

# Misbehavior Detection Systems and Security for Vehicular Communication Networks

Yi Qian, Ph.D.

Professor

University of Nebraska-Lincoln

Omaha, NE 68182

Web: <http://cns.unl.edu/yqian>

Email: [yi.qian@unl.edu](mailto:yi.qian@unl.edu)

***Abstract*** – Vehicular communication networks are susceptible to various security attacks. Due to the wireless nature of vehicular communications, how to secure vehicular networks are great challenges that have hampered the implementation of vehicular services. Many solutions have been proposed by researchers and the industry in the recent years. In this tutorial, we first present an overview of security issues for vehicular networks, followed by a survey on the state-of-the-art solutions on security for vehicular networks. After that, we present a new study on misbehavior detections in vehicular communication networks by introducing machine learning and reputation-based misbehavior detection systems to enhance the detection accuracy as well as to ensure the reliability of both vehicles and messages. Misbehavior detection systems are trained using datasets generated through extensive simulation based on the realistic vehicular network environment. We show that various machine learning schemes can be exploited in accurately identifying several misbehaviors in vehicular networks.

***Keywords*** - Security, machine learning, misbehavior detection system, vehicular communication network.

## I. SHORT BIO OF THE TUTORIAL PRESENTER

Yi Qian received a Ph.D. degree in electrical engineering from Clemson University, in South Carolina, USA. He is currently a professor in the Department of Electrical and Computer Engineering, University of Nebraska-Lincoln (UNL). Prior to joining UNL, he worked in the telecommunications industry, academia, and government. Some of his previous professional positions include serving as a senior member of scientific staff and a technical advisor at Nortel Networks, a senior system engineer and a technical advisor at several startup companies, an assistant professor at the University of Puerto Rico at Mayaguez, and a senior researcher at the National Institute of Standards and Technology. His research interests include communication networks and systems, and information and communication network security. Prof. Yi Qian is a Fellow of IEEE. He was previously Chair of the IEEE Technical Committee for

Communications and Information Security. He was the Technical Program Chair for IEEE International Conference on Communications 2018. He serves on the Editorial Boards of several international journals and magazines, including as the Editor-in-Chief for IEEE Wireless Communications. He was a Distinguished Lecturer for IEEE Vehicular Technology Society and a Distinguished Lecturer for IEEE Communications Society.

Prof. Yi Qian received the Henry Y. Kleinkauf Family Distinguished New Faculty Teaching Award in 2011, the Holling Family Distinguished Teaching Award in 2012, the Holling Family Distinguished Teaching/Advising/Mentoring Award in 2018, and the Holling Family Distinguished Teaching Award for Innovative Use of Instructional Technology in 2018, all from University of Nebraska-Lincoln. He is the principal author of the textbook, "Security in Wireless Communication Networks", published by IEEE Press/Wiley in 2021.

## II. OBJECTIVES AND MOTIVATION

There have been many recent research activities to address the communication and networking capabilities in vehicles and transportation infrastructure. Vehicular communication networks together with existing vehicle sensing capabilities provide support for enhanced safety use cases, passenger infotainment and vehicle traffic optimization. Vehicular networks should support variety of use cases like forward collision warning, do not pass warning, queue warning, parking discovery, optimal speed advisory, curve speed warning, etc. On the other hand, the implementation of vehicular networks confronts many challenges especially security issues. For example, vehicular networks are susceptible to various attacks from

malicious nodes within a network. The collaborative misbehavior detection system (MDS) can be used to detect these attacks. However, in a collaborative MDS, an attacker may send false feedback which affects the detection accuracy. A trust model can be used to stimulate vehicles to send true feedbacks, but an attacker can take advantage of weak or strong reputation update methods. A dynamic trust can be used to stimulate vehicles to send true feedbacks.

This tutorial covers the topics on the recent development of security for vehicular communication networks. The tutorial starts with an overview of security issues for vehicular networks at first, followed by a survey on the state-of-the-art solutions on security for vehicular networks. After that, we present two case studies on misbehavior detections in vehicular communication networks, one by introducing machine learning and reputation-based misbehavior detection systems to enhance the detection accuracy as well as to ensure the reliability of both vehicles and messages, another by introducing a deep reinforcement learning based dynamic reputation policy for misbehavior detections vehicular networks. These types of misbehavior detection systems are trained using datasets generated through extensive simulation based on the realistic vehicular network environment. We show that various machine learning schemes can be exploited in accurately identifying several misbehaviors in vehicular networks.

## III. PROPOSED DURATION

Half day

3 hours of instruction

#### IV. INTENDED AUDIENCE

Graduate students, professors, researchers, scientists, practitioners, engineers, industry managers, consultants, and government agencies.

#### V. A DESCRIPTION OF THE TECHNICAL ISSUES THAT THE TUTORIAL WILL ADDRESS

In the first half of this tutorial we will survey the security issues of vehicular networks and the recent solutions on security for vehicular networks. After that, we will focus on the application of machine learning and deep reinforcement learning algorithms for a very important type of security mechanisms, misbehavior detection systems, for vehicular communication networks. This part of the tutorial will present a most recent research result of the tutorial speaker, as described below.

Since a vehicular network is susceptible to various attacks from malicious nodes within the network, a collaborative misbehavior detection system (MDS) can be used to detect these attacks. However, in a collaborative MDS, an attacker may send false feedback which affects the detection accuracy. A trust model can be used to stimulate vehicles to send true feedbacks, but an attacker can take advantage of weak or strong reputation update methods. A dynamic trust can be used to stimulate vehicles to send true feedbacks. In this talk, we present our latest research result on misbehavior detection in cellular based vehicular communication networks, by introducing a machine learning and reputation based MDS to enhance the detection accuracy as well as to ensure the reliability of both vehicles and messages. The proposed MDS is trained using datasets generated through extensive simulation based on the realistic vehicular network environment. To improve the accuracy of the detection, we have employed the Dempster-Shafer (DS) theory-based collaborative misbehavior detection system. In the

proposed scheme, the reputation score of each vehicle is used as a belief value for Dempster-Shafer based feedback combination. In addition, we propose a beta distribution-based reputation update and revocation scheme. Moreover, we show that our proposed scheme is better compared to previous methods in terms of accurately identifying various misbehaviors.

#### VI. OUTLINE OF THE TUTORIAL CONTENT & TENTATIVE SCHEDULE

1. Introduction of vehicular communication networks and security issues  
(30 minutes)
  - a. Vehicular communication networks and applications
  - b. Security requirements for vehicular communication networks
  - c. Security attacks for vehicular communications networks
2. Current state-of-the-art in security for vehicular networks  
(80 minutes)
  - a. Security mechanisms in vehicular networks
  - b. Authentication
  - c. Availability
  - d. Confidentiality and Integrity
  - e. Authorization
  - f. Privacy
3. Machine learning and reputation-based misbehavior detections  
(60 minutes)
  - a. Motivations
  - b. The vehicular communication network architecture

- c. Overview of machine learning and reputation-based misbehavior detections
  - d. Attacker models
  - e. Reputation system
  - f. Machine learning based detections
  - g. Simulations and performance evaluations
  - h. Summary
4. Conclusions and Future Challenges  
(10 minutes)

## VII. PREVIOUS TUTORIAL DELIVERY OF THE SPEAKER

Yi Qian has given several tutorials in various IEEE conferences recently:

1. Yi Qian, "Authentication Protocols for Next Generation Wireless Networks", IEEE GLOBECOM 2021, 9:00 - 12:30 CET (MADRID TIME) December 7, 2021. (Online)
2. Yi Qian, "Secure Protocol Designs for Next Generation Wireless Systems", IEEE VTC 2021-Fall, September 27-30, 2021. (Online)
3. Yi Qian, "Security and Privacy for V2X Communications", IEEE VTC 2020-Spring, May 25, 2020, Antwerp, Belgium. (Online).
4. Yi Qian, "V2X Communications and Security", IEEE VTC 2019-Fall, 2:00 pm - 5:30 pm, September 22, 2019, Honolulu, Hawaii, USA.
5. Yi Qian, "Cellular-Based V2X Communications", IEEE ICC 2019, 2:00 pm – 5:30 pm, May 20, 2019, Shanghai, China.
6. Yi Qian, "4G and 5G based V2X Communications", IEEE VTC 2018-Fall, 9:00 am – 12:30 pm, August 27, 2018, Chicago, USA
7. Yi Qian, "Challenges and Solutions for LTE and 5G based V2X Communications", IEEE/CIC 2018, 9:00 am – 12:30 pm, August 16, 2018, Beijing, China.
8. Yi Qian, "Challenges and Development for 5G Wireless Network Security", IEEE GLOBECOM 2017, Singapore, 2:00 pm - 5:30 pm, December 8, 2017.
9. Yi Qian, "Security for 5G Wireless Communication Systems - Recent Development and Challenges", IEEE LATINCOM 2017, Guatemala City, Guatemala, 10:45 am – 17:30 pm (5 hours) November 8, 2017.
10. Yi Qian, "Security for 5G Wireless Network Systems", IEEE VTC 2017-Spring, Sydney, Australia, 8:30 am - 12:00 noon, June 4, 2017. With 20 registered attendees.
11. Yi Qian, "Security for 5G Wireless Network Systems", IEEE ICC 2017, Paris, France, 2:00 pm - 5:30 pm, May 25, 2017. With 8 registered attendees.
12. Yi Qian, "Security for Next Generation Mobile Wireless Networks", IEEE VTC 2016 Spring, Nanjing, China, 8:30 am - 12:00 noon, May 15, 2016. The classroom was full, with about 25 registered attendees.
13. Rose Qingyang Hu and Yi Qian, "Recent Advances in Communication Infrastructures for Smart Grid", IEEE ICC 2014. The classroom was full of the attendees.
14. Rose Qingyang Hu, Yi Qian, Qian Li, "Towards Spectrum and Energy Efficient Heterogeneous Wireless Networks", IEEE WCNC 2013. The classroom was full of the attendees.
15. Dusit Niyato, Rose Qingyang Hu, Ekram

Hossain, Yi Qian, “Communications and Networking for Smart Grid Systems”, IEEE GLOBECOM 2011. With more than 100 attendees.

16. Yi Qian, and David Tipper, “Security and Dependability of Networked Information Systems”, IEEE ICC 2008. With 10 registered attendees.
17. Yi Qian, “Security and Survivability and Their Interactions for Wireless Networks”, IEEE VTC 2008-Spring. With 8 registered attendees.

#### REFERENCES

- [1] Yi Qian, Feng Ye, and Hsiao-Hwa Chen, *Security in Wireless Communication Networks*, John Wiley/IEEE Press, 2021.
- [2] J. Huang, D. Fang, Y. Qian, R. Q. Hu, “Recent Advances and Challenges in Security and Privacy for V2X Communications,” IEEE Open Journal of Vehicular Technology, Vol.1, No.1, pp.244-266, June 2020.
- [3] S. Gyawali, S. Xu, Y. Qian, R. Q. Hu, “Challenges and Solutions for Cellular based V2X Communications,” IEEE Communications Surveys and Tutorials, Vol.23, No.1, pp.222-255, First Quarter 2021.
- [4] S. Gyawali, Y. Qian, R. Q. Hu, “Machine Learning and Reputation based Misbehavior Detection in Vehicular Communication Networks,” IEEE Transactions on Vehicular Technology, Vol.69, No.8, pp.8871-8885, August 2020.
- [5] S. Gyawali, Y. Qian, R. Q. Hu, “Deep Reinforcement Learning based Dynamic Reputation Policy in 5G based Vehicular Communication Networks,” IEEE Transactions on Vehicular Technology, Vol.70, No.6, pp.6136-6146, June 2021.
- [6] D. Fang, Y. Qian, and R. Q. Hu, “Security for 5G Mobile Wireless Networks,” IEEE Access, Vol.6, pp.4850-4874, February 2018.