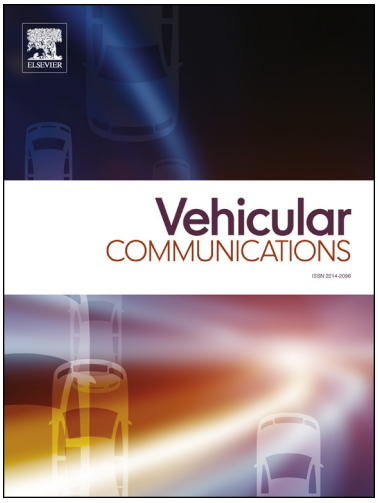
Accepted Manuscript



UAV-assisted technique for the detection of malicious and selfish nodes in VANETs

Chaker Abdelaziz Kerrache, Abderrahmane Lakas, Nasreddine Lagraa, Ezedin Barka

PII: S2214-2096(17)30079-7
DOI: https://doi.org/10.1016/j.vehcom.2017.12.001
Reference: VEHCOM 108

To appear in: *Vehicular Communications*

Received date: 29 May 2017
Revised date: 8 November 2017
Accepted date: 6 December 2017

Please cite this article in press as: C.A. Kerrache et al., UAV-assisted technique for the detection of malicious and selfish nodes in VANETs, *Veh. Commun.* (2017), https://doi.org/10.1016/j.vehcom.2017.12.001

UAV-assisted Technique for the Detection of Malicious and Selfish Nodes in VANETs

Chaker Abdelaziz Kerrache[a,b,*], Abderrahmane Lakas[c], Nasreddine Lagraa[a], Ezedin Barka[c]

[a] *Laboratoire d'Informatique et de Mathématiques, University of Laghouat, BP 37G, route de Ghardaia, Laghouat, Algeria*
[b] *University of Ghardaia, Algeria*
[c] *CIT, UAE University, Al Ain, UAE*

Abstract

Detecting malicious and selfish nodes is an important task in Vehicular Adhoc NETworks (VANETs). Various proposals adopted trust management as an alternative solution since it is less costly than cryptography-based solution in terms of computation delay and mobility support. However, the existing solutions assume that, in general, the attackers have always a dishonest behavior that persists over time. This assumption may be misleading, as the attackers can behave intelligently to avoid being detected. Moreover, pseudonyms changing strategies to preserve vehicles' privacy are another issue to take into account. In this paper, a new solution for the detection of intelligent malicious behaviors based on the adaptive detection threshold is proposed. In addition to the detection of malicious nodes, our solution relies on Unmanned Aerial Vehicles to face the negative impact of pseudonym changes on the detection process. Our solution also incites attackers to behave well since any malicious behavior will be immediately detected thanks to the adaptive detection threshold adopted. Simulation results depict the high efficiency of our proposal at ensuring high ratios for both detection and packet delivery.

Keywords: UAV, Trust Management, VANETs, Pseudonyms changing.

*Corresponding author
Email addresses: ch.kerrache@lagh-univ.dz (Chaker Abdelaziz Kerrache), alakas@uaeu.ac.ae (Abderrahmane Lakas), n.lagraa@lagh-univ.dz (Nasreddine Lagraa), ebarka@uaeu.ac.ae (Ezedin Barka)