Indian Journal of Science and Technology, Vol 9(24), DOI: 10.17485/ijst/2016/v9i24/96027, June 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Cyber Security Issues in Connected Vehicle of Intelligent Transport System

Jinkeun Hong*

Division of Information and Communication, Baekseok University, South Korea;
jkhong@bu.ac.kr

Abstract

Background/Objectives: Requirement for security and safety with interest and growth to C-ITS application is increased. It is needed to security threat issue and risk consideration in the connected vehicle environment. **Methods/Statistical Analysis**: For efficient communication assistance of connected vehicle, the understanding and access of WAVE mode such as CCH, SCH for multi channel and WSMP specification are preferred in control, communication and signal processing for cooperative intelligence transport system. In security risk assessment and debugging, it is applied to reviewing of source code, analysis and evaluating of compliance, fuzzing and conducting of vulnerability. **Findings:** Main objectives of this article are to see risk issue and cyber threats in connected vehicle of ITS. Understanding for issues of risk assessment such as debugging, fuzzing, real time application, evaluating of compliance, connectivity and computational performance are required. Also for build up security of ITS it should be established guideline of ITS security factors such as PKI, security architecture, cost and interoperable solution. **Application/Improvements:** The risk assessment and cyber threats are basically emphasized guideline of ITS security and safety in terms of cyber security procedure and security considerations.

Keywords: Intelligence Traffic Security, Standard, Traffic, Vehicle Communication

1. Introduction

In Horizon 2020, it has objectives for information communication technology as follows: reduction of the injured person, fatality and traffic congestion/collision, enhancement of energy efficiency, transport schedule and availability of traffic information. Cooperative Intelligent Transportation System (ITS) is connected to Vehicle-to-Vehicle, Vehicle-to-Infrastructure and Vehicle-to-Nomadic Device. R. Moalla et al. present issue of cooperative ITS vehicle application oriented security framework[1]. Recently, smart city industry is increased focus of interest for each country and UAE has an interest in this area[2]. In addition, the interest of safety and security of ITS require efficient monitoring and alert scheme[3]. Against the ITS attack, the guideline is suggested securing goals such as hardware, software and communication (WIFI, 3G/4G/5G, Bluetooth etc.) between ITS device and device. Of course Defense in Depth (DiD) is required to whole ITS in respect with physical and system architecture. In the ITS standard, it is defined in IEEE1609.2 "trial use standard for WAVE security services for application and management messages". The multi channel of IEEE802.11p is consisted of Control Channel (CCH) and Service Channel (SCH). The CCH support broadcast communication and dedicated to short, high priority, data and management frames for safety critical communication with low latency and initialization of two-way communication. In case of SCH, it is consisted of two-way communication between roadside unit and on board unit or between OBU-OBU.

Also WAVE short message is suggested to Figure 1 and Figure 2 is over-air frame format[4].

The operation modes of IEEE802.11p are consisted of without WBSS and with WBSS. Without WAVE basic service set mode is safety critical and applied for low latency message and control message. Mainly without WBSS

*Author for correspondence

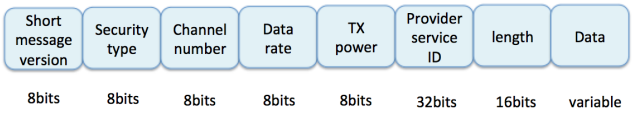

Figure 1. Frame format of WAVE short message.

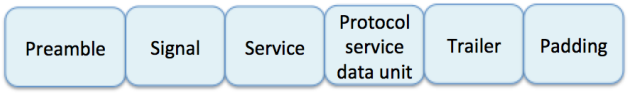

Figure 2. Over air Frame format of WAVE.

mode is broadcast and use on CCH only. But with WBSS mode is applied to two-way transaction and required to use a SCH and initiation on CCH. WBSS mode is not required to authentication and association procedures. The data plane of WAVE in each layer is as follows in Figure 3.

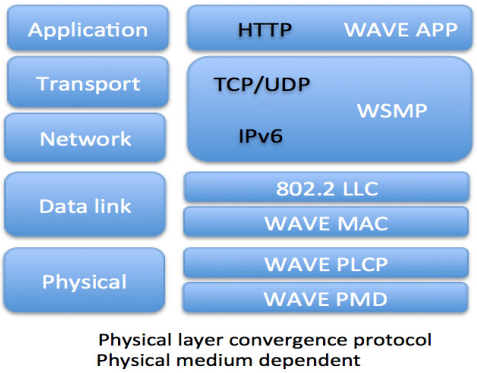

Figure 3. Data plane of WAVE.

IEEE802.11p is similar to PHY of IEEE802.11a (OFDM modulation) and MAC of IEEE802.11 (CSMA/CA), IEEE802.11e (MAC enhancement, which is considered message prioritization). The guard period of IEEE802.11p is longer than IEEE802.11a due to less inter symbol interference and better resistance against multi path error. Roadside unit has a fixed 48 bit MAC address and generate a random MAC address. Also it is used TCP/UDP on transport layer and Mobile IPv6 in IP based communication and is applied SCH for transmission only. In non-IP based communication, it is applied CCH or SCH for transmission and based on WAVE Short Message Protocol (WSMP). The WSMP can use CCH and SCH mode.

In the related research to security, Hong-Jong Jeong et al. reviewed the fast and secure mobility management scheme based on heterogeneity inclusion and mobility adaptation through locator ID split HIMALIS for cooperative ITS services in future networks[5]. HIMALIS architecture consists of edge node, global and logical control node. In the edge node, it is required to authenticate and access control. The flow of network is processed traffic between mobile node, roadside unit, authentication node for host authentication, local name server for resolution of ID, hostname and gateway. According to Hong-Jong Jeong, to authenticate first it is transmitted event information of router advertisement with ID from gateway to mobile node. Next RSU send to mobile node EXP request ID message and receive Extended Authentication Protocol (EAP) response message. And then access request message is transmitted to local name server and gateway through authentication node. Last from gateway, EAP information (ID, key) to authentication is sent to mobile node. Also Hong-Jong Jeong et al. described additional handover procedure to security. There used extended master key, re-authentication Root Key (rRK) and re-authentication Integrity Key (iIK) to authenticate. Then that approach was applied to adapt conventional authentication and handover procedure.

In this paper, we present cyber security issues of intelligent transport system. In Section 2, we illustrate cyber threats and risk of intelligent transport system. In Section 3, we present our concluding remarks.

2. Cyber Security Considerations in Connected Vehicle of Intelligent Transportation System

2.1 Cyber Threats of Intelligent Transport System

Henk Wymeersch et al. present about challenges for cooperative ITS and illustrated phase evolution about control (control strategy, optimization problem), communication (wireless media) and signal processing (sensor fusion and input)[6]. In the control area, there are controlled of ego vehicle and conservative (phase 1), limited coordination and aggressive control (phase 2), extensive coordination and scalability (phase 3) and full coordination and scalability (phase 4). In the communication area, there are considered limited communication and low density (phase 1), sharing of state data with delay and scalability

critical (phase 2), sharing of state and control date with delay and scalability critical (phase 3) and sharing of state and control data with delay and scalability critical (phase 4). In signal processing area, there are considered sophisticated sensors and high cost, estimation (phase 1), acted as sensor and reduced cost (phase 2), acted as sensor and reduced cost (phases 3 and 4). In vehicle system, the sensors are road condition, magnetic, vehicle distance, forward obstacle, blind spot monitoring camera, driver recorder, side obstacle, air pressure, inside door lock/unlock, rear obstacle, GPS, airbag, road-vehicle/V2V communication, rear view camera, driver monitoring, steering angle, electronic control throttle, electronic control brake, fire detection, vehicle speed and so on.

Pierpaolo Cincilla et al. present security of C-ITS messages and introduced IRT system ISE project[7]. First for implement security countermeasure to build up ITS, it is established guideline to implement security scheme PKI, design architecture of security, safety, cost, induce interoperable solution, support emergence of vehicle and develop trust relationship between cooperative systems.

Michael Feiri et al. describe pre-distribution of certificate in VANET and guide to parameter values such as field size (2.5 Km * 1 Km), MAC (802.11 p, 6 Mbps), fading (Rayleigh), path loss (two ray ground), noise (additive), simulation runs (5), transmit power (23 dBm), beaconing frequency (10 Hz), PKAlgorithm (NISTP256), ECC Key type (compressed), single Cert size (140 bytes), signature size (65 bytes)[8]. It shown that pre-distribution is more effective when vehicle change pseudonym. To robust authentication and pseudonymous communication, certificate is always added to beacon frame with location data. As like suggestion of Michael Feiri et al. it is required certificate pre-distribution scheme and induced to reduce certificate packet loss.

Chakkaphong Suthaputchakun and Aura Ganz presents secure priority based inter-vehicle communication MAC protocol[9]. For inter vehicle communication, it is concerned threats and risk factors. Therefore it is considered risk factors such as message forgery and reply, impersonation, privacy, jamming and interference, security requirements and security requirement which are included in authentication, integrity, non repudiation, messages freshness, anonymity and so on.

In the IT security center of IPA, it is guided to approaches for vehicle information security[10]. So by user operation, the case of threats is incorrect setting and virus infection. In attacker interference, threats are unauthorized use, unauthorized setting, information leakage, sniffing, DoS attack, tampered message, loss of logs and unauthorized relay. According to guideline, security measures are security architecture design for security function design, use of security functions such as encryption, authentication and access control to clarify, conduct and decide, secure coding which can be prevent known vulnerability for secure implementation, security test which can be detect known vulnerability for security assessment and provision of manuals. In each phase of vehicle, security level has level 1 ~ level 4. Level 1 is no security effort and level 2 is relegated personnel issue, level 3 and level 4 are considered as an organizational issue. In security assessment and debugging, it is consisted of reviewing source code, applying a static analysis, evaluating the compliance, fuzzing and conducting vulnerability assessment for region of cooperative intelligent transport system.

2.2 Cyber Risk in Connected Vehicle of Intelligent Transport System

Cyber risks for vehicle are limited vehicle external connectivity, limited computational performance, real time operation, vehicle which is consisted of various components, unpredictable attack scenarios and threats, hazard to drivers and passengers lives. For hazard assessment, ISO26262 is specified to risk analysis with exposure, controllability and severity about functions such as CD/DVD control, navigation, emergency Call, camera monitoring, air conditioner control, signal, power window, air bag and so on[11].

Also to guideline of vehicle cyber security, there are IEC62443 (IEC – industrial system), NIST-800-61 (NIST – industrial system and pc/internet), Guide to industrial control system security (NIST – industrial system), CIP (NERC – pc/internet and industrial system), EVITA (EU - vehicle), vehicle information security guide (agency IPA - vehicle) and J3061 (SAE - vehicle).

When it is understood category of vehicle security, it will be suggested and checked to modern vehicle security categorization examples such as power train (throttle valve data, CAN bus data message for the power control module, adaptive cruise control date, local interconnect network steering wheel data, ABS brake by wire data), vehicle safety (OBD II emissions data, TPMS data, firmware update over the air remote diagnostics data, airbag control unit data, GPS data) using NIST SP 800-60 and FIPS 199[12].

Pierre Kleberger et al. present security aspects (problems of weak protection in CAN and FlexRay protocols, architecture to modify protocols and provide integrity, intrusion detection systems with anomaly based and specification based scheme, honey pots which is separated from in-vehicle network, threats and attacks to classify connected car environment) of In-vehicle network[13]. Security problems of In-vehicle network are insufficient. As like Pierre Kleberger et al. when it is taken security problem of In-vehicle network, there are considered insufficient bus protection, weak authentication, misuse of protocols, poor protocol implementation and leakage of information.

Erland Jonsson and Laleh Pirzadeh describes framework for security metrics based on OS[14]. According to necessity of security metric for evaluation measure, the security metrics in the security model will be suggested protective security metrics that how could protective security be measured and behavioural security metrics those have reliability, availability, safety and confidentiality with/without latency.

Florian Sagstetter et al. describe security challenges in automotive architecture design[15]. The architecture of In-vehicle network has a category of Local Interconnect Network (LIN) for sub network, Control Area Network (CAN) for comfort, MOST for infotainment, CAN for safety and FlexRay for chassis. It is required to cryptographic function and physical protection scheme to ECU and firmware update process, connecting bus and gateway. It is emphasized the necessity of battery security (battery management system monitoring), protection of charging plug against intrusion access attack and protection from drive by wire functionality additionally. Also there will be considered to issues of Ethernet/IP and On Board (OBD) security, security and external mobility services and migration towards Ethernet/IP. OBD security is required to detect malware and consisted of malware detector, DB (whitelist/blacklist), activity monitor, reporter and manager.

Peter Knapik et al. reviewed security function based on V2X communication[16]. It was measured as preventive, protective, detecting and reactive method in the automotive type. The preventive method is preventive navigation, awareness campaigns, vehicle choice and vehicle decal. The protective method is system locking, vehicle armoring, electronic immobilizer utilizing. The detecting method is system alarm, vehicle bait and automatic number plate recognition usage. And reactive method is vehicle tracking system usage and remote disabling function.

Tao Zhang et al. describes defending connected vehicles against malware[17]. The main channel of communication is Bluetooth (unlicensed 2.4 GHz of very low power consumption and short range for hands free calling)/USB for user, smart phone to support calling and emergency call, 3G/4G cellular module for V2V/I2V, WiFi to telematics services of V2V local broadcasts and DSRC to integrate active safety services of large scale consumer vehicle networks. Then these channels are threated from attacks such as virus, worm, Trojan horse, spyware, ransom ware and root kit.

Francesco Alesiani presents towards collaborative mobility and approach main innovation those are three primary services (authentication, integrity and confidentiality), security and privacy – preserving categories (system security, communications security and location privacy protection), multimodal security solution, uses of result from singular communication modes, integrate different PKI solution, trust hierarchy for ITS, balanced processing effort[18]. As like Francesco et al. for secure primary service of connected vehicle, it will be emphasized use cases such as privacy protecting use cases (user profile, preservation, pseudonym linkage), protection of V2X communication channels (broadcast/unicast/aggregated), protection of local data and systems (storage/installation/interconnection) and derived security use cases (credentials)[19]. Today automotive ecosystem is focused on the factors as follows: Increasing of connected vehicles, sharing of electronic components in vehicle platform, connection of external/internal devices, integration of service and content, lack of security countermeasure. It have been occurred to attacks such as modified or dysfunctional attack for ADAS, Engine, steering, braking and airbag, man in the middle attack for vehicle bus communication and TCU, side channel attack for infotainment, TCU and comfort system, spoofing for DSRC and WiFi and compromised privacy attack for smart phone and connected services. However Cornelius Bittersohl[19] suggests value chain of attacker vector in respect of attack category, critical element of attack vector part.

First weak communication protection from external access will be tolerable to man in the middle attack.

Second weak countermeasure against access control about decompiling of software and operation system image will be tolerable to side channel attack.

Table 1. Various security consideration of connect vehicle in ITS

Issue	Considerations
Authentication and reauthentication	EAP issues in intialization and handover phase
Challenges and evolution of security in ITS	Secuirty phase evolution in control, communication and signal processing area
Implementation necessity of security countermeasure in connected vehicle	Guideline to implement security scheme PKI, design architecture of security, safety, cost, induce interoperable solution, support emergence of vehicle and develop trust relationship between cooperative systems
Pre-distribution of certificate in VANET	To robust authentication and pseudonymous communication, necessity of certificate, which is always added to beacon frame with location data
Secure priority based inter-vehicle communication MAC protocol	Threats and risk factors such as message forgery and reply, impersonation, privacy, jamming and interference, security requirements, and security requirement which is included in authentication, integrity, non repudiation, messages freshness, anonymity and so on
Approaches for vehicle information security	In attacker interference, threats such as unauthorized use, unauthorized setting, information leakage, sniffing, DoS attack, tampered message, loss of logs, and unauthorized relay In security assessment and debugging, measures such as reviewing source code, applying a static analysis, evaluating the compliance, fuzzing, and conducting vulnerability assessment for region of cooperative intelligent transport system
Cyber risks for vehicle	ISO26262 is specified to risk analysis with exposure, controllability and severity about functions
Guideline of vehicle cyber security	IEC62443 (IEC – industrial system), NIST-800-61 (NIST – industrial system and pc/internet), Guide to industrial control system security (NIST – industrial system), CIP (NERC – pc/internet and industrial system), EVITA (EU - vehicle), vehicle information security guide (agency IPA - vehicle), and J3061(SAE - vehicle).
Modern vehicle security categorization examples	Power train(throttle valve data, CAN bus data message for the power control module, adaptive cruise control date, local interconnect network steering wheel data, ABS brake by wire data), vehicle safety(OBD II emissions data, TPMS data, firmware update over the air remote diagnostics data, airbag control unit data, GPS data) using NIST SP 800-60 and FIPS 199
Security aspects	Insufficient bus protection, weak authentication, misuse of protocols, poor protocol implementation, and leakage of information
Framework for security metrics	Protective security metrics that how could protective security be measured, and behavioural security metrics those have reliability, availability, safety, and confidentiality with/without latency
Security challenges in automotive architecture design	Issues of Ethernet/IP and On Board (OBD) security, security and external mobility services, and migration towards Ethernet/IP. OBD security is required to detect malware and consisted of malware detector, DB(whitelist/blacklist), activity monitor, reporter and manager
Security function based on V2X communication	Measured to preventive, protective, detecting, and reactive method in the automotive
Defending connected vehicles against malware	Attacks such as virus, worm, Trojan horse, spyware, ransomware, and rootkit
Collaborative mobility and approach main innovation	primary services (authentication, integrity and confidentiality), security and privacy – preserving categories (system security, communications security and location privacy protection), multimodal security solution, uses of result from singular communication modes, integrate different PKI solution, trust hierarchy for ITS, balanced processing effort
Various restrictions in future connected vehicle	modified or dysfunctional attack, man in the middle attack, side channel attack, spoofing, compromised privacy attack

Future view (short/mid/log term) of automotive cyber security technology	Countermeasure : Hardened OS + secure coding, and virtualization, boot/RAM/debug, F/W/intrusion detection/prevention system, and hardware security module, vehicle bus communication and tamper proof hardware
Cycle of five stages for automotive cyber security system	Requirements definition (specification of risk assessment), design and implementation (function and service), test and audit (fuzz, penetration, integrity test). Each component module is automotive cyber security strategy, security standard, derivation of guideline, organizational system change, integration of process (business/development), integration of technology, testing and evaluation validation of items such as exposure, critical factor, credential, breach attractiveness, side channel attack, integration, and attack vectors

Third unauthorized software modification which is applied to integrity function will be tolerable to side channel attack.

Fourth unauthorized identification of critical infrastructure resource in network will be tolerable to spoofing and privacy attack.

Fifth unauthorized software and hardware modification of chip device and diagnostic tool will be tolerable to side channel attack.

Sixth unauthorized reverse engineering for known diagnostic protocol will be tolerable to communication bus manipulation attack.

However issue of man in the middle attack is related to safety function with driving strategy and issue of side channel attack is related to proper control of vehicle and detect misbehavior in driving situation. Software modification and DoS attack are related to braking of acceleration and safety in driving situation. Issue of spoofing attack is related to scalability of service.

Also like the suggestion of Cornelius Bittersohl, it will be described future view (short/mid/log term) of automotive cyber security technology as follows: In short term, security scheme will be applied to hardened OS + secure coding and virtualization. In midterm, it will be applied to secure boot/RAM/debug, F/W/intrusion detection/prevention system and hardware security module. In long term, it will be applied to encrypted vehicle bus communication and tamper proof hardware.

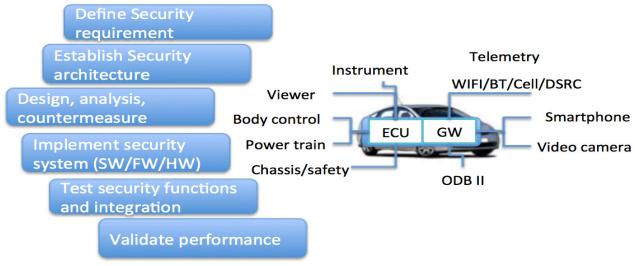

Figure 4. Cyber security procedure of risk assessment in connected vehicle of ITS.

Like the approach of Cornelius Bittersohl, for automotive cyber security ECO system, it will be fitted cycle of five stages such as requirements definition (specification of risk assessment), design and implementation (function and service), test and audit (fuzz, penetration and integrity test). Each component module is automotive cyber security strategy, security standard, derivation of guideline, organizational system change, integration of process (business/development), integration of technology, testing and evaluation validation of items such as exposure, critical factor, credential, breach attractiveness, side channel attack, integration, and attack vectors.

From issue of the related research of cooperative intelligent transport system and connected vehicle, we will be induced to various considerations and summarized as follows in Table1.

3. Conclusions

This paper is focused on security threats and consideration, cyber risk of connected vehicle. When it is taken security problem of In-vehicle network, there must be considered insufficient bus protection, weak authentication, misuse of protocols, poor protocol implementation and leakage of information. According to necessity of security metric for evaluation measure, the issue of security metrics in the security model will be required protective security metrics that how could protective security be measured and behavioral security metrics those have reliability, availability, safety and confidentiality with/without latency. Especially, when it is considered the architecture of In-vehicle network, it is needed to approach to issues of Ethernet/IP and On Board (OBD) security, security and external mobility services and migration towards Ethernet/IP. OBD security is required to detect malware and consisted of malware detector, DB (whitelist/blacklist), activity monitor, reporter and manager. Therefore it must be analyzed and considered

different security elements of the various consideration and access in each various connected vehicle.

4. Acknowledgment

This paper is supported from Department of Industry – Academia Cooperation of Baekseok University.

5. References

1. Varga N, Borkor L, Fishcer HJ. LDM based dynamic network discovery and selection for IPv6 mobility management optimization in C-ITS environments. Proceedings of MT-ITS; Hungary. 2015. p. 483–90.
2. Madakam S, Ramaswamy R. Sustainable smart city: Masdar (UAE) (A City: Ecologically Balanced). Indian Journal of Science and Technology. 2016 Feb; 9(6):1–8.
3. Sagar TSJ, Balamurugan MS, Vivek JA. A wireless framework for automotive monitoring systems. Indian Journal of Science and Technology. 2015 Aug; 8(19):1–9.
4. Rockl M, Robertson P. Data dissemination in cooperative ITS from an information centric perspective. Proceedings of IEEE ICC; South Africa. 2010. p. 1–6.
5. Jeong HJ, Kafle VP, Yoo H, Kim D. HIMALIS-C-ITS: Fast and secure mobility management scheme based on HIMALIS for cooperative ITS service in future networks. Proceedings of ICUFN; Vietnam. 2013. p. 60–5.
6. Wymeersch H, de Campos GR, Falcone P, Svensson L, Strom EG. Challenges for cooperative ITS: Improving road safety through the integreation of wireless communications. Control and Positioning. Proceedings of ICCNC; USA. 2015. p. 573–8.
7. Cincilla P, Kaiser A, Lonc B, Labiod H. Security of C-ITS messages: A practical solution. Proceedings of NTMS; France. 2015. p. 1–5.
8. Feiri M, Pielage R, Petit J, Zannone N, Kargl F. Predistribution of certificates for pseudonym broadcast authentication in VANET. Proceedings of VTC; UK. 2015. p. 1–5.
9. Suthaputchakun C, Ganz A. Secure priority based Inter-vehicle communication MAC protocol for highway safety messaging. Proceedings of IEEE ISWCS; Norway. 2007. p. 518–23.
10. IT Security Center. Approaches for vehicle information security: Information security for networked vehicles. Proceedings of IPA Information Technology Promotion Agency; Japan. 2013. p. 1–48.
11. Onishi H. Guidelines for vehicle cyber security. Proceedings of World Congress SAE; USA. 2014. p. 1–26.
12. NHTSA. National Institute of Standards and Technology Cybersecurity Risk Management Framework Applied to Modern Vehicles. October 2014. p. 1–27.
13. Kleberger P, Olovsson T, Jonsson E. Security aspects of the In-vehicle network in the connected car. Proceedings of IEEE IV; Germany. 2011. p. 528–33.
14. Jonsson E, Pirrzadeh L. A framework for security metrics based on operational system attributes. Proceedings of IWSMM; Canada. 2011. p. 58–61.
15. Sagstetter F, Lukasiewycz M, Steinhorst S. Security challenges in automotive hardware/software architecture design. Proceedings of DATE; France. 2013. p. 458–63.
16. Knapik P, Schoch E, Kargl F. Electronic decal: A security function based on V2X communication. Proceedings of VTC; Canada. 2014. p. 1–14.
17. Zhang T, Antunes H, Aggarwal S. Defending connected vehicles against malware: Challenges and a solution framework. IEEE Internet of Things Journal. 2014; 1(1):10–21.
18. Alesiani F. Towards collaborative mobility. Proceedings of ITS WC.; Japan. 2013. p. 1–22.
19. Bittersohl C. Automotive cyber security: Developing a thriving security ecosystem within automotive organizations. White Paper of Timothy G. Thoppil. P3 North America Inc; p. 1–22.