UNIVERSITÀ DI PISA

METHOD AND CORRESPONDING DEVICE FOR PROTECTING VEHICLE FROM CYBER ATTACK

INVENTORS:
Rosadini Christian
Nesci Walter
Baldanzi Luca
Crocetti Luca
Fanucci Luca

CO-OWNER/S:MAGNETI MARELLI S.P.A.

PATENT STATUS: GRANTED

PRIORITY NUMBER: 102018000021550

PRIORITY DATE: 31/12/2018

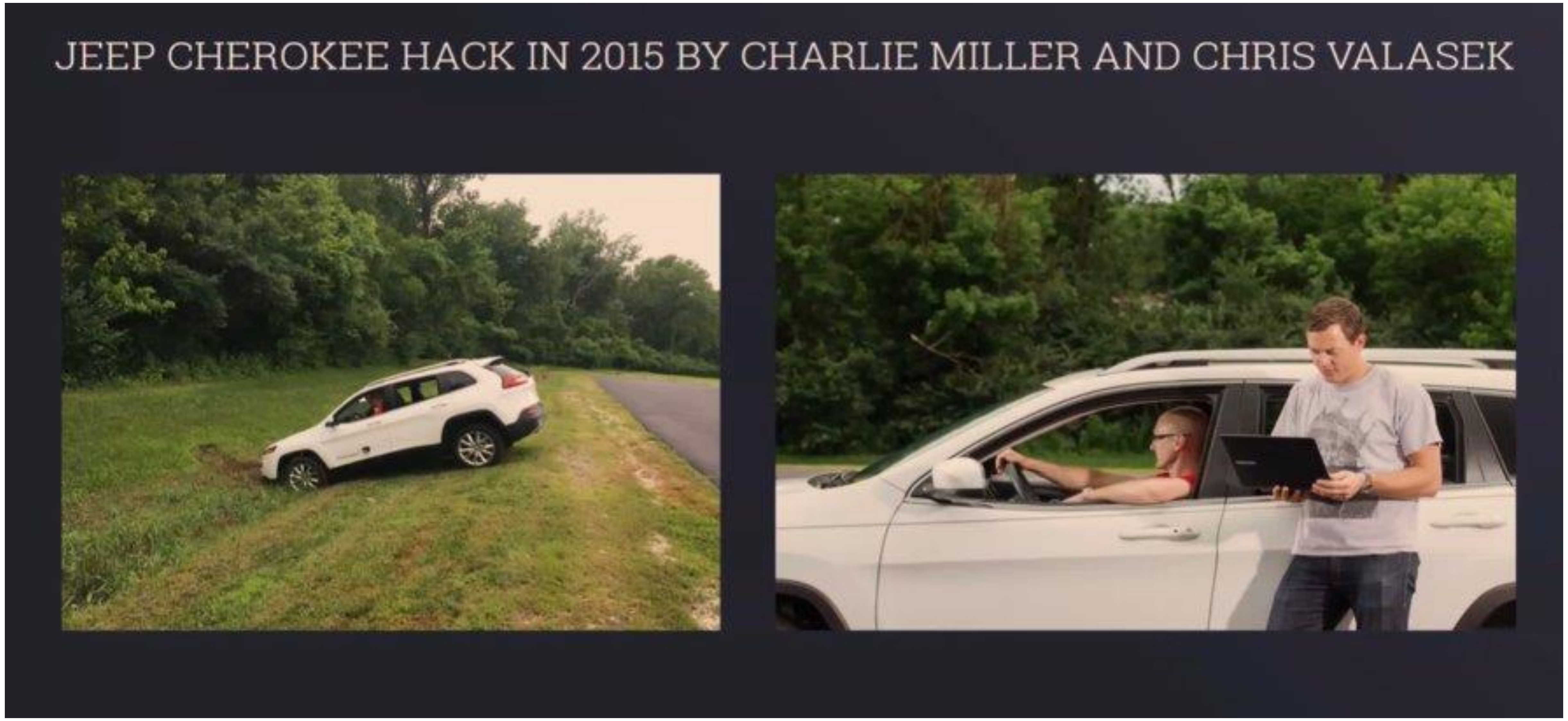
PUBLISHED AS: IN201914048739, JP2020109953, CN111385286

Invention

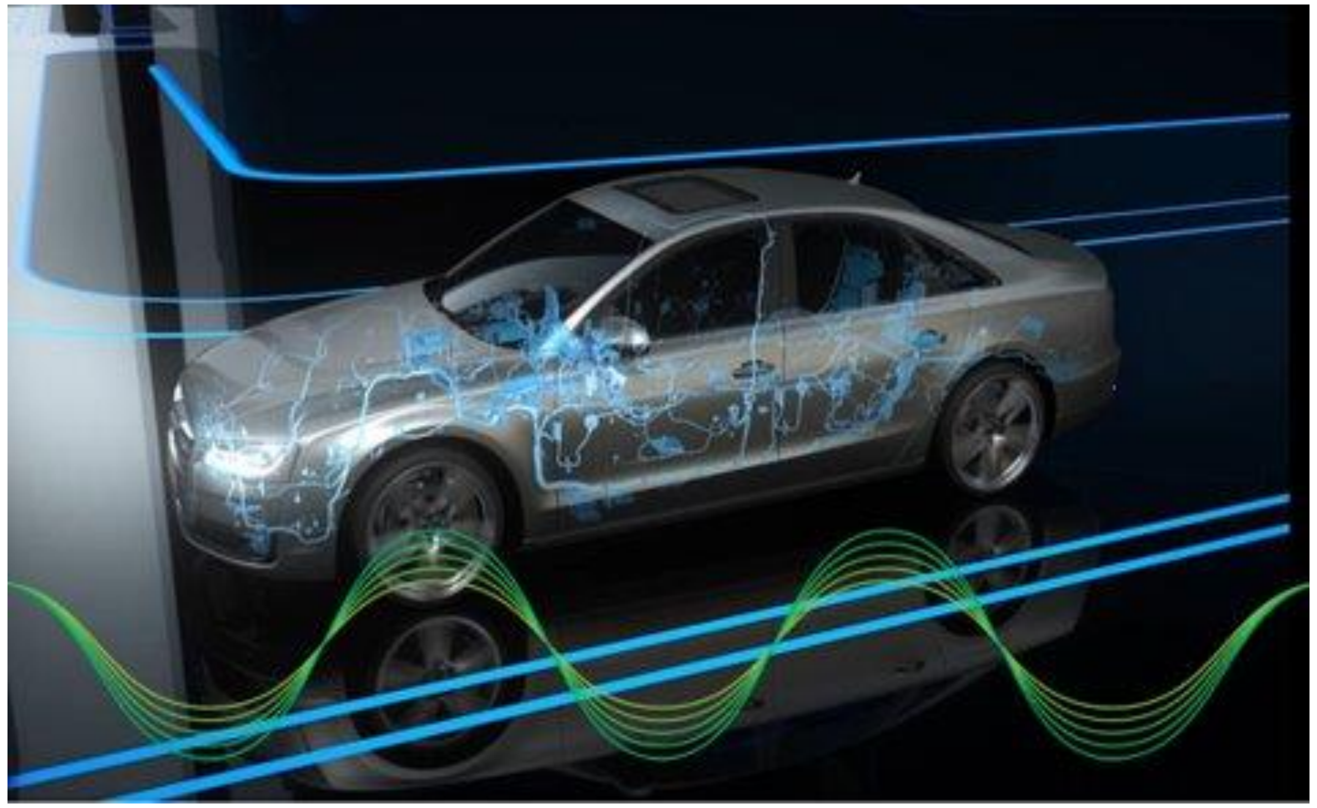
The invention concerns techniques for protection against computer attacks in a CAN (Controller Area Network) communication network in a vehicle using the CAN-bus system, the intelligent electronic system that is replacing the old control units. The CAN-bus system makes it possible to diagnose faults and anomalies autonomously and intelligently and to notify them by means of a message or warning light on the dashboard. This advanced electronic system aims to increase the safety of the vehicle through an on-board PC or ECU that constantly monitors all the vital parameters of the car. Protecting this type of system from possible infomatics attacks is the purpose of the present invention.

In 2015, Charlie Miller and Chris Valasek, a security engineer at Twitter and a researcher at IOActive, respectively, managed to hack a Jeep Cherokee by being able to send commands through the CAN-bus and made any component of the vehicle do whatever they wanted. They were able to take control of the steering wheel, engine, transmission, brakes, not to mention the windshield wipers, air conditioning, and door locks. And they did it all remotely, using the Sprint cellular network. The experience of the two researchers demonstrated the vulnerability of the system and the importance of systems like our proposed invention to prevent such attacks.

Drawings
& pictures



JEEP CHEROKEE HACK IN 2015 BY CHARLIE MILLER AND CHRIS VALASEK



Industrial applications

The invention is in the area of cybersecurity applicable to next-generation vehicles. The device and procedure covered by the patent enable a number of advantages:

- avoid the time mismatch between the corrupted message (sent on the bus) and the "Error-Frame" message generated by the CAN node receiving the corrupted message;

- mask, through an appropriate obfuscation process, the corruption operation to the CAN node that sent the illegal frame. This avoids the automatic retransmission, with consequent occupation of the CAN bus, by the malicious CAN node;

- not introducing any delay in the propagation of CAN messages, ensuring their use in a transparent way by the CAN nodes involved;

- operate with diagnostic CAN messages. Thanks to a dedicated control logic, it is possible to recognize a sequence of multi-frame diagnostic messages and invalidate, if the diagnostic service is identified as malicious, the entire chain of messages.

Possible developments

A prototype of the technology has been built and is being validated and tested on real vehicles. The research team is interested in collaborating with industrial partners to increase the technological maturity of the invention.

For more information:

Tech Transfer Office of University of Pisa

Headquarters: Lungarno Pacinotti 43/44, Pisa (PI) 56126

Web site: www.unipi.it/index.php/trasferimento

E-mail: valorizzazionericerca@unipi.it

For more information:

Ufficio Regionale di Trasferimento Tecnologico

Headquarters: Via Luigi Carlo Farini, 8 50121 Firenze (FI)

E-mail: urtt@regione.toscana.it

IN SUPREMÆ DIGNITATIS 1343
UNIVERSITÀ
DI PISA

REGIONE
TOSCANA

urtt
Ufficio Regionale
di Trasferimento Tecnologico