March 2020

SECURING CONNECTED AND AUTONOMOUS ELECTRIC VEHICLE (CAEV) FLEETS BY ENFORCING AUTHORIZED CHARGING

Yaron Sella

SECURING CONNECTED AND AUTONOMOUS ELECTRIC VEHICLE (CAEV) FLEETS BY ENFORCING AUTHORIZED CHARGING

AUTHOR:
Yaron Sella

ABSTRACT

Provided herein are techniques for using charging events of connected, autonomous and electric vehicles (CAEVs) as an enforcement point in which an owner/operator of a vehicle gives authorization to the vehicle to proceed with the charging, and hence continue operating normally. Such techniques can be utilized for fleets of CAEVs.

DETAILED DESCRIPTION

The automotive industry is undergoing several major developments simultaneously: connectivity, electrification, and autonomous driving. These changes are at different maturity levels and each of them is occurring at its own pace. However, it is forecast that together these changes will reshape the mobility landscape. One common prediction involves the emergence of large fleets of connected, autonomous and electric vehicles (CAEVs) that people can utilize on-demand, similar to current taxicab or ride share services.

When this future is realized, the owners and operators of CAEV fleets will need to protect them. While taxicabs today might be subject to stealing or plain vandalism, for most people, the presence of a driver is a deterrent. Autonomous vehicles, however, have no driver.

Proposed herein is a solution that can be utilized to significantly deter people from stealing CAEVs. Refueling internal combustion engine (ICE) vehicles is a relatively simple process since, essentially, one refills the gasoline tank of a vehicle with liquid fuel, which typically takes just a few minutes. In contrast, charging the battery of an electric vehicle is slightly more involved. This is because lithium-ion batteries are quite sensitive to charging conditions. They typically cannot accept overcharging or trickle charging. Prolonged charging at too high a voltage can even cause the lithium-ion cells to catch fire,

so safety devices must interrupt charging in such instances. Additionally, charging to less than a full charge (say 80%) is recommended, as it prolongs the life of the battery.

Protocols have been developed that provide for an On Board Charger (OBC) to continuously update a charging station with the battery state. Charging also takes significantly longer than refueling.

The battery in an electric vehicle is the single most expensive element of the car. It is obviously an essential part, because without it the vehicle cannot move. Since the battery is large and heavy, for stability reasons, its installation is typically spread across the entire bottom part of a vehicle. All of these factors make the battery for a CAEV a critical component that is not easily accessible or replaceable.

Techniques herein provide for utilizing the hi-tech nature of electric vehicle (EV) charging as an enforcement point to deter theft. That is, whenever an EV needs to recharge, it must receive explicit permission to do so from an authorized party. In the case of a vehicle fleet, the authorizing party would be the fleet owner or operator.

Such techniques may be implemented as follows: when a vehicle connects to a charging station, it can send its Vehicle Identification Number (VIN) plus a random challenge. In response, the authorized party signs the VIN plus random challenge combination using a strong cryptographic Public-key (PK) signature. Finally, the vehicle verifies the signature, and if the signature is OK, the vehicle proceeds to charge the battery. In some instance, other information such as date, time, etc. may be utilized in the process. Figure 1, below illustrates example details that may be associated with this theft deterrent technique.

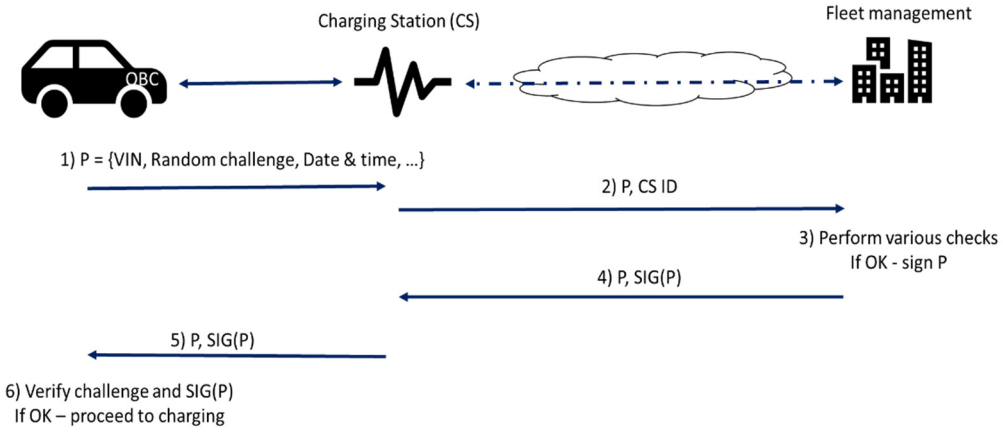

Figure 1

Utilizing techniques proposed herein may create a strong deterrent against stealing fleet vehicles; since, as soon as their batteries are drained, they can no longer drive. Of course, one can always steal a vehicle by loading it onto a truck, but this is certainly more cumbersome than driving away with the vehicle itself. Furthermore, the most valuable asset of the vehicle becomes useless, unless it is removed or taken apart, a doable but rather complicated procedure.

There may be other events in an EV's life cycle that can be used for verifying with its operator or owner whether it can continue operating normally. Still, charging events provide a very convenient, simple, and safe opportunity for such enforcement. First, the cadence of charging events is advantageous - they occur often enough to provide good security but do not occur too often. For comparison, consider the alternative of using startup events as a potential theft deterrent. Usually, vehicle startup events happen at least once a day and often more. This can create an unnecessary extra burden on the security system. Second, when a vehicle starts operating, it may be temporarily outside cellular coverage, e.g., if it was parked in an underground basement. Thus, it might be difficult for the vehicle to determine whether connectivity is maliciously jammed or temporarily blocked. At other times, e.g., when the vehicle is in motion, it might be dangerous to apply sanctions. Thus, the EV would have to mark for itself whether it is in a suspicious state and defer potential sanctions for a later time. More generally, adding a new device whose main purpose and function is to enforce security, like immobilizers, often results in a design that can be bypassed.

In contrast, when a CAEV is charging, it is connected by wire, and a data-exchange is already present as the vehicle typically sends updates on its battery status between the EV's OBC and the charging-station. As was explained above, this connectivity is required for safe and efficient charging, i.e., there is no need to add anything for improved security enforcement. Further, it is unlikely that charging-stations will not have network connectivity.

As usual with security countermeasures, careful implementation of the feature is important. For example, if the Electronic Control Units (ECUs) that implement the charging authorization procedure can be easily reprogrammed, replaced or bypassed using some other method, then the feature may be less effective. Integration of the security

protocol into the OBC may help to overcome this potential issue, as it is often difficult (though probably not impossible) to bypass protocols integrated into the OBC.

In summary, techniques are provided herein that utilize charging events of CAEVs as an enforcement point in which an owner/operator of a vehicle gives authorization to the vehicle to proceed with the charging, and hence continue operating normally.