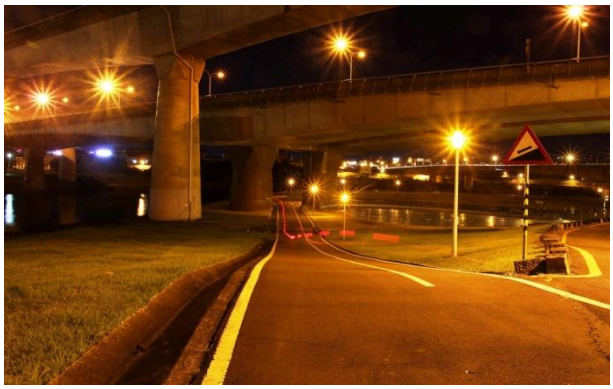
Secure and Safe Automated Vehicle Platooning

Jiafa Liu
University of Michigan-Dearborn
jiafal@umich.edu

Di Ma
University of Michigan-Dearborn
dmadma@umich.edu

André Weimerskirch
Lear Corporation
aweimerskirch@lear.com

Haojin Zhu
Shanghai Jiao Tong University
zhu-hj@cs.sjtu.edu.cn



Abstract - Cooperative adaptive cruise control (CACC) or platooning recently becomes promising as vehicles can learn of nearby vehicles' intentions and dynamics through wireless vehicle to vehicle (V2V) communication and advanced on-board sensing technologies. The complexity of automated vehicle platoon system opens doors to various malicious cyber attacks. Violation of cybersecurity often results in serious safety issues as been demonstrated in recent studies. However, safety and security in a vehicle platoon so far have been considered separately by different sets of experts. Consequently no existing solution solves both safety and security in a coherent way.

In this article, we show cyber attacks on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems (CPS). Based on a deep comprehension on the interrelation of safety and security, we present a safety-security co-design engineering process to derive functional security requirements for a safe automated vehicle platoon system. Finally we offer a vision of the future research issues on this important area of automated and connected vehicles.

Keywords - IoT security, vehicle to vehicle communication, cyber physical systems

I、INTRODUCTION

Vehicle platooning has been studied as a method of increasing the capacity of roads since the 1960's. In a vehicle platoon, a group of vehicles, following one another, acts as a single unit through coordinated movements. Because vehicles in a platoon travel together closely yet safely, this leads to a reduction in the amount of space used by the number of vehicles on a highway, thus has the great potential to *maximize highway throughput*. Cooperative adaptive cruise control (CACC) or automated vehicle platooning recently becomes promising as vehicles can learn of nearby vehicles' intentions and dynamics through wireless vehicle to vehicle (V2V) communication and advanced on-board sensing technologies. Automation-capable vehicles in tightly spaced, computer-controlled platoons offer additional benefits such as *improved mileage and energy efficiency* due to reduced aerodynamic forces, as well as increased *passenger comfort* as the ride is much smoother with fewer changes in acceleration.

The complexity of an automated vehicle platoon system – including inter-vehicle communications, vehicle's internal networking and its connection to external networks, as well as complicated and distributed platooning controllers – opens doors to malicious attacks. A number of research has demonstrated various attacks targeting every component of the platoon system [2], [8], [9], [14]. All these attacks could cause a wide array of problems in a deployed platoon, for example, an attacker could cause crashes, reduce fuel economy through inducing oscillations in spacing, prevent the platoon from reaching its (or each individual's) destination(s), or cause the platoon to break up. The full potential of automated vehicle platooning will not be realized until the issues related to communication and application security can be satisfyingly resolved.

The violation of cybersecurity could result in serious safety violations such as car crashes in a cyber physical system. However, safety and security in a vehicle platoon have so far been considered separately by different sets of experts. On one hand, the safety discipline usually considers system failures (including systematic/random hardware and systematic software failures) or natural disasters as safety hazard

resources. Safety solutions developed are usually not evaluated in an adversarial environment. On the other hand, the security discipline considers various attacks that can lead to different consequences such as loss of life, loss of privacy, financial loss, etc. The variety of security goals to address different types of attacks makes it very unlikely to be aligned with the goal of safety. Consequently security solutions proposed are rarely evaluated in terms of safety. For example, the model-based detection scheme [8], the only scheme proposed so far for platoon security, is designed from the **security point of view** by monitoring any misbehavior of the proceeding car. Although the scheme is able to detect vehicle misbehavior, whether it can lead to a safe platoon is not answered. To date, no existing platooning solution solves both safety and security in a reconciled and coherent way.

The need for a safety and security co-design is urgent today with the practicality of automated vehicle platooning technology. Actually there has been calls long ago for safety and security communities to work together [4]. Past efforts in the automotive industry have reached a consensus that functional safety hazards can arise from malicious activities in addition to systematic failures and random hardware failures [5]. So security should be considered as a pre-requisite for safety while safety should be one of the driving forces for security design. Although a couple of works have described a safety and security engineering process [5], [7], a lot of challenges need to be addressed to come up with a concrete safe and secure platoon system: How to reconcile different safety and security risks? How to align the goal of security with that of the safety? The most important, how to arrive at a solution that satisfies both the safety and security requirements? There are also performance challenges such as efficiency, real time, as well as maintaining the string stability of platoon.

In this article, we show cyber attacks on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems (CPS). Based on a deep comprehension on the interrelation of safety and security, we present a safety-security co-design engineering process to derive functional security requirements for a safe automated vehicle platoon system. Finally we offer a vision of the future research issues on this important area of automated and connected vehicles.

II、SECURITY-INDUCED SAFETY RISK ANALYSIS

The EU project EVITA provides a risk model to measure the safety risks of in-vehicle systems [1]. The risk analysis rationale of EVITA is that as it is too costly to protect against every threat, it is necessary to rank risks in order to prioritize countermeasures. Risk associated with a security attack depends on (1) **severity** of impact and (2) **probability** of successful attack. In this section, we analyze the severity as well as the probability of platooning attacks by using the EVITA model.

In response to various safety risks, ISO 26262 severity classification defines four severity levels (S0, S1, S2 and S3) in terms of the estimated personal injury that could result from the risk. S0 refers to no injuries. S1 refers to light or moderate injuries. S2 means severe to life-threatening injuries (survival probable). S3 means life threatening (survival uncertain) or fatal injuries. The EVITA model extends the ISO 26262 safety classification by including a fifth level S4 which means fatal injuries of **multiple vehicles** as cyber security attacks may have more widespread implication than unintended hardware or software bugs can cause.

Previous work has shown that many cyber attacks (such as message falsification attack, remote control attack, etc.) can result in serious safety issue. However, it is not clear the severity level of such attacks. To understand the severity level of a collision that resulted from a cyber attack, we introduce a new attack called leader crash attack by extending the collision induction attack proposed in [8]. In the leader crash attack, the leading car stops suddenly (intentionally or not) and causes the following cars to crash over each other. This crash attack can be mounted by any insider, not just the leader, in the platoon. However it is very likely a crash attack induced by the leader can have the most severe consequence.

We firstly argue collision induction attack is very possible (**probability**). It has been demonstrated successfully on several modern vehicle models that an attacker can totally control a vehicle by compromising its hardware or software locally or remotely through a wide range of attack vectors [6], [10]–[12]. When a leader or any insider of the platoon is compromised and can be remotely controlled, an attacker can issue an instruction to the victim vehicle to brake abruptly so that the following cars will crash into the front ones. The risk of insider crash attack will become more serious with the advancement in vehicle automation. If an insider car is a compromised driverless automated vehicle, such an attack can be mounted with severe consequence at a low cost. Also, we do not exclude the case when the driver himself is reckless.

We use the PLEXE simulator to demonstrate the consequence of this attack (**severity**). PLEXE is an Open Source extension to the known and widely used Veins simulation framework by adding platooning capabilities and controllers. In this simulation, initially a platoon of four vehicles is driving at the speed of 100 km/h with a gap of 5 meters. At the time of 50s, we instruct the leader vehicle to stop. We set the deceleration of the leader car extremely large so that the speed can decelerate to zero in a very short time interval. In this way, the leader vehicle acts just like it suddenly hits the brake so that it stops immediately. We see how the following

vehicles will respond under the CACC controller strategy. From the mobility traces of the platoon collected, we can we can see that following vehicles crash into preceding vehicles at 50.41s, 50.75s and 51.10s respectively.

To obtain an insight of speed changing of the platoon in the crash, we utilize the statistics collected from PLEXE which are shown in Figure 1. In Figure 1, Vehicle 0 with the red line is the leader vehicle. Vehicle 0 decelerates from 100 km/h (27.77 m/s) to 0 km/h in a very short time interval. The following vehicles are trying to prevent crash by decelerating, but the 5-meter gap is not long enough for them to fully stop before they crash into the car before it. The above three lines terminating at different time spot shows that each of them has crashed into the leader vehicle.

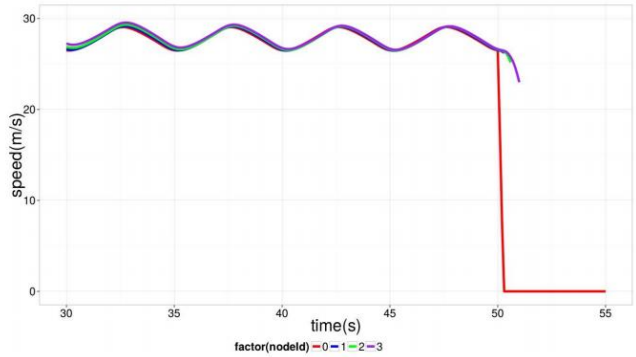


Fig. 1: Speed Changes of Platoon during the Crash

More on severity. The above simulation clearly demonstrates that the leader car crash attack can potentially result in multiple car damage and life injuries and has the highest level of safety severity. However, the maximum safety impact of security attack demonstrated is only a **local** event to several vehicles. We believe the worst security impact can potentially be *nation-wide* impacting thousands or millions of cars and suggest a new severity level of **S5: nation-wide wide spread and harmful impact**. For example, in the platoon context, suppose there is a security weakness that has an impact due to forged DSRC messages, also suppose future smartphones are DSRC enabled and malware spread on smartphones, we can easily see a nation-wide attack platform to attack the platoon mechanism.

Due to the severity and probability of security attacks on platoon systems, we strongly argue the importance of designing safe and secure platoon systems.

III、SAFETY-SECURITY CO-DESIGN

Safety has a long tradition in many engineering disciplines and has had successful standardization efforts. In automotive systems, the international standard ISO 26262 [15] is the state of the art standard for safety critical system development. Automotive security has evolved quite recently with networked systems and concerns about privacy, data integrity, authenticity and protection. As long as safety critical systems were not networked, the two fields did not have to interact and as a result, the two domains have evolved separately so far with little overlap. As cyber-physical systems evolved into networked systems, security became a relevant issue for safety critical systems.

The Vehicle Cybersecurity Systems Engineering Committee of SAE has been working on J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems [13]. J3601 is an overall guidebook on implementing cybersecurity for the entire vehicle. The safety-security co-design is being discussed in the secure software SAE committee at the moment and there is no final product yet. We are able to work with several key members of the SAE cybersecurity committee to understand the concepts and requirements as well as discuss the proposed safety-security engineering process.

We propose a safety-security co-design engineering process which consists of four main steps: (1) Define the safety goal for the system; (2) Define attack model; (3) Derive security goals; (4) Derive functional security requirements.

Safety Goal. Safety is very important in automotive industry and therefore highly regulated. For end users, it means that users do not face any risk or danger coming from the motor vehicle or its spare parts. Unacceptable consequences for safety are loss of human life and injuries. The safety goal of individual vehicle is to protect users from injuries and life threatening risks. In our context, we set up the safety goal of vehicle platoon as avoiding car collisions that can cause human life and injuries.

Attack Model and Security Goal. Unlike safety, cybersecurity has a broader range of unacceptable consequences such as human life and injury (safety), human security, financial loss, loss of privacy, etc. Figure 2 shows the interrelation of safety and security. From Figure 2, we can see that safety can be an objective (or impact) of a security attack. It can also be an unintended consequence caused by hardware or software bugs. Meanwhile, cyber security attacks can have different impacts. The intersection part concerns both safety and security, or safety-related security risks, which is of interest of this paper.

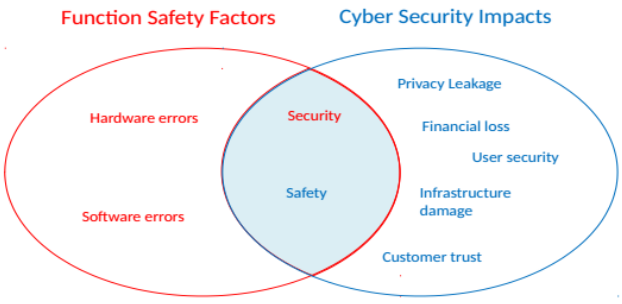


Fig. 2: Interrelation of Safety and Security

To derive our attack model that lead to safety, we summarize various of attacks, targeting at automotive platoon systems, proposed by researchers in the literature and their corresponding possible consequences in Table I. From the table, we can see that there are five attacks which can lead to car collisions, result in safety issues, and thus belong to the intersection in Figure 2. The security goal for a safe platoon is to develop a system that is resilient to these attacks.

Reference	Attack	Impact
[3]	Message falsification attack	Collision
	Message spoofing	Collision
	Message replay	Collision
	DoS (jamming)	Dissolved platoon
	System tampering	Collision
[8]	Collision induction attack	Collision
	Reduced headway attack	Decreased string stability
	Joining without radar	Decreased string stability
	Mis-report attack	Decreased performance
	Non-attack abnormalities	Decreased performance
[14]	Destabilization attack	Decreased string stability
	Platoon control taken attack	Dissolved platoon

TABLE I: Attacks and impacts

If a vehicle is a victim of *System tampering* attack, we mean an attacker is able to control the vehicle remotely through compromised hardware or software. The victim vehicle will behave like the one in either collision induction attack or message falsification attack, without the awareness and involvement of the driver. For us, we only need to focus on attack behaviors without worrying about who, the driver or a remote attacker, initiates the attack. Therefore in the following of the paper, we only consider collision induction attack and message falsification attack and ignore who initiates the attack.

Based on the discussion above, we derive an attack model emphasizing on safety of platoon as follows:
Adversary Model for Safety: We consider cyber attacks that can lead to safety issues such as car crashes in this work. Attacks that result in different consequences such as system performance, driver privacy, financial loss, etc. are not considered in this model as they can be treated in the regular way without considering safety. The adversary or the vehicle controlled by the adversary is part of the platoon system and thus is able to send valid V2V messages. However, there is no guarantee on the correctness of information in the messages it sends. Also the adversary does not need to follow the control law. The adversary is able to control one or more vehicles, including the leader, in the platoon. However, it cannot control all the radars or radar signals of vehicles in the platoon because of the line-of-sight requirement.

Functional Security Requirements.

From the analysis above, we can derive functional security requirements as follows:

- It shall not be able for an attacker to spoof a message;
- It shall not be possible to replay an old message;
- It shall not be possible for an attacker to broadcast a message with false information without being detected;
- The system shall be able to take a response action whenever a misbehavior is detected;
- The system shall ensure there is enough time for the system to respond.

IV、FUTURE RESEARCH ISSUES

The practical use of automated vehicle platooning systems relies on the security, safety, and reliability provided by such systems. Many existing techniques (such as cryptographic functions, secure hardware and software, etc.) can be used to defend against many attacks targeting a platoon system. Further work needs to be done to strengthen the security and safety aspects of such systems.

Securing platoon controllers. Stable coordinated movements in a platoon are described as string stability which ensures range errors decrease as they propagate along the stream of vehicles in a platoon to achieve constant inter-vehicle spacing. A lot of vehicle platooning control algorithms have been developed to achieve string stability. However, these algorithms have not been developed and analyzed under adversarial environment where an adversary wants to inhibit the performance of the control algorithm and hence cause instability of the system which may further cause intelligent collisions. It is clear that many potential attacks could happen to the underlying control algorithm. Thus it is important to systematically access the security risks/needs in automated platooning by looking at factors that affect, directly or indirectly, the coordinated movements of vehicles.

Resilient sensor fusion. There is a strong opinion today that a successful platoon will require wireless communication between vehicles for coordination. However, we believe that the wireless link is the weakest sensor of an automated car, compared to radar, LIDAR, and camera, and that it can easily be forged by a motivated attacker. Hence it seems that a vehicle in a platoon, and possibly an automated vehicle, must not rely on wireless communication if it has any impact to the vehicles control algorithms. Furthermore, it has recently been demonstrated that it is fairly easy to forge LIDAR and radar sensors by using a modulated laser. Hence we need strategies to fuse sensor input and detect forged individual input. One idea is to assign confidence levels to sensors (e.g. DSRC is lower than camera) and correct sensor input if individual sensors show unreasonable inputs based on the confidence

levels. Apparently more complex strategies are required to account for an attacker that will forge several sensors in parallel. It might be necessary to include some kind of heuristic, e.g. machine learning, to detect abnormal sensor input.

Securing the leader. The leader in a platoon is responsible for setting the trajectory and speed to the vehicles behind it. In a distributed platoon control algorithm, a vehicle adjusts its movements based on knowledge of the preceding vehicle and the lead vehicle to determine its next movement. Information of the preceding vehicle is usually direct hearing and can be further cross-verified with in-vehicle sensor data. However, information of the leading vehicle could be second-hand information — the vehicle might not be in the transmission range of the leader and receives the leaders status information indirectly from proceeding vehicles. It is important to protect the authenticity of messages of the leader and the leader itself to prevent leader impersonation. Especially, when a new car joins the platoon, the first task is to correctly identify the leader. Message authenticity has been well studied. It might be useful to have an endorsement mechanism to protect the leadership of the leader from being impersonated by using some efficient cryptographic primitives. The leadership is established through the endorsement of participating vehicles in the platoon. A vehicle who has endorsed the leader cannot deny its endorsement. An adversary should not be able to alter the endorsement even when it (and its collaborators) is one of the endorsers. A possible cryptographic primitive that can be used to protect leadership is aggregate signature scheme which allows multiple entities co-sign one document.

Securing the following vehicles. It appears that following vehicles need slightly different control and protection algorithms than the leading vehicle. The following vehicles cannot necessarily use their cameras which are the most resilient (against cybersecurity attacks) sensors, however, they are more dependent on the received wireless messages which are least reliable in terms of cybersecurity. Hence the control algorithms defined above will be revisited and refined for this case.

V、CONCLUSION

In this article, we show that cyber attacks on a platoon system can have the most severe and widespread safety impact as defined by the EVITA vehicle security risk model. We argue the importance of safety-security co-design for safety critical cyber physical systems and make the first effort toward a safety-security co-design engineering process which allows functional security requirements to be derived for a safe automated vehicle platoon system. We also offer a vision of the future research issues on this important area of automated and connected vehicles.

REFERENCES

[1] Evita: E-safety vehicle intrusion protected applications. http://www.evita-project.org/.

[2] Researcher hacks self-driving car sensors. http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors.

[3] M. Amoozadeh, A. Raghuramu, C. Chuah, D. Ghosal, H. Zhang, J. Rowe, and K. Levitt. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. *Communications Magazine, IEEE*, pages 126–132, 2015.

[4] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. on Dependent and Secure Computing*, 1:11–33, 2004.

[5] S. Burton, J. Likkei, P. Vembar, and M. Wolf. Automotive functional safety = safety + security. In *First International Conference on Security of Internet of Things (SecureIT 2012)*, 2012.

[6] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, and T. Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, 2011, August.

[7] B. Czemy. System security and system safety engineering: different similarities and a system security engineering process based on the ISO 26262 process framework. *SAE Int. J. Passeng. Cars - Electron. Electr. Syst.*, 6:349–359, 2013.

[8] B. DeBruhl. Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. In *Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2015.

[9] E. B. Hamida, H. Noura, and W. Znaidi. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics 4.3*, pages 380–423, 2015.

[10] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, and S. Savage. Experimental security analysis of a modern automobile. In *In Security and Privacy (SP), 2010 IEEE Symposium on (pp. 447-462). IEEE*, 2010, May.

[11] C. Miller and C. Valasek. Remote exploitation of an unaltered passenger vehicle. In *Black Hat USA*, 2015.

[12] I. Roufa, R. M., H. Mustafaa, T. Taylora, S. O., W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb. Security and privacy vulnerabilities of incar wireless networks: A tire pressure monitoring system case study. In *In 19th USENIX Security Symposium, Washington DC (pp. 11-13)*, 2010, February.

[13] SAE International. Cybersecurity guidebook for cyber-physical vehicle systems. http://standards.sae.org/wip/j3061/.

[14] D. Soodeh, R. M. Gerdes, and R. Sharma. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, 2015.

[15] I. Standards. Road vehicles – functional safety. http://www.iso.org/iso/home/store/catalogue tc/catalogue detail.htm?csnumber=43464.

AUTHOR BIOGRAPHY

Jiafa Liu is a graduate student in the Computer and Information Science Department at the University of Michigan-Dearborn. He is interested in vehicle security, platoon security and smartphone security. He received the B.S. degree in computer science from Shanghai Jiaotong University. He won the Shanghai Jiaotong University Scholarship Second Prize in 2014 and 2015.

Di Ma is an Associate Professor in the Computer and Information Science Department at the University of Michigan-Dearborn, where she leads the Security and Forensics Research Lab (SAFE). She is broadly interested in the general area of security, privacy, and applied cryptography. Her research spans a wide range of topics, including smartphone and mobile device security, RFID and sensor security, vehicular network and vehicle security, computation over authenticated/encrypted data, fine-grained access control, secure storage systems, and so on. Her research is supported by NSF, NHTSA, AFOSR, Intel, Ford, and Research in Motion. She received the PhD degree from the University of California, Irvine, in 2009. She was with IBM Almaden Research Center in 2008 and the Institute for Infocomm Research, Singapore in 2000-2005. She won the Tan Kah Kee Young Inventor Award in 2004.

Andre Weimerskirch is VP Global Cyber Security at Lear Corporation. Before that, André established the transportation cyber security group at the University of Michigan Transportation Research Institute (UMTRI), and co-founded the embedded systems security company ESCRYPT which was sold to Bosch in 2012. André is active in all areas of automotive and transportation cyber security and privacy, published numerous articles in the area of automotive and embedded cyber security, and is co-founder of the American workshop on embedded security in cars (escar USA). André is vice chair of the SAE Vehicle Electrical System Security Committee, and co-chairs the Michigan Mobility Transformation Center (MTC) cyber security working group.

Haojin Zhu received his B.Sc. degree (2002) from Wuhan University (China), his M.Sc. (2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. His current research interests include network security and data privacy. He published 33 international journal papers, including IEEE Trans. on Parallel and Distributed Systems, IEEE Trans. on Mobile Computing, IEEE Trans. on Wireless Communication, IEEE Trans. on Vehicular Technology, IEEE Wireless Communications, IEEE Communications, and 50 international conference papers, including ACM CCS, ACM MOBICOM, ACM MOBIHOC, IEEE INFOCOM, IEEE ICDCS, IEEE GLOBECOM, IEEE ICC, IEEE WCNC. He received a number of awards including: IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award (2014), Top 100 Most Cited Chinese Papers Published in International Journals (2014), Supervisor of Shanghai Excellent Master Thesis Award (2014), Distinguished Member of the IEEE INFOCOM Technical Program Committee (2015), Outstanding Youth Post Expert Award for Shanghai Jiao Tong University (2014), SMC Young Research Award of Shanghai Jiao Tong University (2011). He was a co-recipient of best paper awards of IEEE ICC (2007) and Chinacom (2008) as well as IEEE GLOBECOM Best Paper Nomination (2014). He serves as the Associate/Guest Editor of IEEE Internet of Things Journal, IEEE Wireless Communications, IEEE Network, and Peer-to-Peer Networking and Applications.