3-9-2022

Establishing Trust in Vehicle-to-Vehicle Coordination: A Sensor Fusion Approach

Jakob Veselsky
Loyola University Chicago

Jack West
Loyola University Chicago

Isaac Ahlgren
Loyola University Chicago

George K. Thiruvathukal
Loyola University Chicago, gkt@cs.luc.edu

Neil Klingensmith
Loyola University Chicago, nklingensmith@luc.edu

See next page for additional authors

Recommended Citation

Jakob Veselsky, Jack West, Isaac Ahlgren, George K. Thiruvathukal, Neil Klingensmith, Abhinav Goel, Wenxin Jiang, James C. Davis, Kyuin Lee, and Younghyun Kim. 2022. Establishing trust in vehicle-to-vehicle coordination: a sensor fusion approach. In Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications (HotMobile '22). Association for Computing Machinery, New York, NY, USA, 128. DOI:https://doi.org/10.1145/3508396.3517075

Poster: Establishing Trust in Vehicle-to-Vehicle Coordination: A Sensor Fusion Approach

Jakob Veselsky, Jack West, Isaac Ahlgren, George K. Thiruvathukal, and Neil Klingensmith
Loyola University Chicago

Abhinav Goel, Wenxin Jiang, and James C. Davis
Purdue University

Kyuin Lee and Younghyun Kim
University of Wisconsin–Madison

EXTENDED ABSTRACT

As we add more autonomous and semi-autonomous vehicles (AVs) to our roads, their effects on passenger and pedestrian safety are becoming more important. Despite extensive testing, AVs do not always identify roadway hazards. Failures in object recognition components have already led to several fatal collisions, e.g. as a result of faults in sensors, software, or vantage point. Although a particular AV may fail, there is an untapped pool of information held by *other* AVs in the vicinity that could be used to identify roadway hazards before they present a safety threat.

Consider the scenario depicted in Figure 1: *A vehicle (③) on a side street stops at an intersection. The vehicle needs to turn into the main road, but parked cars and trees occlude the cross traffic. Other vehicles (① and ②) on the busy road have a clear view of traffic conditions, and they could alert vehicle ③) when it is (un)safe to turn.*

If the occlusions in the roadway are too large, vehicle ② may be invisible to vehicle ③. It would be dangerous to begin the turn immediately after vehicle ① passes. Driving situations like these are common. They could be prevented with coordination. But even simple AV coordination—in the scenario, vehicle ② broadcasting its position and velocity to vehicle ③—requires some reliable method to establish trust.

Enabling *coordination* between untrusting AVs is a significant challenge. Because AVs are safety-critical systems, they cannot make decisions based on data from untrusted external sources. Existing vehicle-to-vehicle (V2V) standards lack a workable trust scheme for vehicles and the data they share.

As a first step toward enabling AV coordination, we need a mechanism by which AVs can establish mutual trust. Existing V2V coordination standards like DSRC[2], C-V2X[1], and WAVE[3] rely on a public key infrastructure to authenticate the source of transmissions. But AVs may not always be able to rely on a centralized trust broker, e.g., when in areas with spotty cellular coverage. Since we know that the most prevalent class of attack on cyber-physical systems involves a physically remote attacker, our threat model addresses adversaries that do not know the current location of two vehicles attempting authentication.

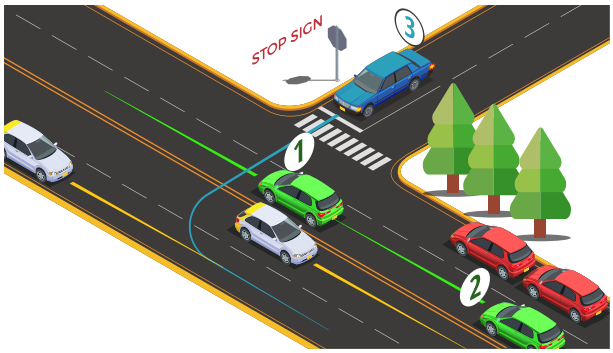

Figure 1: Vehicles in the roadway gathering visual data from objects. The keys they generate will be based on overlapping observations of moving objects.

The algorithm we propose is designed with sensor-fusion for mobile trust establishment, which combines GPS and visual data. The data is collected using the GlobalSat BU-353-24 USB GPS and Microsoft Kinect V2 which are connected to a Nvidia Jetson board. The visual data is then segmented into clusters using the DBSCAN clustering algorithm. Using the mean of depth values from each point in a cluster we can extract a centroid; with this centroid we can estimate the GPS coordinates of the cluster.

After the estimated GPS coordinate is determined we apply our fuzzy key agreement scheme. Our scheme generates a circle of a select radius around each centroid and arbitrarily picks points within the circle. These points are then hashed using an efficient elliptic curve algorithm which allows for increased randomness and secure 1024-bit numbers. We show that keys are truly random by passing all but one NIST test for randomness and sets of keys attain an 80% key agreement rate when the radius of the circle is ten meters with an error between two different centroid of five meters.

REFERENCES

[1] ETSI. 2017. Service requirements for V2X services.
[2] John B. Kenney. 2011. Dedicated Short-Range Communications (DSRC) Standards in the United States. *Proc. IEEE* 99, 7 (2011), 1162–1182. https://doi.org/10.1109/JPROC.2011.2132790
[3] Yunxin (Jeff) Li. 2012. An Overview of the DSRC/WAVE Technology. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, Xi Zhang and Daji Qiao (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 544–558.

HotMobile '22, March 9–10, 2022, Tempe, AZ, USA

ACM ISBN 978-1-4503-9218-1/22/03.
https://doi.org/10.1145/3508396.3517075