Secret Key Generation For Wireless Communication In Cyber-Physical Automotive Systems

Tech ID: 27124 / UC Case 2016-285-0

BRIEF DESCRIPTION

Automotive-based wireless communications rely on broadcasting signals over public channels, which must be encrypted due to their vulnerability to hacking by outside sources. Recently, researchers at UCI have developed a technique which utilizes the random motion of the vehicle to provide more secure and less energetically costly encryption over standard protocols.

FULL DESCRIPTION

Wireless communication has become ubiquitous in automobiles, as it is responsible for many aspects of intra-vehicular monitoring, and also allows for the implementation of common technologies such as Bluetooth, WiFi, and satellite GPS. These wirelessly transmitted signals, whether traveling within or to an automotive, are broadcast over a public channel that is susceptible to attack from an outside source. These attacks may allow a third party to hijack a vehicle from a remote source, or access drivers' personal information. Increasing the randomness with which the transmitted signal is encrypted provides increased security against these third party attacks. Current encryption in automotives is largely based on pseudo-random key generation, which places additional energy, memory, and performance demands on the vehicle.

Researchers at UCI have developed a novel key generation technique which instead utilizes the physical randomness provided by a moving automotive. The channel experiences spatial and temporal variations in the environment as the vehicle moves; these physical variations are truly random and as such, the keys generated in this manner are nearly impossible to predict or extract. Additionally, rather than relying on a single, pre-stored key, a new key is generated for each communication session. This technique provides increased security over standard procedures, while simultaneously reducing energy and performance overhead.

SUGGESTED USES

Automotive software

ADVANTAGES

Higher security than pre-stored key techniques

Lower performance (30%) and energy (10%) overhead than current state-of-the-art techniques

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Issued Patent	10,129,022	11/13/2018	2016-285

CONTACT

Edward Hsieh
hsiehe5@uci.edu
tel: 949-824-8428.

OTHER INFORMATION

CATEGORIZED AS

» **Transportation**
» Automotive

RELATED CASES

2016-285-0

UCI Beall
Applied Innovation

5270 California Avenue / Irvine,CA
92697-7700 / Tel: 949.824.2683