use one byte as unique identifier for the message, one bytes to encode the sequence number, and one byte to carry the information if the chunk in question is the last chunk.

E. Workflow

Figure 2 summarizes the various messages exchanged in the *PowerCam* system using a sequence diagram. In the example, the entire process begins with a CAM message generated by a vehicle's OBU. This could be, for example, a message signaling that an emergency vehicle like an ambulance is approaching or a message signaling a road hazard. The CAM message is dispatched as a broadcast 802.11p frame to all the devices near the vehicle itself. The CAM message is then received by an RSU and forwarded to the ITS-G5 back-end where it is published on a publish/subscribe bus.

The *PowerCam* is configured to subscribe to a series of events on the publish/subscribe bus, among which the reception of a CAM message. When this happens, the *PowerCam* system creates an alert on the SD-RAN controller. The alert carries with the CAM message, an expiration date (to avoid old CAM messages to persist on the system), and the dissemination radius of this message expressed in meters.

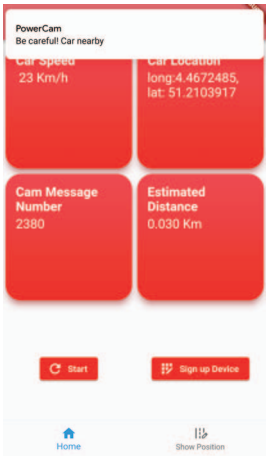
VRUs subscribe to the alert service using the *PowerCam* mobile app. After they are subscribed every probe request message sent by the VRU will be processed by the SD-RAN controller. In particular the SD-RAN controller will check if a regular probe response message should be generated, e.g. for a real Wi-Fi network. In addition to this the SD-RAN controller checks if the probe request message is coming from a VRUs that subscribed to the *PowerCam* platform and if the the Wi-Fi AP that received the probe request message is within a certain radius from the OBU that generated the message (CAM message are geo-localized). If both conditions are verified, then the SD-RAN controller generated a variable number of probe response messages (encoding the CAM message using the mechanism described in the previous section) is generated.

Probe response messages are then dispatched to the VRU mobile phone by the Wi-AP than originally sent the probe request message. An application has been implemented for the Android operating system to gather the various probe response messages and reconstruct the original CAM/DENM message. The application supports various features including a dynamic map which visualize the potential traffic hazards. A screenshot of the *PowerCam* mobile application is shown in Fig. 4

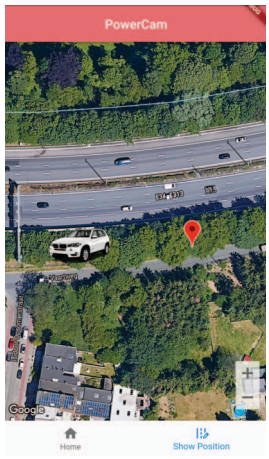
IV. Evaluation

A. Evaluation Methodology

The *PowerCam* system has been validated over a testbed composed of a single RSU installed on the roadside and one OBU installed on a BMW X5 test vehicle. The OBU has been configured to broadcast CAM messages with a frequency of 10Hz. The testbed is equipped with 2 Wi-Fi APs, one close to the RSU and another more distant. The setup is representative



(a) App and notifications.



(b) Map view.

Fig. 4. The *PowerCam* mobile app.

of a metropolitan scenario with RSUs deployed at critical points, e.g., traffic lights, and Wi-Fi hotspots deployed in the same area with the purpose of providing citizens with Internet connectivity. It is assumed that the APs are under the control of an SD-RAN controller which is realistic current managed deployments. We positioned one AP within the dissemination radius of the RSU and one right outside it in order to verify that CAM messages are properly disseminated.

Our evaluation campaign aimed at assessing two main key performance indicators related to CAM message dissemination, namely end-to-end latency and MAC channel utilization. This analysis is conducted for an increasing length of the CAM messages. Measurements have been conducted with this duplication factor varying from 1 to 3. Finally, each measurement has been repeated 10 times and we report as results the average value and the confidence interval.

B. Results

Figure 5 plots the results regarding the end-to-end message delivery latency. This is measured as the interval of time between the probe request is generated by the VRU's terminal and the time all CAM message fragments are successfully received and reassembled at the VRU's terminal. As it can be seen from the plot there is a linear dependency between the end-to-end latency and the message length. This was to be expected in that a longer message requires more *Beacons* to the transmitted. The latency seems also to increase with the number of repetitions. This is due to the fact more repetitions result in a higher communication and reassembly overhead.

We also studied how often the VRUs can transmit probe request frames as this is the trigger for the delivery of the CAM messages. In fact, albeit the *PowerCam* mobile application as been configured to transmit probe requests at the rate of 10Hz we noticed that this setting is not honored by the Android platform. Results of this measurement are plotted in Fig. 6. The reason behind an end-to-end latency higher than 2 seconds is due to the fact that the VRU's mobile phone can send probe requests at a rate of one every two seconds (for battery saving purposes) as a result also the beacons are generated

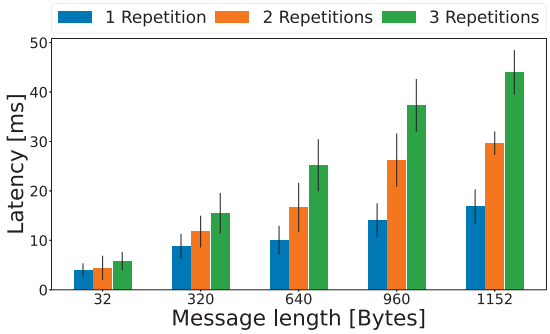


Fig. 5. The end-to-end latency to deliver a single CAM message.

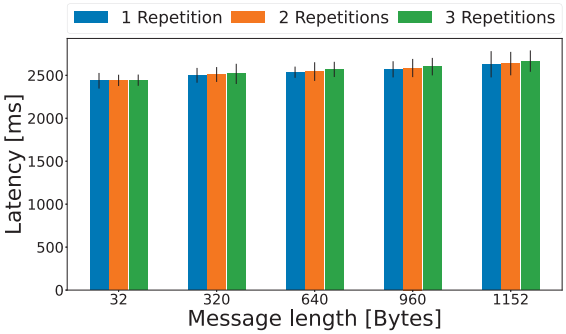


Fig. 6. The end-to-end latency required to deliver a CAM message taking in consideration also the phone probe request rate.

at that frequency. We postulate that if the *PowerCam* mobile application could run at the system level it would be possible to decrease the overall communication latency. Notice that we have also tried to used periodic beacons at the AP instead of probe requests to deliver CAM message but we noticed that, again due to power saving measures, the VRU mobile phone would rarely pick any of those messages, i.e. the phone essentially listed only to probe response messages generated as a result of a probe Request message.

In Fig. 7 we report the bitrate utilized by the *PowerCam* platform. This is the wireless channel capacity utilized to deliver CAM messages to a single VRU. As it can be seen, even in the worst case (longest CAM message and 3 repetitions) the bitrate does not go above 40KBytes/s which is negligible is compared with the current multi-gigabit/s throughput that are available on modern Wi-Fi AP. Given this channel utilization with 1 Mbytes/s it would be possible to support 25 VRU. Moreover, probe responses could be also eavesdropped by other VRUs without requiring further transmissions.

Finally, Fig. 8 reports the battery duration with and without the *PowerCam* app active. Notice that in this graph we plot the time need for the phone to drop from fully charged to 1% of charge. As it can be seen, the *PowerCam* app has a small impact of the battery duration due to the additional probing generated by the app. Consider also that this is a worse case scenario in that every time that a CAM message is generated a notification is triggered on the mobile phone and the screen is turned on. Battery consumption could be reduce

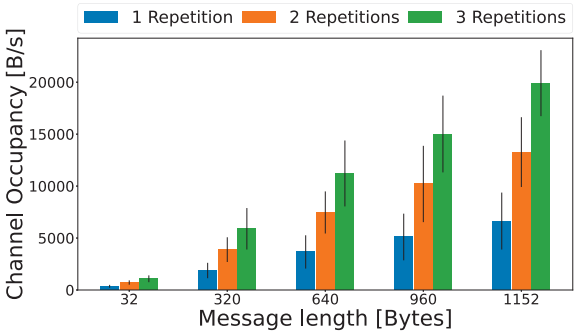


Fig. 7. The overall MAC level bitrate utilized by the *PowerCam* system.

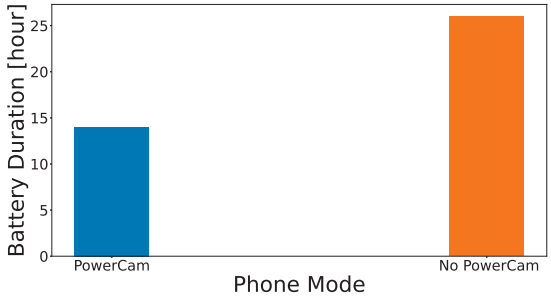


Fig. 8. Battery life with and without *PowerCam*

by for example avoiding turning on the phone screen when the notification is generated.

V. Conclusions

In this paper we have presented *PowerCam* a novel system enabling interoperability between ITS-G5 and standard 802.11 networks. *PowerCam* allows CAM/DENM messages to be delivered to VRUs equipped with standard mobile phones (i.e., without 11p or PC5 support) using a technique known as *Beacon stuffing*. This technique allows for very low bitrate communication between two 802.11 devices without the need for actual association or authentication. The system has been implemented and test over the Smart Highway testbed deployed in Antwerp, Belgium. Results show how the system can provide timely delivery of CAM messages to VRU users.

The system presents also some limitations. In particular due to the way probe request are generated in modern Android-based mobile phones, the end-to-end message dissemination latency is in some specific scenarios above 2s making it suitable only for non-critical messages. In order to address this limitation the *PowerCam* mobile application should be allowed to run as high priority system service providing it with lower level access to the Wi-Fi subsystem in order to allow for higher frequency probing rate. As an alternative the phone could also be configured to proactively listen for standard beacons. The impact that this approach has on battery life is an open point. We plan to address such challenge as part of the future work.

Acknowledgments

This work has been performed in the framework of the European Union's Horizon 2020 project AI@EDGE co-funded by the EU under grant agreement No 825012, within the European Union's Horizon 2020 project 5G-Blueprint with the Grant Agreement No. 952189. It has been also supported by the Flemish Ministry of Mobility and Public Works (MOW) and the regional Agency for Roads and Traffic (AWV), Belgium.

References

[1] 5GAA, "An Assessment of LTE-V2X (PC5) and 802.11p Direct Communications Technologies for Improved Road Safety in the EU," Dec. 2017, White Paper.

[2] Marquez-Barja, J. and Lannoo, Bart and Naudts, Dries and Braem, B. and Donato, C. and Maglogiannis, Vasilis and Mercelis, S. and Berkvens, R. and Hellinckx, P. and Weyn, M. and Moerman, Ingrid and Latré, Steven, "Smart Highway : ITS-G5 and C2VX based testbed for vehicular communications in real environments enhanced by edge/cloud technologies," in *2019 European Conference on Networks and Communications (EuCNC), Abstracts*. IEEE, 2019, p. 2.

[3] K. Dhondge, S. Song, B.-Y. Choi, and H. Park, "Wifihonk: Smartphone-based beacon stuffed wifi car2x-communication system for vulnerable road user safety," in *2014 IEEE 79th Vehicular Technology Conference (VTC Spring)*, 2014, pp. 1–5.

[4] P.-F. Ho and J.-C. Chen, "Wisafe: Wi-fi pedestrian collision avoidance system," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 6, pp. 4564–4578, 2017.

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

[6] A. Tahmasbi-Sarvestani, H. Nourkhiz Mahjoub, Y. P. Fallah, E. Moradi-Pari, and O. Abuchaar, "Implementation and evaluation of a cooperative vehicle-to-pedestrian safety application," *IEEE Intelligent Transportation Systems Magazine*, vol. 9, no. 4, pp. 62–75, 2017.

[7] R. Chandra, J. Padhye, L. Ravindranath, and A. Wolman, "Beacon-stuffing: Wi-fi without associations," in *Eighth IEEE Workshop on Mobile Computing Systems and Applications*, 2007, pp. 53–57.

[8] European Telecommunications Standards Institute (ETSI), *Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition; Release 2* , Std. ETSI TS 103 300, May 2020.

[9] Q.-H. Nguyen, M. Morold, K. David, and F. Dressler, "Car-to-pedestrian communication with mec-support for adaptive safety of vulnerable road users," *Computer Communications*, vol. 150, 11 2019.

[10] D. Thielen, T. Lorenz, M. Hannibal, F. Köster, and J. Plättner, "A feasibility study on a cooperative safety application for cyclists crossing intersections," in *2012 15th International IEEE Conference on Intelligent Transportation Systems*, 2012, pp. 1197–1204.

[11] N. Cardona, E. Coronado, S. Latré, R. Riggio, and J. M. Marquez-Barja, "Software-defined vehicular networking: Opportunities and challenges," *IEEE Access*, vol. 8, pp. 219 971–219 995, 2020.

[12] D. Naudts, V. Maglogiannis, S. A. Hadiwardoyo, D. van den Akker, S. Vanneste, S. Mercelis, P. Hellinckx, B. Lannoo, J. M. Márquez-Barja, and I. Moerman, "Vehicular communication management framework: A flexible hybrid connectivity platform for ccam services," *Future Internet*, vol. 13, p. 81, 2021.

[13] "Cohda wireless." [Online]. Available: https://www.cohdawireless.com/

[14] E. Coronado, S. N. Khan, and R. Riggio, "5G-EmPOWER: A Software-Defined Networking Platform for 5G Radio Access Networks," *IEEE Transactions on Network and Service Management*, vol. 16, no. 2, pp. 715–728, 2019.

[15] S. Vanneste, J. de Hoog, T. Huybrechts, S. Bosmans, R. Eyckerman, M. Sharif, S. Mercelis, and P. Hellinckx, "Distributed uniform streaming framework: An elastic fog computing platform for event stream processing and platform transparency," *Future Internet*, vol. 11, p. 158, 2019.