Poster

Poster Abstract: Privacy-preserving Control Message Dissemination for PVCPS

Kai Li

Yousef Emami

Eduardo Tovar

CISTER-TR-190203

Poster Abstract: Privacy-preserving Control Message Dissemination for PVCPS

Kai Li, Yousef Emami, Eduardo Tovar

CISTER Research Centre

Polytechnic Institute of Porto (ISEP P.Porto)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail:

https://www.cister-labs.pt

Abstract

Privacy preservation is critical for control information disseminationin Platoon-based Vehicular Cyber-Physical Systems (PVCPS).However, the vehicular communication is vulnerable to wirelesseavesdropping attack and message modification, due to broadcastnature of radio channels. In this poster, we present a secret key generationtestbed for PVCPS security, which is built based on off-theshelfautonomous robotic vehicles and TelosB wireless transceivers.A cooperative secret key agreement (CoopKey) scheme is demonstratedfor encrypting/decrypting the disseminated control messages.To unify the secret key generated by the vehicles, CoopKeyexplores received signal strength (RSS) measurements and channelestimation on the inter-node radio channel. In addition, a Pythonbaseduser interface is also implemented to show real-time bitmismatch rate of CoopKey.

Poster Abstract: Privacy-preserving Control Message Dissemination for PVCPS

Kai Li
Real-Time and Embedded Computing
Systems Research Centre (CISTER)
Porto, Portugal
kaili@isep.ipp.pt

Yousef Emami
Real-Time and Embedded Computing
Systems Research Centre (CISTER)
Porto, Portugal
emami@isep.ipp.pt

Eduardo Tovar
Real-Time and Embedded Computing
Systems Research Centre (CISTER)
Porto, Portugal
emt@isep.ipp.pt

ABSTRACT

Privacy preservation is critical for control information dissemination in Platoon-based Vehicular Cyber-Physical Systems (PVCPS). However, the vehicular communication is vulnerable to wireless eavesdropping attack and message modification, due to broadcast nature of radio channels. In this poster, we present a secret key generation testbed for PVCPS security, which is built based on off-the-shelf autonomous robotic vehicles and TelosB wireless transceivers. A cooperative secret key agreement (CoopKey) scheme is demonstrated for encrypting/decrypting the disseminated control messages. To unify the secret key generated by the vehicles, CoopKey explores received signal strength (RSS) measurements and channel estimation on the inter-node radio channel. In addition, a Python-based user interface is also implemented to show real-time bit mismatch rate of CoopKey.

CCS CONCEPTS

• **Computer systems organization → Sensor networks**.

KEYWORDS

Vehicular platoons, Cyber-Physical Systems, Secret key, Testbed

ACM Reference Format:
Kai Li, Yousef Emami, and Eduardo Tovar. 2019. Poster Abstract: Privacy-preserving Control Message Dissemination for PVCPS. In *IPSN '19: The 18th ACM/IEEE International Conference on Information Processing in Sensor Networks, April 16–18, 2019, Montreal, Canada.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

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 [2, 4]. The lead vehicle decides the platoon's driving status, i.e., driving speed, heading direction, acceleration/deceleration values, and road emergency. Thanks to inter-vehicle wireless communications, the lead vehicle (managing the platoon) periodically broadcasts driving control information to update the driving status of the following vehicles. The following vehicle acts as a data-forwarding node, so that the messages from the leader can be disseminated to all the nodes in the platoon. However, the control message dissemination in PVCPS is vulnerable to eavesdropping attacks due to the broadcast nature of radio channels [1]. Adversaries could track the location of vehicles of interest, and launch spoofing, playback, or impersonation attacks to abuse mobility patterns of the platoon. Consequently, a secret key for message encryption/decryption is crucial to support control message confidentiality, integrity, and sender authentication, which is also critical to the driving safety in PVCPS.

Several methods are studied to explore wireless link dynamics to generate a pair of shared secret key for two nodes [5]. Unfortunately, the existing solutions are hardly applied to vehicular platoons since all the nodes in PVCPS have to agree upon one unanimous secret key so that the disseminated control message from the preceding node can be timely decoded by the following one. In our preliminary work [3], we experimentally study the secret key generation for data dissemination security, where the key is generated based on locally quantized received signal strength (RSS) measurements on each node. The experimental results in [3] show that the distance between the nodes and number of quantization intervals can affect the secret bit mismatch rate. By extending the system design and experiments in [3] for the secret key agreement of multiple nodes, this demonstration implements a cooperative secret key agreement (CoopKey) scheme for PVCPS, which generate a unanimous secret key for multiple nodes based on estimation of RSS measurements. Moreover, the CoopKey testbed supports an intuitive user-interface to display the real-time secret bit mismatch rate of the key generation.

2 TESTBED AND IMPLEMENTATION OF COOPKEY

2.1 System overview and implementation

Figure 1 illustrates the CoopKey testbed for PVCPS security, which is built with a platoon of 4 mobile nodes. The nodes travel in a straight line with the same velocity which is determined by the lead node. The inter-node distance is maintained at 2 meters. With regards to the wireless communication interface, the Crossbow TelosB wireless transceiver mounted on a 1m-high plastic pole is placed on top of the node. The TelosB node has the maximum data rate of 250 kbps, while the maximum transmission power is 0 dBm. In particular, the data rate and transmission power of all nodes are set to the maximum level during our experiments. In terms of packet length, the payload of the data packet has 100 bytes.

IPSN '19, April 16–18, 2019, Montreal, Canada

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

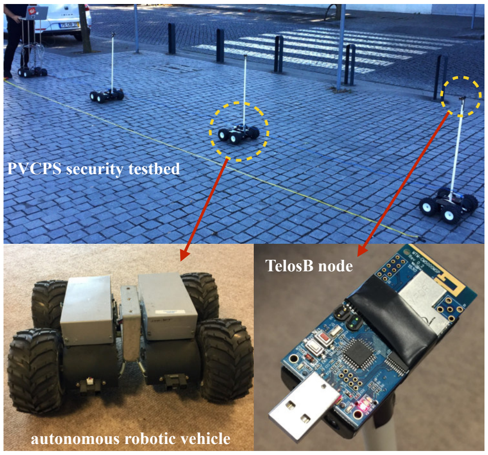

Figure 1: The CoopKey testbed for PVCPS security.

The transmission of data packets is initialized by the lead node. The data packets are encrypted by CoopKey at the lead node, and immediately disseminated to its adjacent following node all the way to the tail node. When the tail node successfully receives the data, it broadcasts an acknowledgement packet so that the lead node can transmit a new packet. In case of packet loss during the dissemination, a timeout of the packet dissemination at the lead node is set to 3 seconds. In other words, the lead node disseminates a new data packet if the acknowledgement from the tail node is not received within 3 seconds.

We implement three steps that incorporate CoopKey for the cooperative key generation: RSS measurement and estimation, channel quantization intervals reconciliation, and secret key extraction. Specifically, the nodes broadcast a single beacon packet in turn in order to share their link information. Transmitting the beacon packet is initialized by the lead node, which solely decides the driving status. Similarly, the adjacent following node broadcasts its beacon packet once the beacon from the lead node is successfully received. When all the nodes in PVCPS finish the beacon transmission, the following vehicles estimate the RSS values between the first two nodes in PVCPS. Next, CoopKey cooperatively quantizes the measured/estimated RSS readings on each node. Note that output of the quantized RSS readings is an alternating sequence of multiple 0s and 1s, which are taken as the secret bit sequence. The RSS quantization intervals are recursively adjusted until a unanimous secret key can be generated.

2.2 Secret bit mismatch rate

In terms of the performance metric, we define bit mismatch rate (BMMR) as the ratio of the number of secret bits that mismatch between the lead node and the following nodes to the key length.

The total number of quantization intervals is set to 10. Figure 4 shows BMMR at the tail node in PVCPS with regards to different number of generated keys (or at different time). Thanks to the intuitive Python-based user interface of our CoopKey testbed, displaying the real-time BMMR, it can be observed that BMMR of CoopKey is time varying, and the average value is around 18%. This confirms that the generated secret bits in CoopKey are random in the presence of channel dynamics, indicating that any eavesdropper experiencing independent channel fading is not able to obtain the same key as the node in PVCPS.

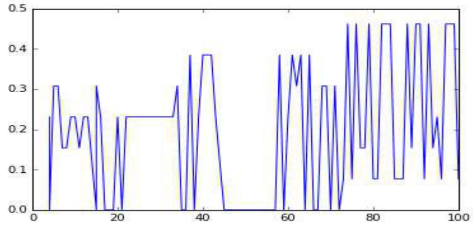

Figure 2: BMMR with respect to 100 secret keys.

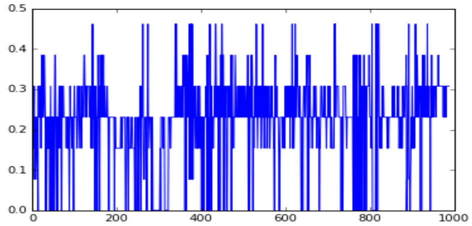

Figure 3: BMMR with respect to 1000 secret keys.

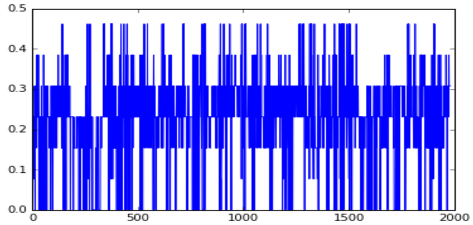

Figure 4: BMMR with respect to 2000 secret keys.

ACKNOWLEDGEMENT

This work was supported by National Funds through FCT/MEC (Portuguese Foundation for Science and Technology) and co-financed by ERDF (European Regional Development Fund) under the PT2020 Partnership, within the CISTER Research Unit (CEC/04234); also by FCT/MEC and the EU ECSEL JU under the H2020 Framework Programme, within project ECSEL/0002/2015, JU grant nr. 692529-2 (SAFECOP).

REFERENCES

[1] Mani Amoozadeh, Arun Raghuramu, Chen-Nee Chuah, Dipak Ghosal, H Michael Zhang, Jeff Rowe, and Karl Levitt. 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *IEEE Communications Magazine* 53, 6 (2015), 126–132.

[2] Dongyao Jia, Kejie Lu, Jianping Wang, Xiang Zhang, and Xuemin Shen. 2016. A survey on platoon-based vehicular cyber-physical systems. *IEEE communications surveys & tutorials* 18, 1 (2016), 263–284.

[3] 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*. IEEE, 331–332.

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

[5] Yiliang Liu, Hsiao-Hwa Chen, and Liangmin Wang. 2017. Physical layer security for next generation wireless networks: Theories, technologies, and challenges. *IEEE Communications Surveys & Tutorials* 19, 1 (2017), 347–376.