Chapter 5
Security and Connectivity Analysis in Vehicular Communication Networks

Hamada Alshaer
Khalifa University, UAE

Sami Muhaidat
Khalifa University, UAE

Raed Shubair
Khalifa University, UAE

Moein Shayegannia
Simon Fraser University, Canada

ABSTRACT

Reliable Vehicular Ad-Hoc Networks (VANETs) require secured uninterrupted uplink and downlink connectivity to guarantee secure ubiquitous vehicular communications. VANET mobility, multi-fading wireless, and radio channels could result in unsecured and disrupted vehicular communications, isolating some vehicle nodes and making them vulnerable to security attacks. A VANET is considered to be connected and secured if there is a secured path connecting any pair of Communication-Enabled Vehicles (CEVs) in this network. Among many parameters, VANET connectivity depends on two main elements: communication transmission range and statistical distribution characterizing inter-vehicle spacing. To guarantee persistent VANET connectivity, a vehicle transmission radio range must be set properly based on the characteristic of the statistical distribution modeling the inter-vehicle spacing. This chapter analyzes three inter-vehicle spacing models based on exponential, Generalized Extreme Value (GEV), and Exponential with Robustness Factor (EwRF) statistical distributions. Based on vehicle nodes spatial density on a road segment, each vehicle node can adjust its transmission range to increase network connectivity and guarantee ubiquitous vehicular communications. Communications among vehicle nodes are secured through trusted Road-Side Units (RSUs) which distribute efficiently secret keys to vehicle nodes under their coverage to establish secure communication sessions.

DOI: 10.4018/978-1-4666-4691-9.ch005

Copyright © 2014, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

Next generation intelligent transport systems (NGITSs) enable vehicles to communicate with its neighbors through vehicular ad-hoc networks (VANETs) connectivity and exchange information with road-side units (RSUs) as well as road communication gateways (RCGs), installed along the roads, through vehicle-to-road (V2R) or vehicle-to-infrastructure (V2I) connectivity (Alshaer & Elmirghani, 2009; Alshae & Horlait, 2004; Alshaer & Horlait, 2005). Communication-enabled vehicles (CEVs) are equipped with small-sized wireless devices with increasing computing capabilities which can enable them to network together through peer-to-peer (P2P) communications without the need for fixed communication infrastructure (Blum & Eskandarian & Hoffman, 2004; Hartenstein & Laberteaux, 2008). Reliable VANETs require establishing security and privacy techniques to secure vehicular information messages delivery. VANET security should (i) ensure the information received by vehicle nodes is correct and (ii) verify message integrity and source authentication (Sun & Zhang & Zhang & Fang, 2010). Because of the high and fluctuating mobility of vehicle nodes and transmission power constraints, a VANET might suffer continuous and persistent disruptions. This makes it challenging to maintain security and connectivity of VANET at a determined level.

VANET connectivity ensures the relay of information messages from a vehicle to reach all the other vehicles in the network. To guarantee this connectivity, a road must be sufficiently dense. If the vehicles are too sparsely distributed, the distance between two consecutive vehicles may exceed their radio transmission range, which makes them unable to communicate, causing disconnections in the network connecting them. The number of vehicle nodes involved in VANETs may vary, depending on the change in the transmission ranges assigned to vehicle nodes. A vehicle node that transmits at a large transmission range will increase the probability of finding a receiver in the desired direction and significantly contribute in the successful data transmission range. But, this may result in a higher probability of collisions with other data transmissions and increase energy (power) consumption. The converse is correct for short transmission range.

Despite vehicles in VANETs are highly mobile, both velocity and flow of vehicles are dependent on vehicle density (Nagatani, 2002). The increase in vehicle density causes traffic to shift from free-flow stage, where vehicles movement is unrestricted, to traffic jams caused by dense traffic. While many research studies have been conducted on the connectivity of VANETs (Panichpapiboon & Atikom, 2008; Santi & Blough, 2003; Penrose,1999; Desai & Manjunath, 2002; Panichpapiboon & Pattara-atikom, 2008), most of them rely on the crucial assumption that the inter-vehicle spacing between consecutive vehicles is exponentially distributed. Although an exponential distribution is a good approximation for the inter-vehicle spacing in extremely light traffic conditions, a new empirical analysis (Cheng & Panichpapiboon, 2012) suggests that in a moderate condition the inter-vehicle spacing better be described by other statistical distributions. If the inter-vehicle spacing distribution is not exponential, how does it affect the connectivity analysis? To what extent would the density and the transmission range required for network connectivity change if the inter-vehicle spacing distribution was not exponential? This chapter answers these questions and associates connectivity analysis with security.

Some vehicular traffic information systems still rely on a centralized communication model, where the collected traffic data are sent to a central processing unit before being distributed back to drivers on the roads. This is inefficient in terms of delay and other quality-of-service (QoS) requirements; and the communication infrastructure required for the centralized communication model could be costly (Alshaer & Ernst & Fortelle, 2012). The whole communication system becomes more ef-

23 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-and-connectivity-analysis-in-vehicular-communication-networks/86302

Related Content

Mobile Multimedia Streaming Using Secure Multipath in Wireless Ad Hoc Networks
Lei Chenand Chung-Wei Lee (2012). *Emergent Trends in Personal, Mobile, and Handheld Computing Technologies (pp. 141-159).*
www.irma-international.org/chapter/mobile-multimedia-streaming-using-secure/65337

High-Efficiency Multihomed Multimedia Transmission in Wireless Sensors
Haitao Wangand Yanli Chen (2022). *International Journal of Mobile Computing and Multimedia Communications (pp. 1-19).*
www.irma-international.org/article/high-efficiency-multihomed-multimedia-transmission-in-wireless-sensors/297966

Enhancing Outdoor Learning Through Participatory Design and Development: A Case Study of Embedding Mobile Learning at a Field Study Centre
Trevor Collins (2015). *International Journal of Mobile Human Computer Interaction (pp. 42-58).*
www.irma-international.org/article/enhancing-outdoor-learning-through-participatory-design-and-development-a-case-study-of-embedding-mobile-learning-at-a-field-study-centre/123364

From Ethnography to Interface Design
Jeni Paay (2008). *Handbook of Research on User Interface Design and Evaluation for Mobile Technology (pp. 1-15).*
www.irma-international.org/chapter/ethnography-interface-design/21820

A Secure and Optimized Proximity Mobile Payment Framework With Formal Verification
Shaik Shakeel Ahamad, V.N. Sastryand Siba K. Udgata (2018). *Mobile Commerce: Concepts, Methodologies, Tools, and Applications (pp. 161-189).*
www.irma-international.org/chapter/a-secure-and-optimized-proximity-mobile-payment-framework-with-formal-verification/183286