A Vehicle Collision-Warning System based on Multipeer Connectivity and Off-the-shelf Smart-Devices

Bogdan Groza and Cosmin Briceag

Politehnica University of Timisoara, Romania
Email: bogdan.groza@aut.upt.ro, briceagcosmin@gmail.com

Abstract. Traffic related deaths and injuries take high tolls each year and vehicular collision warning systems can make the future safer. To deploy such systems there are strong efforts from the industry in the development and standardization of Car2X communication technologies, e.g., the 802.11p suite. However, it is unlikely that modern infrastructures will cover all areas of the world and even less likely for all cars to attain communication capabilities in the short term. In this work we study the development of a system that is based on existing off-the-shelf smart-phones and facilitates the creation of ad-hoc networks based on the existing Multipeer technology developed by Apple. This is a non-restrictive approach since similar ad-hoc networking technologies from competitors exists, e.g., WiFi-Direct on Android.

1 Introduction and motivation

As traffic related deaths and injuries take high tolls each year, vehicular collision warning systems may play a crucial role in the future. To give more motivation some data on road safety from the World Health Organization [11] may be useful. The highest death rates are in countries with less developed infrastructure, e.g., Africa, Asia and the Southern Americas. The distribution of traffic casualties by type of road user shows that even in the most developed countries, e.g., the USA or Western Europe, about half of the casualties occur among the drives and passengers of 4-wheeled vehicles. It is thus clear that more research in this direction and faster introduction of such technologies may be beneficial. Nonetheless, the increasing number of reported attacks on vehicular systems [6], [2], [7] may bring adversaries that target traffic safety by manipulating vehicle electronics. This should trigger even more attention toward developing more advanced safety mechanisms.

To deploy Car2X communication, i.e., Car2Car and Car2Infrastructure communication, an appropriate network infrastructure is needed. Recently emerged standards, such as the 802.11p, are a proof of the continuous development efforts by the industry. Still, it is unlikely that this infrastructure will quickly cover all areas worldwide and it is hard to forecast an extensive use of modern vehicular communication technologies in less developed parts of the world (this is easier to project for smartphones which are cheap and available everywhere). Moreover, it is also unlikely for all cars to be equipped with such systems in the short run since cars commonly have lifespans of a decade or more.

Motivated by these, we study the development of a system that is based on existing off-the-shelf iPhones that facilitate the creation of ad-hoc networks based on an

existing communication layer, i.e., Multipeer. While this technology is present in all Apple products, alternatives exists for Windows and Android based devices with ad-hoc networking technologies such as WifiDirect. Thus, our proposal is not restricted to the iOS share of the market. We experiment with iPhones only for convenience, but the concepts are general. Mobile phones are cheap and ubiquitous devices while similar capabilities are expressed by after-market infotainment units which are a popular choice among consumers for upgrading older vehicles. Such items cost in the order of several hundred euros and are affordable for most users. Also, they will become even cheaper as production increases. While such gadgets become ubiquitous, the challenge remains in designing suitable solutions. There are numerous constraints both from the existing communication layers, e.g., an ad-hoc networking layer is needed, and also from the computational capabilities of the device. Nonetheless, delays are crucial and the implementation of security mechanisms, which is mandatory for making the solution suitable for real-world needs, comes at a cost. We discuss all these aspects in the forthcoming sections.

1.1 Related work

A survey on security implications and requirements for Car2X communications can be found in [9]. In our system we do account for basic security objectives such as authentication and cope with real-time needs. Wi-Fi Direct as a communication layer has been previously used for warning systems to avoid collisions with pedestrians and bicyclists in [4]. We believe that the range of Wi-Fi or of the related Multipeer technology, i.e., up to 200m, is also sufficient for deploying ad-hoc vehicle networks and help in preventing collisions. Another system for collision signaling and avoidance is discussed in [3]. Trajectory predictions has been previously explored by the use of visual information, a survey can be found in [8]. However, the use of visual information requires more demanding algorithms for image processing that we find to be unsuitable for our application setup (image processing requires too much computational time and can also drain the phone's battery). Such algorithms may be of interest as future work in order to coroborate between existing GPS data and also to spot potential malicious reports that contradict visual evidence. A more recent work in [10] provides and excellent survey over intersection monitoring and algorithms for predicting vehicle behaviour. This provides useful information for one of our target scenarios, i.e., a crossroad. In [5] some models are provided for estimating the effectiveness of V2X systems in preventing collisions (in the forthcoming section we briefly discuss the effectiveness of our approach on similar metrics/scenarios).

2 Addressed scenarios and constraints

We first discuss on the setup that we address by presenting two relevant scenarios. We also elaborate on the impact of delays which are the most significant constraint of our problem.

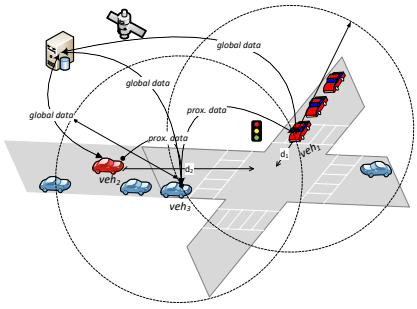

Fig. 1. A vehicle intersection scenario

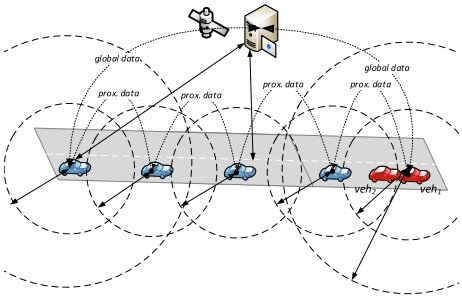

Fig. 2. A highway lane based scenario

2.1 Addressed scenarios

While we generally target any traffic related scenario, we do theoretically analyze the effectiveness of the mechanism on two target settings: an intersection as depicted in Figure 1 and a highway as depicted in Figure 2. These scenarios are useful for assessing the effectiveness of the mechanism (which translates in the number of collisions that can be avoided). Nonetheless, these scenarios provide two of the most prevalent practical setups as crossroads and highways are a common place for vehicle crashes. We now give some metrics on how a collision warning system may help in these scenarios.

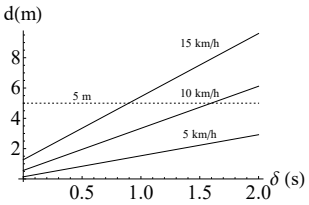

Fig. 3. Braking distance at 0–2s for speeds of 5, 10 and 15 km/h

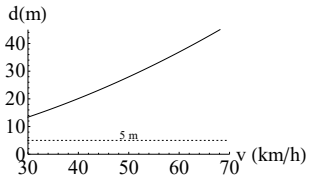

Fig. 4. Braking distance in 1s reaction for speed 3–70km/h

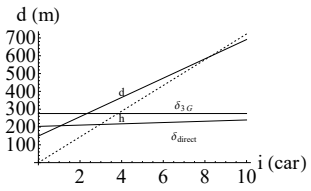

Fig. 5. Case of the i-th vehicle on the highway lane

Crossroad. For the vehicle crossroad, we consider that the column starting with vehicle veh_1 is departing at green light while vehicle veh_2 is speeding up to takeover the other cars without noticing the red light. The braking distance can be easily computed as: $d = v^2/(2\mu g) + 1.5v$. Here $1.5s$ is the driver reaction time and is a standard value in traffic modelling (reaction time may get under $1s$ or increase over $2s$ depending on driver experience, age, etc.). To provide some hints on the braking distance due to reaction time, in Figure 3 we show the braking distance due to a reaction time of $2s$ at various speeds 5, 10 and $15km/h$ and in Figure 4 the braking distance at 1s given a speed from 30 to $70km/h$. As depicted in Figure 3, for a vehicle departing at green light, assuming reaction time of $1.5s$ and and a speed of at most 10 km/h, the

braking distance d_1 stays in the order of several meters and is below a reasonable $5m$ to the center of the intersection. For the second vehicle however, the braking distance d_2 may be well above $30m$ even at speed of around $50km/h$. Vehicle veh_3 may easily beacon both vehicles veh_1 and veh_2 to signal the potential collision and thus it can be prevented. This happens because signalling will take several hundred milliseconds added to driver's reaction time which lead to a under $2s$ response time. According to Figure 3 the driver of veh_1 could still stop in the $5m$ to the center of the intersection if his speed is around $10km/h$ (this is realistic for a car departing at green light).

Highway lane. Figure 2 depicts a scenario where a potential chain-collision between vehicles may take place. We assume that for some reason vehicle veh_1 slows down and veh_2 collides with it due to insufficient distance. In the light of this event, we analyze the impact of a chain-collision due to poor reaction of the rest of the drivers from the lane. The distance between the i-th car in the formation and the front car is ib where b is the recommended 2-second distance between vehicles (at 130 km/h we have $b = 72m$). The braking distance of the i-th vehicle accounts for the time of the driver to react, that is: $d(i) = 1.5iv + v^2/(2\mu g)$. From Figure 5 it is easy to see that only vehicle 8 may have sufficient distance to stop until the collision point. However, in case of Multipeer/WiFi-Direct the delay of $1.5i$ becomes $\delta_{direct} = 1.5 + 0.1i$ (which considers the driver reaction time and a $100s$ propagation delay between each car) and for 3G considering a 2s delay δ_{3G} the 3-rd car may stop within safe distance. Consequently, both Multipeer/WiFi-Direct and 3G significantly reduce the number of cars from 7 to 3.

3 Setup and results

3.1 Practical considerations and addressed setup

Having in mind the required periodicity of 1 status message every 100 milli-seconds [9], each vehicle will need to be able to sign/authenticate 10 messages each second for its position alone. In addition, the vehicle must receive and verify messages from the other participants. It is uneasy to estimate the exact number of messages to be verified each second since this is highly dependent on the concrete scenario, but current research places the number of messages that needs to be verified from several hundreds up to 5000 [9].

This leads to a high amount of signing and verification operations each second and we need to adjust to these needs. Since verification is done more often than signing, RSA seems to be a natural choice due to its higher verification speed. In Table 1 we give some computational timings (in milliseconds) for hash functions and in Table 2 for RSA on an iPhone 6s. The computational time is short-enough for allowing the requested 5000 signature verifications/second and 10 signatures. Similar collision warning systems, e.g., WiFiHonk [4], do not implement security mechanisms but we believe that the lack of security is not desirable.

We choose to separate between location and authentication data which allows more flexibility in choosing to use (which we recommend) or ignore the authentication data. This leads to a frame having the structure suggested in Figure 6. The location frame

Table 1. Computational overhead for authentication tags

Function	Time (ms) for input size (bytes)					
	16	32	64	128	256	512
HMAC-SHA1	0.015	0.002	0.001	0.001	0.001	0.004
HMAC-SHA256	0.004	0.001	0.002	0.001	0.001	0.001

Table 2. Computation time for signing and verification

Function	Time (ms) for input size (bytes)					
	16	32	64	128	256	512
RSA-1024 Sign	1.713	1.698	1.843	1.875	1.730	1.713
RSA-1024 Verify	0.044	0.045	0.044	0.044	0.044	0.045

in Figure 6 (i) starts with the length of the frame, followed by the ID of the sender, a fixed value set to 0x00h, a timestamp, current vehicle location. The ID of the other participants follows along with their location. In the authentication frames from Figure 6 (ii) we start again with frame length, sender ID, a fixed value 0xFF to separate from location frames, a timestamp and a signature. Then short Message Authentication Codes (MAC) follow to authenticate data for short-range peers. Moreover, authentication data includes both digital signatures as well as faster MACs which can be used for short-range peers.

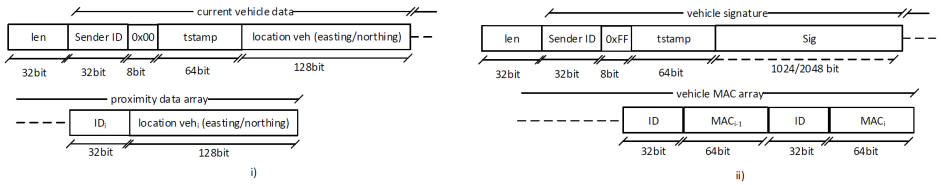

Fig. 6. Structure of location frames (i) and authentication frames (ii)

To save some computational time one can prefer a MAC-based solution but this would require a secret key that is shared between participants. We believe that such a solution may be preferable whenever vehicles clusters are formed, e.g., on a highway. From a security perspective this simply requires an authenticated key-exchange protocol for sharing the key. Coming up with a new authentication protocol per paper is not desirable since it is known that authentication protocols are prone to subtle security flaws. The automotive domain is industry driven and the industry targets standardized solutions which makes it preferable to stay closer to standards. The work in [1] did a careful analysis by formal verification of ISO standardized protocols for key agreement and recommended several fixes. Such protocols can be safely used for sharing keys between two vehicles. Besides these we do of course recommend that the 3G/4G communication with the server is done inside a SSL/TLS channel which is again a standard solution for remote connectivity.

3.2 Implementation and experiments

The multipeer framework makes the physical transport of data transparent, i.e., switching between both Wi-Fi and Bluetooth. Indeed, once connected over Bluetooth, the range of collision prediction becomes lower than Wi-Fi and thus Wi-Fi is preferable.

Connectivity with the server is maintained via 3G and Multipeer facilitates direct connection between 2 peers as soon as they are in close range. According to the documentation up to 8 peers can be connected by Multipeer with rapid switching between these connections.

The development environments that helped us to develop a proof of concept were numerous. Amongst the most used tools were Xcode 8.0 which helped us to design and to implement the application deployed later on iPhone. We also made use of Eclipse CDT which allowed us to implement the server application. The hardware that we used consists in two iPhones (4s respectively 6s), one of them running iOS 9.3 and the other one running iOS 10.3.

Having in mind the requirements for a system able to accomplish V2x communication, we designed two redundant mechanisms in order to eliminate any dead time that could occur during a transmission initiated by one peer and disconnected by an interference. On one side, we have the Multipeer framework which makes possible advertising (broadcast a service to the other traffic participants) and browsing (finding services put by other traffic participants) in the same time without the need of an Access Point.

On the left side of Figure 7 we present the flowchart of the client application which begins with a fork from which all the others components start. The iOS application is broken into three main blocks: *Location Updater*, *LTE Handler* and *MP Handler*. Each of these has a well established purpose that is suggested by its: updating the location of the vehicle, handler the LTE or the Multipeer connectivity. The Location Updater updates the coordinates of the current location and converts them from Latitude/Longitude to Easting/Northing since it is more convenient to use such coordinates in 2D Cartesian system. The second one, is specialized in handling both incoming and outgoing packets by LTE, it connects to the server then sends and receives frames. The third block handles the Multipeer connections. The application starts by advertising and browsing for nearby peers. In advertising mode, it exposes v2x-service to other peers and it is waiting for incoming invitations. Once the invitation has arrived, the application checks for its signature and it accepts or denies the invitation. In browsing mode, the application is looking for nearby services. Once found, it sends an invitation for connection and if the invitation was accepted, it starts to send data. The right side of Figure 7 depicts the server application which takes the incoming frames from the clients and sends back all the neighbors in a range of 200 meters. The server is used for data transfer in LTE mode when the Multipeer connection is not available. The server application starts its life cycle listening on a local port which is set to 5555. For experimental purposes we used port forwarding mechanisms allowing us to run the server on a local machine without the need of having a registered domain. The previously suggested structure for location and authentication frames, i.e., from Figure 6, can be used for data sent between devices, i.e., by Multipeer connectivity, or received by devices from the server, i.e., by 3G connectivity.

We now discuss experimental results. First, in Figure 8 we show the trace for two moving persons. We chose this, rather then recording the trace of two cars, to get more flexibility in testing the application. As the individuals approac each other the blue dots on the plot mark a collision warning reported by the application. Secondly, Figure 9 depicts a trace for two moving vehicles. For safety, we run this while two vehicles were

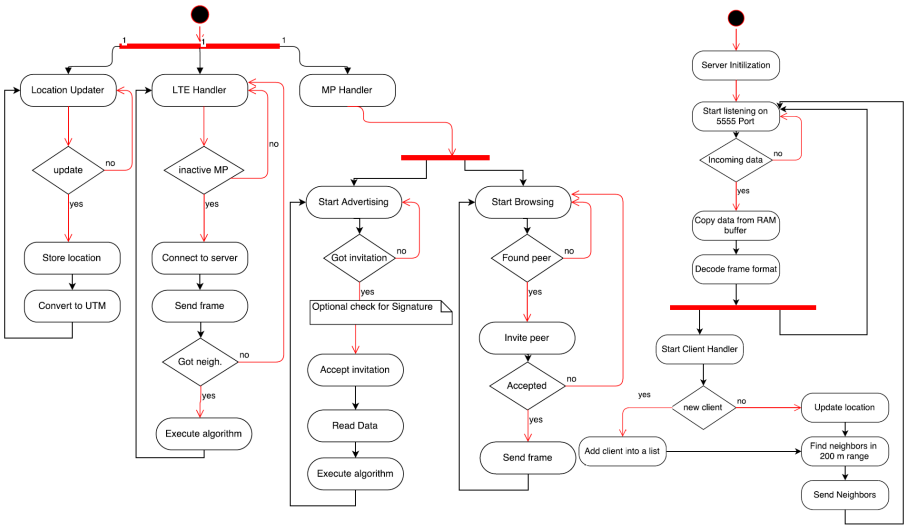

Fig. 7. Flowchart of client (left) and server (right) applications

moving inside a parking lot. Again the application correctly identifies and signals a potential collision that is marked by red dots. Based on experiments, the accuracy of the GPS localization was very good reaching at around 1m in some situations which is excellent for our application.

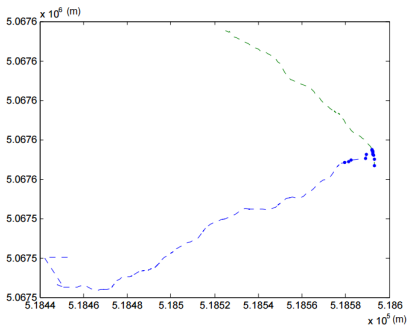

Fig. 8. Trace for two individuals with iPhones

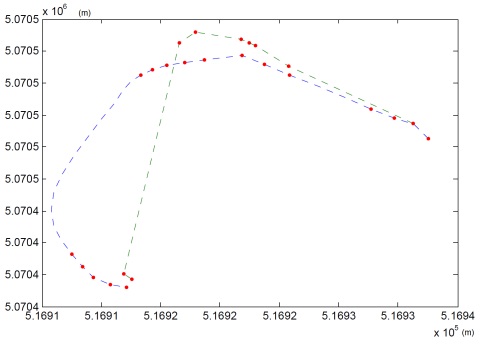

Fig. 9. Trace for two cars with iPhones

4 Conclusion

Our practical deployment and experiments showed that collision-warning systems based on smart-phones can be an effective technology. In this work we only explored the pro-

posal as a concept, showing key advantages of such a solution and proving that it can be implemented in practice. Our results so far rely only on small scale experiments but we believe that a real-world deployment of such applications while challenging it is still within reach. This would require large-scale simulation/experiments, formal verification of the security suite, interest from car owners and nonetheless cooperation from the industry. We may pursue such direction as future work.

Acknowledgement. This work was supported by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS-UEFISCDI, project number PN-II-RU-TE-2014-4-1501 (2015-2017).

References

1. D. Basin, C. Cremers, and S. Meier. Provably repairing the ISO/IEC 9798 standard for entity authentication. *Journal of Computer Security*, 21(6):817–846, 2013.
2. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*. San Francisco, 2011.
3. L.-W. Chen and P.-C. Chou. Big-cca: Beacon-less, infrastructure-less, and gps-less cooperative collision avoidance based on vehicular sensor networks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 46(11):1518–1528, 2016.
4. 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 *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*, pages 1–5. IEEE, 2014.
5. S. Joerer, M. Segata, B. Bloessl, R. L. Cigno, C. Sommer, and F. Dressler. To crash or not to crash: Estimating its likelihood and potentials of beacon-based ivc systems. In *Vehicular Networking Conference (VNC), 2012 IEEE*, pages 25–32. IEEE, 2012.
6. K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010.
7. C. Miller and C. Valasek. A survey of remote automotive attack surfaces. *Black Hat USA*, 2014.
8. B. T. Morris and M. M. Trivedi. A survey of vision-based trajectory learning and analysis for surveillance. *IEEE transactions on circuits and systems for video technology*, 18(8):1114–1127, 2008.
9. T. Schütze. Automotive security: Cryptography for Car2X communication. In *Embedded World Conference*, volume 3, 2011.
10. M. S. Shirazi and B. T. Morris. Looking at intersections: A survey of intersection monitoring, behavior and safety analysis of recent studies. *IEEE Transactions on Intelligent Transportation Systems*, 18(1):4–24, 2017.
11. World Health Organization. Road traffic deaths, http://www.who.int/gho/road_safety/mortality/en/. Technical report, 2013.