Combined cyber and physical security system for charging electric vehicles

February 5 2015

As electricity grids become more sophisticated, grid administrators can collect instantaneous data on consumer and supplier behavior. The 'smart grid' then learns to improve the reliability, costs and sustainability of electricity distribution. However, smart grids present new security challenges, especially for mobile systems such as electric vehicles (EVs), which can be attacked both electronically and physically.

Now, Jianying Zhou and Aldar Chan at the A*STAR Institute of Infocomm Research have developed the first automatic security system that protects EVs from combined cyber–physical attacks.

"Most existing authentication systems merely apply cybersecurity schemes directly to the smart grid, leaving gaps in the protection," explains Zhou. "The problem is especially serious for EVs, because the charging infrastructure is publicly open. Anyone could plug in an EV, even if it is stolen."

A particular danger is the so-called substitution attack, whereby a criminal can 'digitally imitate' an EV, plugging in their own device while the EV owner pays for the electricity. Chan and Zhou demonstrated a successful substitution attack on an existing EV charging station. "We plugged in kettles and hair dryers; it could be anything that draws current," says Zhou.

After proving that this security loophole existed, the researchers worked to improve the classic 'challenge-response' protocol for online security.

"Instead of using a single challenge—which is a random number used to test if a user really is who he claims to be—we used one challenge sent through the wireless cyber path and another challenge through a physical path or the charging cable," says Zhou. "This ensures that the EV is connected physically to the right spot in the power grid, and that it is a real EV meeting existing EV standards."

Perhaps inevitably, Chan and Zhou found they could not achieve physical authentication using software alone. They had to design a new onboard hardware mechanism that binds an EV to its digital identity. However, they discovered a way to embed the challenge number in one of the signaling lines of the charging cable, so that existing charging stations will not need to be modified.

The researchers believe that their new security system could protect other components in the power grid, such as relays and transformers, as well as cardless ATMs. "With more research we could devise systems to ensure that the person withdrawing cash actually has digital authorization," says Zhou.

More information: Chan, A. C.-F. & Zhou, J. "Cyber–physical device authentication for smart grid electric vehicle ecosystem." *IEEE Journal on Selected Areas in Communications* 32, 1509–1517 (2014).

Provided by ResearchSEA