

---

## Editorial

---

### Zonghua Zhang\*

Information Security Research Center,  
NICT,  
Japan  
E-mail: zonghua.zhang@nict.go.jp

\*Corresponding author

### Farid Naït-Abdesselam

Lille University of Science and Technologies,  
France  
E-mail: farid.nait-abdesselam@lifl.fr

### Sherali Zeadally

University of the District of Columbia,  
Washington, DC 20008, USA  
E-mail: szeadally@udc.edu

### António Casimiro

University of Lisboa,  
Portugal  
E-mail: casim@di.fc.ul.pt

**Abstract:** The rapid advancement in wireless communication technologies, along with mobile computing platforms, have led to significant accessibility to internet services, as well as high-speed and high-quality information exchange between mobile/portable devices located anywhere in the globe. Among the various application scenarios enabled by these technologies, vehicular *ad hoc* network (VANET) designs and applications have emerged and continue to attract a lot of attention. Their applications in practice, however, can be dramatically impeded because of critical security, trust and privacy issues. The purpose of this special issue is to present contributions of six technical papers that address the aforementioned issues from different perspectives, leading to a complete snapshot on the progress of security, trust and privacy-preserving techniques for VANET.

**Keywords:** security and privacy; trust; reputation.

**Biographical notes:** Dr. Zonghua Zhang is now working with NICT, Japan. Before joining in NICT in April 2008, he was a Postdoctoral Researcher at INRIA Lille – Nord Europe, France. Prior to that, he spent over one year, from June 2006 to June 2007, as a Postdoctoral Fellow at the University of Waterloo, Canada. He obtained his PhD in Information Science from Japan Advanced Institute of Science and Technology (JAIST), MSc in Computer Science and

BSc in Information Science from Xidian University, China, in 2006, 2003 and 2000, respectively. His research interest covers a variety of security issues in computer systems and networks, with emphasis on anomaly detection, network forensics and reputation management.

Farid Naït-Abdesselam received his state engineering degree in Computer Science from the University of Sciences and Technologies Houari Boumediene, Algeria, MS in Computer Science from the University of Paris Descartes, France and PhD in Computer Science, respectively, in 1993, 1994 and 2000. He is actually an Associate Professor at the University of Sciences and Technologies of Lille. His research interests lie in the field of computer and communication networks with emphasis on architectures and protocols for quality of service and security in IP-based wired and wireless networks.

Sherali Zeadally received his BA and MA in Computer Science from Cambridge University, England, and his PhD in Computer Science from the University of Buckingham, England. He is an Associate Professor at the University of the District of Columbia, Washington, DC. He is a Fellow of the British Computer Society (FBCS). His research interests include computer networks, mobile computing, network and system security.

António Casimiro received the Master's degree of Electrotechnic and Computers Engineering (1995) from the Instituto Superior Técnico de Lisboa (IST). He received the PhD in Informatics (2003) from the University of Lisboa. He is currently an Assistant Professor at the Department of Informatics (DI) from the University of Lisboa Faculty of Sciences. He is a Member of the LASIGE research laboratory, where he co-leads one of the Navigators group research lines. His research interests include dependable and adaptive distributed systems, real-time and event-based communication, and sensor networks. He is a Member of the IEEE.

The rapid development and wide-spread application of wireless communication technologies and mobile computing paradigms are significantly reshaping today's cyber-infrastructure, enhancing the accessibility of internet services, and leading to a wide range of techniques for high-speed and high-quality information exchange between mobile/portable devices located anywhere in the globe. Among the various application scenarios enabled by these technologies, vehicular *ad hoc* networks (VANETs) continue to be an area of strong interests to designers and researchers.

Vehicular communications allow the real-time information exchange between vehicles and infrastructures, with the objective of enhancing road safety and optimising road traffic. VANETs are primarily enabled by inter-vehicular (or Car-to-Car, C2C) communications and vehicle-roadside communications (or Car-to-Infrastructure, C2I). For instance, a driver of a car equipped with a VANET terminal, which is known as on-board units, can access internet via access point (Roadside Units, RSUs) on the roadside and meanwhile communicate with the others along the same road. As a result, the driver can obtain all the information of interest in real-time, for example, weather condition, road environment and traffic/signal conditions. The management complexity of road administration offices can be significantly reduced, increase the easiness of driving and enhance safety on roads.

However, one strong prerequisite for achieving those benefits is that VANET always works in a dependable and secure way. Otherwise, the deployment of VANET, in practice, will be dramatically impeded. More seriously, the failure of VANET, either by accidental system errors or by intentional attacks, could disrupt a city's transportation system, and we may have the loss of public and personal property, and even human life. Therefore, it is extremely important to develop effective and efficient fault-tolerance and security mechanisms to ensure the quality and robustness of services provided by VANET. This special issue does not intend to cover both dependability and security issues in VANET. It is rather devoted to present the state-of-the-art proposals and cutting-edge research achievements on addressing security, trust and privacy challenges in VANETs.

Each paper submitted for consideration for this special issue went through a rigorous peer review process, with each submission receiving at least three reviews from experts in the domain. These reviews provided detailed and insightful comments on the quality of the submitted papers. Based on the referee reports, we carefully selected six high-quality papers for inclusion in this special issue.

Security architectures in VANETs are discussed by Casola et al. in their paper "An interoperability system for authentication and authorisation in VANETs", and by Coronado and Cherkaoui in "A secure service architecture to support wireless vehicular networks". In particular, the former paper proposes an interoperability system to enable the communication between VANET nodes in different and mutually untrusted domains. The latter paper primarily considers an approach to securely deliver information services provided by roadside infrastructure. A secure service provisioning architecture is presented, discussed and analysed.

In the paper "A vehicle gateway to manage IP multimedia subsystem autonomous mobility" authored by Radier et al., an autonomic architecture is proposed to facilitate the connectivity between VANET and IP multimedia subsystem. Vehicular mobility, connection hand-off and authentication issues are addressed simultaneously, and a middleware called knowledge plane is introduced for achieving better quality of IMS service.

In the paper entitled "Reputation in anonymous vehicular networks", a framework is developed by Miranda and Rodrigues to deal with the implicit relationships between anonymity and reputation problems. The framework allows VANET nodes to exchange their information and infer reputation scores without disclosing real identities, it also provides tamper-resistance guarantee. Chaurasia and Verma address another challenge associated with anonymity in their paper "Maximising anonymity of a vehicle", namely, how to achieve anonymity for a moving vehicle that continually switches identifiers. Since a vehicle's environment is frequently updated as the neighbours, its anonymity can be reduced. The authors study the possibility that node may keep or even enhance its anonymity by changing its pseudonym to reduce the implicit relationship between its environment and identity.

A destructive attack, false data injection, is specifically addressed by Cao et al. in paper "Filtering false data via authentic consensus in vehicle *ad hoc* networks". Successful attacks may allow a driver to disseminate false information to the other drivers and disrupt VANET operations. As a countermeasure, a security scheme based on the notion of proof-of-relevance is proposed for achieving authentic consensus among a group of authenticated witnesses of an event.

We would like to thank all reviewers for their time and effort in reviewing all the assigned papers on time, and providing invaluable comments and suggestions to the authors to improve their papers. We would also like to thank all authors who submitted their papers for consideration for this special issue. We express our gratitude to the Editor-in-Chief, Professor Thanos Vasilakos, for his encouragements and support throughout the preparation of this issue. We hope this special issue will contribute to the advancement of security and privacy research in VANET areas.