Convoy: Physical Context Verification for Vehicle Platoon Admission

Jun Han, Madhumitha Harishankar, Xiao Wang, Albert Jin Chung, and Patrick Tague
Carnegie Mellon University
firstname.lastname@sv.cmu.edu

With the advances in the Internet-of-Things (IoT) technologies, vehicular industries are also quickly migrating to produce smart vehicles. Of these migrations, *vehicle platooning* is an emerging technology that is achieving large traction today [4]. Vehicle platooning is a single file formation driving, where cars follow the preceding vehicle, ultimately the leading vehicle. Platooning is getting significant attention in the commercial trucking industry [1] as it provides benefits of increase in driving safety, convenience, and fuel and road efficiency (due to reduced aerodynamic drags).

Vehicles in the platoon send and receive control messages such as acceleration, braking, and steering information to enable the coordinated driving. Vehicle platooning uses Dedicated Short-Range Communications (DSRC) and Wireless Access in Vehicular Environments (WAVE) as de facto standards for vehicle-to-vehicle (V2V) communications [3]. The current DSRC/WAVE model assumes Public Key Infrastructure (PKI) that authenticates each vehicle's public key by leveraging certificates signed by a trusted third party, such as a Certificate Authority (CA). Unfortunately, this model is susceptible to impersonation attacks such as masquerading or sybil attacks (impersonating as non-existing or "ghost vehicles") [2].

A platooning system that does not bind their *locality* information together with the corresponding *physical identity* and *public key* is critically flawed. Merely verifying the digital certificate has limitations as certificates only serve to bind a vehicle's physical identity (e.g., license plate) to a digital identity, but cannot associate this with the relative physical presence of the vehicle. Even though the certificate of the vehicles may contain their identifiers, other cars in the platoon have no way of verifying vehicles' physical context. We depict an example scenario in Figure 1. *Cars A* and *B* depict vehicles already in an existing platoon, and *Car C* depict a legitimate vehicle wishing to join the platoon, while *Car M* is an attacker's car. Both *Car C and M* hold valid certificate from a trusted CA. Platooning vehicles (*Cars A* and *B*) receive the certificates from both *Cars C* and *M*, but have no adequate method of associating the certificates with the actual car that is behind the platoon.

To address the aforementioned problem, we present *Convoy*, which helps platooning vehicles authenticate and verify their physical context. *Convoy* makes use of accelerometer readings that captures the road and traffic conditions, and leverages them as sources of entropy to establish a symmetric cryptographic key between the vehicles, eventually used to authenticate the digital certificates.

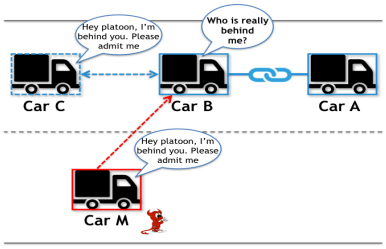

Figure 1: Potential vulnerability of current platooning system which do not provide binding of locality information

We face many challenges in designing such solution. First, even legitimate vehicles in a platoon formation (e.g., *Cars A, B, and C*) would produce similar but unequal signals. We leverage *Fuzzy Commitment* that leverages error-correcting codes to establish a symmetric key from the similar but unequal signals. Second, *Convoy* requires sufficient differences between the accelerometer readings captured from cars across adjacent lanes to guarantee a secure platoon admission. Hence, we design a *Convoy* protocol that requires cars to repeat the context verification protocol multiple times, thereby increasing the confidence over time.

We evaluate *Convoy* by driving a total of 48 miles on a highway spanning over six miles with two distinct vehicles cruising at 65 mph. For data collection, we installed a triple axis accelerometer inside the trunk. From our preliminary experiments, we successfully demonstrate that *Convoy* is able to sufficiently differentiate cars driving on same lanes (even across distinct cars) against adjacent lanes (even across multiple drives of same car).

We plan to extend our empirical study by conducting experiments with longer segments as well as with various traffic conditions. Furthermore, we plan to present solutions and empirical results to thwart potential replay attacks.

1. REFERENCES

[1] European Truck Platooning Challenge – Creating Next Generation Mobility. https://www.eutruckplatooning.com/home/default.aspx, 2016.
[2] N. Bissmeyer, J. Njeukam, J. Petit, and K. M. Bayarou. Central misbehavior evaluation for vanets based on mobility data plausibility. In *ACM VANET*, 2012.
[3] Y. J. Li. *Quality, Reliability, Security and Robustness in Heterogeneous Networks*, chapter An Overview of the DSRC/WAVE Technology. 2012.
[4] Will Knight. 10-4, Good Computer: Automated System Lets Trucks Convoy as One. MIT Technology Review, May 2014.