Privacy-preserving Control Message Dissemination for Platoon-based Vehicular Cyber-Physical Systems

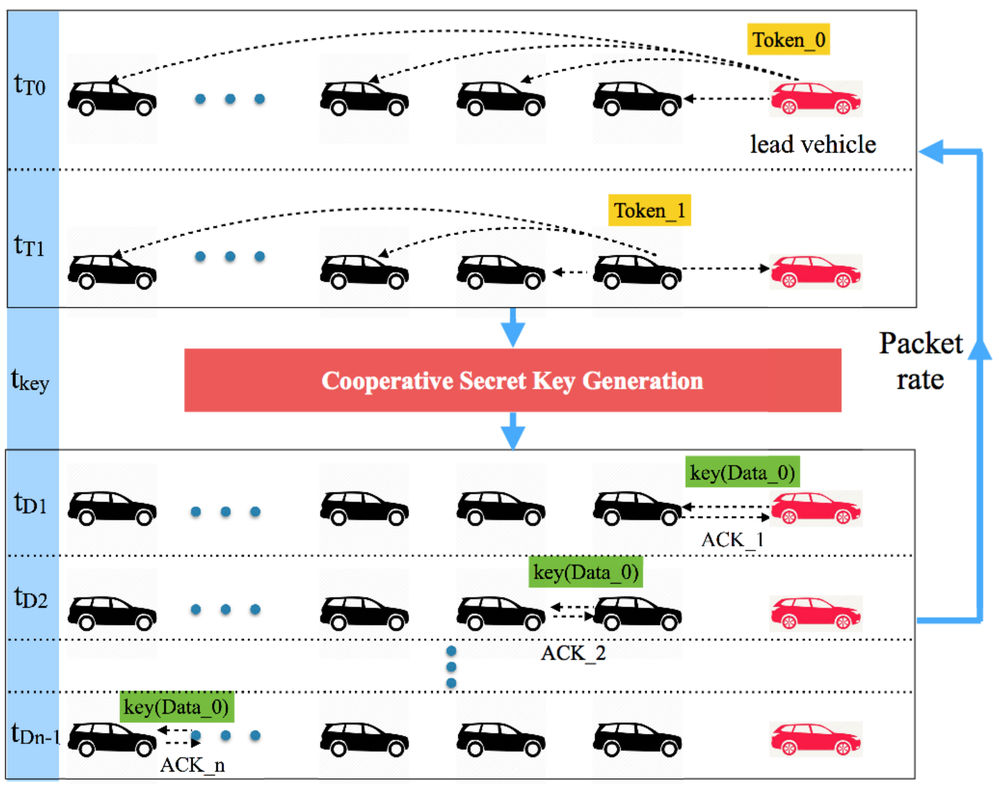
CISTER – Research Centre in
Real-Time & Embedded Computing Systems

Kai Li, Yousef Emami, and Eduardo Tovar
{kaili,emami,emt}@isep.ipp.pt

Motivation

- Platoon-based Vehicular Cyber-Physical System (PVCPS) has enabled a new platoon-based driving paradigm, in which a lead vehicle is driven manually, while the following vehicles follow the lead vehicle in a fully automatic fashion.

- The control message dissemination is vulnerable to eavesdropping attacks due to the broadcast nature of radio channels.

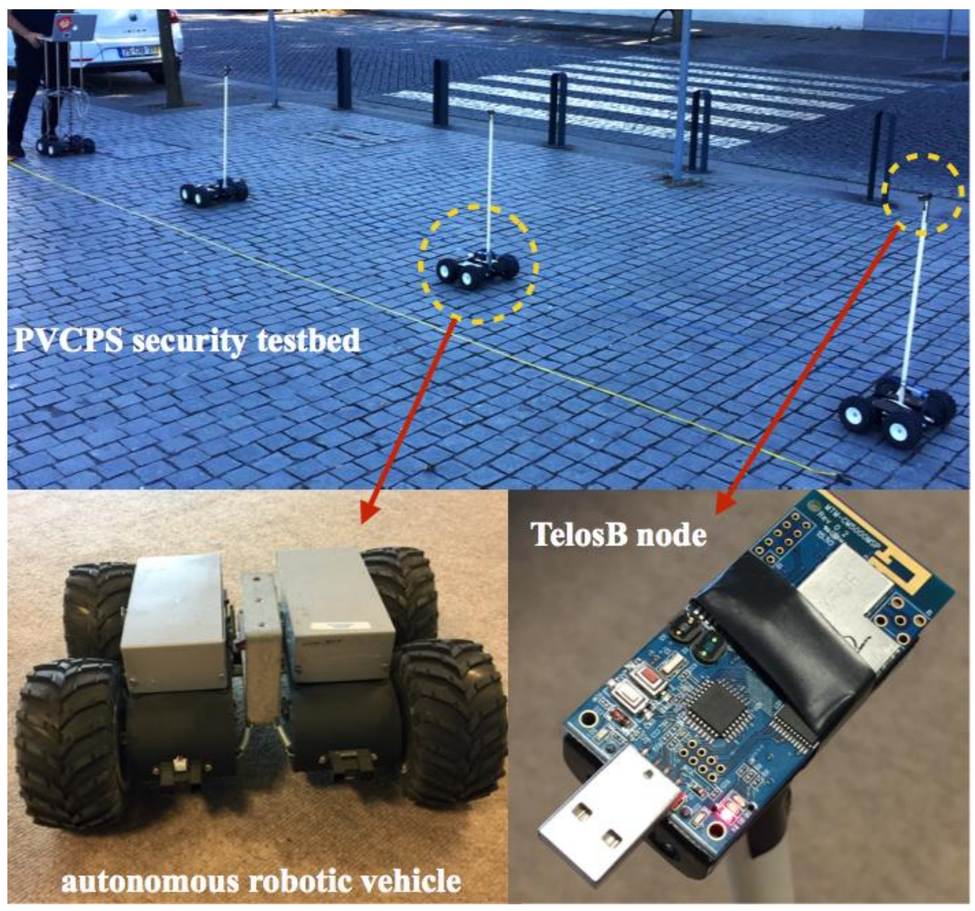


Testbed

- The CoopKey testbed for PVCPS security is built with a platoon of 4 mobile nodes.

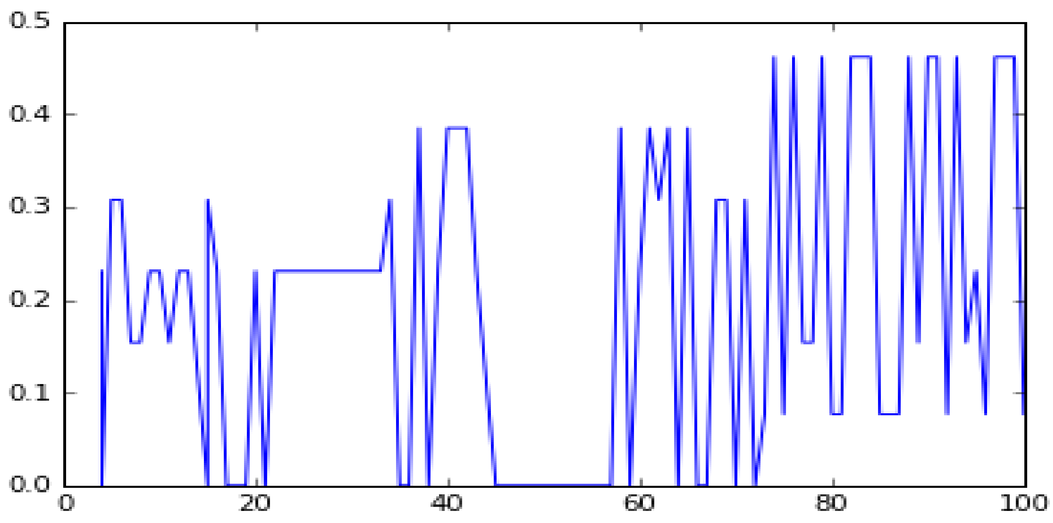
- The Crossbow TelosB wireless transceiver mounted on a 1m-high plastic pole is placed on top of the node.

- Bit mismatch rate (BMMR) is the ratio of the number of secret bits that mismatch between the lead node and the following nodes to the key length.



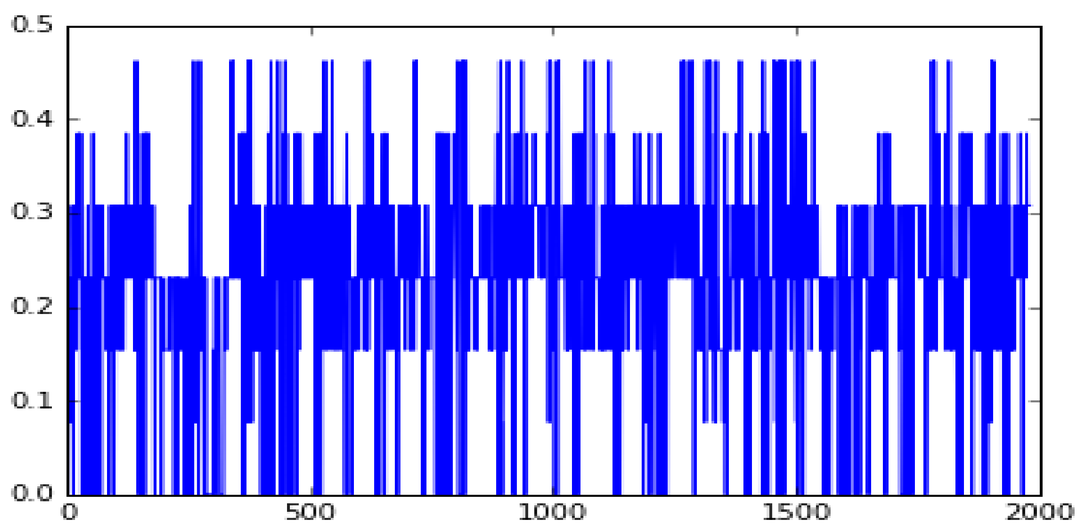
The CoopKey testbed for PVCPS security.

Experimental Results



BMMR with respect to 100 secret keys.

BMMR with respect to 1000 secret keys.



BMMR with respect to 2000 secret keys.

Reference

[1] Kai Li, Harrison Kurunathan, Ricardo Severino, and Eduardo Tovar. 2018. Cooperative key generation for data dissemination in cyber-physical systems. In Proceedings of the 9th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS). IEEE Press, 331–332.

[2] Kai Li, Wei Ni, Eduardo Tovar, and Mohsen Guizani. 2018. LCD: Low latency command dissemination for a platoon of vehicles. In Proceedings of IEEE International Conference on Communications (ICC).

Co-financed by Unidade de I&D CISTER - CEC/04234:
FCT Fundação para a Ciência e a Tecnologia

CISTER Research Centre
ISEP, Polytechnic Institute of Porto
Rua Dr. Antº Bernardino de Almeida, 431
4249-015 Porto, Portugal
+351 228 340 502
www.cister-labs.pt
info@cister-labs.pt
facebook.com/cisterlabspt

isep Instituto Superior de Engenharia do Porto
P.PORTO