Guest Editors’ Introduction: Special Issue on Reliable and Secure VANETs

Alexey Vinel, Xiaomin Ma, and Dijiang Huang

VEHICULAR ad-hoc networks (VANETs) has gained a significant attention during the last decades both from industrial and academia communities. Novel VANET-enabled active safety automotive applications are heavily dependent on reliability and security of underlying inter-vehicle communication protocols. The error-prone nature of the wireless channel and its openness to external invasions as well as dynamic VANET environment, impose the need for intensive studies before applications like platooning or collision avoidance can become a part of our daily life. The aim of this Special Issue is to encompass research advances in all areas of reliability and security in VANETs. The 11 papers comprising this Special Issue provide contributions related to the novel protocols for reliable and secure vehicle-to-vehicle and vehicle-to-infrastructure communication as well as methods for their performance evaluation.

Cooperative driving applications are based on an underlying vehicular-WiFi extension (i.e., ITS-G5/DSRC) known for its unreliability and unbounded delay. Few contributions discuss the protocol design in VANETs to meet the Quality-of-Service (QoS) requirements:

- The paper “V2V QoS Guaranteed Channel Access in IEEE 802.11p VANETs” by Chang et al. proposes a distributed and priority enforced channel access scheme, called EDF-CSMA, to provide guaranteed QoS for real-time streaming in multi-channel VANET environments. It is shown that EDF-CSMA has higher channel utilization than other well-known mechanisms.

- Starting from the observation - confirmed during experiments - that ITS-G5/DSRC packet losses are correlated in time and space, the paper “Random Transmit Power Control for DSRC and its Application to Cooperative Safety” by Kloiber et al. proposes an innovative solution for congestion/awareness control by using a randomized transmit power strategy opposed to current fixed power strategies. Already successfully used in different domains, this unconventional approach shows several benefits, such as packet loss decorrelations, channel load reduction, and even support for ultra-high transmit updates (> 10 Hz) at a 60 percent operational channel load.

- In “Secure and Robust Multi-Constrained QoS aware Routing Algorithm for VANETs” by Eiza et al. the authors propose an ant colony optimization technique to compute the best feasible routes in VANETs subject to multiple QoS constraints determined by the data traffic type is suggested. The authors apply the VANET-oriented evolving graph model to perform plausibility checks on the exchanged routing control messages among vehicles.

- The paper “Securing Vehicular IPv6 Communications” by Fernandez et al. investigates the security design in VANETs and the proposal of integrating state-of-the-art IPv6 technologies to create a secure vehicular mobile network. The implementation and experimental evaluation of the proposal in a vertical handover scenario between 3G and IEEE 802.11p are carried out.

- Huang et al. focuses on channel spectrum availability sensing for cognitive radio enabled VANETs in the paper entitled “Historical Spectrum Sensing Data Mining for Cognitive Radio Enabled Vehicular Ad-hoc Networks”. A new scheme is proposed for channel availability prediction using historical spectrum sensing data mining, Bayesian inference, and a non-parametric hidden Markov chain model. The cognitive radio enabled VANET with the new proposed spectrum sensing can improve the application-level QoS for safety services.

The use of traditional symmetric cryptography in VANETs is discussed in the following papers:

- “PBA: Prediction-based Authentication for Vehicle-to-Vehicle Communications” by Lyu et al. discusses broadcast authentication issue for secure one-hop vehicle-to-vehicle communications. A new broadcast authentication scheme – Prediction-based Authentication – built on symmetric cryptography, is designed to defend against computation-based denial-of-service attacks and resist packet losses caused by high mobility of vehicles. The authors analyze the security of the proposed scheme under varying vehicular network scenarios.

- Li et al. devote their paper “Impossible Differential Fault Analysis on the LED Lightweight Cryptosystem in the Vehicular Ad-hoc Networks” to the security analysis of LED lightweight cryptosystem in VANETs against
the impossible differential fault analysis (IDFA) attack with a half byte-oriented fault model. The analysis allows breaking the 64-bit and 128-bit secret key of LED by only 48 and 96 faults in average, respectively. The result proves that LED is vulnerable to a half byte IDFA.

In VANETs all the vehicles broadcast messages about their current location, speed and direction. Even though this enables safety applications, it also raises privacy concerns. Pseudonyms management is considered in two papers:

- Zhang et al. present “MixGroup: Accumulative Pseudonym Exchanging for Location Privacy Preservation in Vehicular Social Networks”, where a novel privacy-preserving scheme, called MixGroup, which is able to efficiently exploit the sparse meeting opportunities for pseudonym changing based on real-traces observations, is proposed. By integrating the group signature mechanism, MixGroup constructs extended pseudonym-changing regions. Then, vehicles are allowed to successively exchange their pseudonyms. Results indicate that MixGroup significantly outperforms the existing schemes in both high traffic and low traffic conditions.

- “A pseudonym management system to achieve anonymity in vehicular Ad hoc networks” by Artail and Abbani introduces a system for pseudonym generation, distribution, and replenishing to provide anonymity to communicating cars in the VANET. The roadside units play a key role not only by distributing pseudonym sets to cars, but also by shuffling the sets amongst themselves to maximize anonymity. The distribution of pseudonym to the roadside units and to the vehicles is highly adaptive to accommodate the needs of the vehicles. A distributed optimization algorithm is developed to manage the shuffling process, and a novel mechanism was devised for cars to change their pseudonyms.

Finally, some specific VANET applications are studied from the security perspective:

- The paper “Trustworthy Parking Communities: Helping Your Neighbor to Find a Space” by Timpner et al. tackles the challenge of securely exchanging parking spot availability information with neighbors. The high-performance state-of-the-art encryption and signature algorithms as well as a mathematical trust rating model are used to set up Parking Communities for providing a novel trust management for vehicular parking applications without reliance on a central Trusted Third Party for retrieving trust ratings. This approach allows end-to-end encrypted request-response communications in combination with geocast and can be used as an overlay to existing vehicular networking technologies. Attack scenarios on Parking Communities and their mitigations are analyzed. A comprehensive comparison with existing key and trust management schemes for vehicular networks are provided to verify feasibility of the proposed concept.

- Vehicles-to-grid (V2G) is recognized to be one of the most emerging technologies, which can be used for making an energy balance between producers and consumers. To provide secure negotiation between these two parties, Lee et al. in the article entitled “Bayesian Coalition Negotiation Game as a Utility for Secure Energy Management in a Vehicles-to-Grid Environment” propose a novel Bayesian coalition game based technique in V2G environment. Keeping in mind the modern demands for an optimal energy consumption, the authors assume vehicles as the player of the game, which perform finite number of actions with respect to the energy flow between consumers and producers. The efficacy of the proposed scheme is evaluated by selecting various performance evaluation parameters where its performance was found satisfactory with respect to the selected parameters.

A. Vinel
X. Ma
D. Huang
Guest Editors

Alexey Vinel received the bachelor’s (hons.) and master’s (hons.) degrees in information systems from the Saint-Petersburg State University of Aerospace Instrumentation, Saint Petersburg, Russia, in 2003 and 2005, respectively, and the PhD degrees in technology from the Institute for Information Transmission Problems, Moscow, Russia, in 2007, and the Tampere University of Technology, Tampere, Finland, in 2013. He is a full professor of data communications in the School of Information Technology (ITE) of Halmstad University, Halmstad, Sweden. He has been involved in research projects on vehicular networking standards, advanced driver assistance systems, and autonomous driving. He has been an associate editor of the IEEE Communications Letters since 2012 and the IEEE Wireless Communications Magazine since 2015. He is a senior member of the IEEE.
Xiaomin Ma received the MS degree in communication and electronic system, the Beijing University of Aerospace and Aeronautics, Beijing, China, and the PhD degree in information engineering at the Beijing University of Posts & Telecommunications. He was a postdoctoral fellow in the Department of Electrical and Computer Engineering at Duke University, North Carolina. He is a full professor in the Department of Engineering at Oral Roberts University. His research interests include stochastic modeling and analysis of computer and communication systems, physical layer and MAC layer of vehicular ad hoc wireless networks, computational intelligence and its applications to coding, signal processing, and control, and Quality of Service (QoS) and call admission control protocols in wireless networks. He has published more than 100 papers in peer-reviewed journals and conferences. He also holds a US patent. He received the Best Paper Award in IEEE International Conference on Network Infrastructure and Digital Content. He gave several invited lectures and tutorials in US and foreign universities as well as on international conferences. He is in the editorial board of International Journal of Vehicular Technology, Hindawi Publish House. Also, he has been serving as a guest editor of Special Issues in several international journals such as ACM/Springer Mobile Networks & Applications (MONET), and IEEE Transactions on Dependable and Secure Computing, etc. He is (or was) PI, Co-PI or a project leader in several projects sponsored by US National Science Foundation (NSF), NSF EPSCoR, Motorola, Chinese NSF, AFOSR, and ARO, etc. He is a senior member of the IEEE.

Dijiang Huang received the bachelor of science degree in telecommunications from the Beijing University of Posts & Telecommunications in 1995, and the master of science and PhD degrees from the University of Missouri-Kansas City in 2001 and 2004, respectively, both majored in computer science and telecommunications. He joined ASU in 2005 in the Department of Computer Science and Engineering as an assistant professor. From 2011, he has been an associate professor in the School of Computing Informatics and Decision Systems Engineering. His current research interests are in computer and network security, mobile ad hoc networks, network virtualization, and mobile cloud computing. He is an associate editor of the Journal of Network and System Management (JNSM) and an editor of the IEEE Communications Surveys & Tutorials. He has served as an organizer for many International conferences and workshops. His research is supported by federal agencies US National Science Foundation (NSF), ONR, NRL, ARO, and NATO, and organizations such as Consortium of Embedded System (CES), Hewlett-Packard, and China Mobile. He received the ONR Young Investigator Program (YIP) Award 2010, HP Innovation Research Program (IRP) award 2011 and 2012, and JSPS Fellowship 2013. He is a cofounder of Athena Network Solutions LLC (ATHENETS). He is currently leading the Secure Networking and Computing (SNAC) research group at ASU. He is a senior member of the IEEE.

For more information on this or any other computing topic, please visit our Digital Library at www.computer.org/publications/dlib.