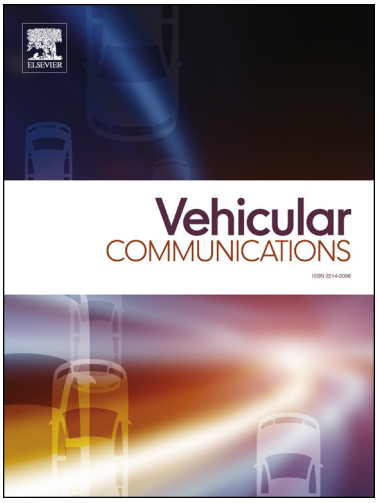
# Accepted Manuscript




Anomaly Intrusion Detection Method for Vehicular Networks Based on Survival Analysis

Mee Lan Han, Byung Il Kwak, Huy Kang Kim

PII: S2214-2096(18)30118-9
DOI: https://doi.org/10.1016/j.vehcom.2018.09.004
Reference: VEHCOM 142

To appear in: *Vehicular Communications*

Received date: 9 May 2018
Revised date: 14 September 2018
Accepted date: 18 September 2018

Please cite this article in press as: M. Lan Han et al., Anomaly Intrusion Detection Method for Vehicular Networks Based on Survival Analysis, *Veh. Commun.* (2018), https://doi.org/10.1016/j.vehcom.2018.09.004

# Anomaly Intrusion Detection Method for Vehicular Networks Based on Survival Analysis

Mee Lan Han, Byung Il Kwak, Huy Kang Kim*

*Graduate School of Information Security, Korea University, Seoul, Republic of Korea*

**Abstract**

In recent years, alongside with the convergence of In-vehicle network (IVN) and wireless communication technology, vehicle communication technology has been steadily progressing. Furthermore, communication with various external networks—such as cloud, vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) communication networks—further reinforces the connectivity between the inside and outside of a vehicle. On the contrary, this means that the functions of existing vehicles using computer-assisted mechanical mechanisms can be manipulated and controlled by a malicious packet attack. Therefore, diversified and advanced architectures of vehicle systems can significantly increase the accessibility of the system to hackers and the possibility of an attack. This paper proposes an intrusion detection method for vehicular networks based on the survival analysis model. Our main aims were to identify malicious CAN messages and accurately detect the normality and abnormality of a vehicle network without semantic knowledge of the CAN ID function. To this end, normal and abnormal driving data were extracted from three different types of vehicles and we evaluated the performance of our proposed method by measuring the accuracy and the time complexity of anomaly detection by considering three attack scenarios and the periodic characteristics of CAN IDs. Based on the results, we concluded that a CAN ID with a long cycle affects the detection accuracy and

*Corresponding author

*Email addresses:* blosst@korea.ac.kr (Mee Lan Han), kwacka12@korea.ac.kr (Byung Il Kwak), cenda@korea.ac.kr (Huy Kang Kim)