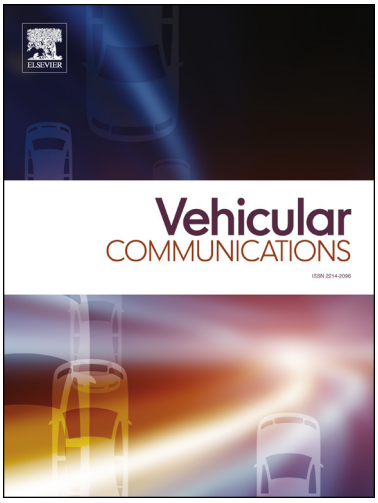
Accepted Manuscript



TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs

Chaker Abdelaziz Kerrache, Nasreddine Lagraa, Carlos T. Calafate, Abderrahmane Lakas

PII: S2214-2096(16)30056-0
DOI: http://dx.doi.org/10.1016/j.vehcom.2016.11.010
Reference: VEHCOM 66

To appear in: *Vehicular Communications*

Received date: 24 May 2016
Revised date: 20 October 2016
Accepted date: 28 November 2016

Please cite this article in press as: C.A. Kerrache et al., TFDD: A trust-based framework for reliable data delivery and DoS defense in VANETs, *Veh. Commun.* (2016), http://dx.doi.org/10.1016/j.vehcom.2016.11.010

TFDD: a Trust-based Framework for Reliable Data Delivery and DoS defense in VANETs

Chaker Abdelaziz Kerrache[a,*], Nasreddine Lagraa[a], Carlos T. Calafate[b], Abderrahmane Lakas[c]

[a] *Laboratoire d'Informatique et de Mathématiques, University of Laghouat, BP 37G, route de Ghardaia, Laghouat, Algeria*
[b] *Department of Computer Engineering, Universitat Politècnica de València, Camino de Vera, S/N, 46022 València, Spain*
[c] *College of Information Technology, United Arab Emirates University PO Box 17551,Al Ain, UAE*

Abstract

A trust establishment scheme for enhancing inter-vehicular communication and preventing DoS attacks 'TFDD' is proposed in this paper. Based on a developed intrusion detection module (IDM) and data centric verification, our framework allows preventing DDoS attacks and eliminating misbehaving nodes in a distributed, collaborative and instantaneous manner. In addition, a trusted routing protocol is proposed that, using context-based information such as link stability and trust information, delivers data through the most reliable way. In this study, the simulation results obtained demonstrate the effectiveness of our trust framework at detecting dishonest nodes, as well as malicious messages that are sent by honest or dishonest nodes, after a very low number of message exchanges. Furthermore, colluding attacks are detected in a small period of time, which results in network resources being released immediately after an overload period. We also show that, in a worst-case scenario, our trust-based framework is able to sustain performance levels, and outperforming existing solutions such as T-CLAIDS and AECFV.

Keywords: Trust Management, Vehicular Ad-hoc Networks, DoS defense,

*Corresponding author
Email addresses: a.kerrache@mail.lagh-univ.dz (Chaker Abdelaziz Kerrache), n.lagraa@mail.lagh-univ.dz (Nasreddine Lagraa), calafate@disca.upv.es (Carlos T. Calafate), alakas@uaeu.ac.ae (Abderrahmane Lakas)