2018 IEEE International Conference on Vehicular Electronics and Safety (ICVES)
September 12-14, 2018, Madrid, Spain

A Survey: Engineering Challenges to Implement VANET Security

Hirofumi Onishi
Alpine Electronics Research of America, Inc.
Torrance (CA), USA
honishi@alpine-la.com

***Abstract*—VANET (Vehicle Ad-hoc Network, i.e., V2V (Vehicle-to-Vehicle) communication) with short communication latency and not needing an infrastructure could play important roles in future road safety, to implement crash warning applications. VANET could be useful for awareness of vehicles in drivers' blind spots in situations that cannot be detected by cameras or radars. However, VANET has additional security difficulties to detect and exclude vehicles that are malicious nodes from the network, besides wireless communication's inherent security vulnerabilities, such as jamming, eavesdropping, and tampering, because nodes are communicating with each other directly and not through a base station or a server. On the other hand, DLT (Distributed Ledger Technologies) typified by blockchain is planned to take important roles even in the auto industry, for example, to record/control the information of a huge number of components or maintenance/inspection histories. However, these technologies still have technical limitations to cover time sensitive safety-related applications provided by VANET. Hence, this report first introduces VANET and its security risks, then addresses blockchain's opportunities in the automotive industry. Finally, this report concludes by discussing technical challenges on blockchain to be applied for VANET, for example, the consensus process to create a new block and 51% issue.**

Keywords— VANET(Vehicle Ad-hoc Network); V2V(Vehicle-to-vehicle) communication; CA(Certification Authority); certificate; DLT(Distributed Ledger Technologies); Blockchain, consensus process;

I. BACKGROUND

The advancement of ICT (Information and Communication Technologies), for example, IoT (Internet of Thing), AI (Artificial Intelligence), Big Data and 5G (5th generation mobile communication) makes our daily lives safer, more convenient and sustainable. However, the recently exposed cyber-vulnerability on widely distributed microprocessors [1] reminded us that cyber-risks from wide connectivity, highly automated functions, and strong dependency on ICT are threatening our society. Responding to these risks, the government, Congress, and industry make various efforts to mitigate these risks [2, 3, 4]. However, sometimes, it is difficult for these activities to catch up with the progress of cyber-attack techniques because cyber-attacking techniques are continuously advanced by international tensions and cyber-attacks' commercialism [5].

As one of the critical infrastructures for our daily lives, modern computerized vehicles supported by ICT, with wider connectivity (to the external IT world [6], Fig. 1), more microprocessors, and extensive software code also have a higher risk to be targets of cyber-attacks than ever. Many researchers and white-hackers have already exposed their various vulnerabilities [7, 8, 9].

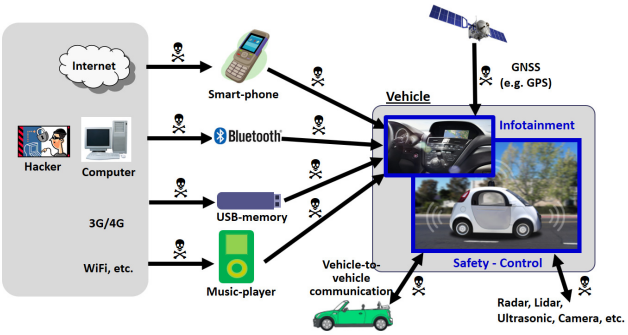

Fig. 1. Examples: Wide attack surfaces on modern vehicles [6]

II. VANET AND ITS SECURITY RISKS

A. VANET

VANET (Vehicle Ad-hoc Network, i.e., V2V (Vehicle-to-vehicle) communication) has two remarkable advantages, such as short communication latency (not through access points or servers) and not needing of an infrastructure.

VANET can leverage these two advantages to integrate crash warning applications where neighboring vehicles (i.e., nodes) are exchanging their location/speed/moving-direction directly each other with short communication latency. In these applications, when vehicles detect potential crashes within a predefined time (e.g., 9 seconds) based on exchanged information, vehicles warn drivers of potential crashes [10]. Besides crash warning applications, in the future, neighboring vehicles can exchange their future directions or intentions on VANET, for road safety.

978-1-5386-3543-8/18/$31.00 ©2018 IEEE

Finally, VANET can be extended to Vehicle-to-Pedestrian communication or Vehicle-to-(Motor-)Bike communication for more advanced safety and convenience.

B. *Cyber-risks on VANET*

Currently, crash warning applications with VANET are not designed to control vehicles directly, therefore, they would not threaten road-users immediately. However, many studies have listed various hackers' motivations to attack these applications [11 – 17].

a) Disable true warnings by blocking true messages.

b) Create false warnings by sending false messages, and degrade drivers' trust on these applications.

c) Create false warnings by sending false messages, and get unfair advantages for unscrupulous drivers.

d) Steal PII (Personally identifiable information), e.g., other drivers' driving histories, and abuse them.

First, hackers for pleasure may conduct "item a or b", though organized hackers seeking profits may not conduct "item a or b". Next, it may be more effective for unscrupulous drivers to manipulate false traffic signals timing or false road-congestion/accident/closure information than to do "item c".

Finally, the privacy information related to VANET, which includes possible times of drivers' absence from home or possible locations/times of drivers' visiting is to be abused for secondary crimes, therefore, individual or organized hackers are motivated to conduct "item d" for their financial or other purposes.

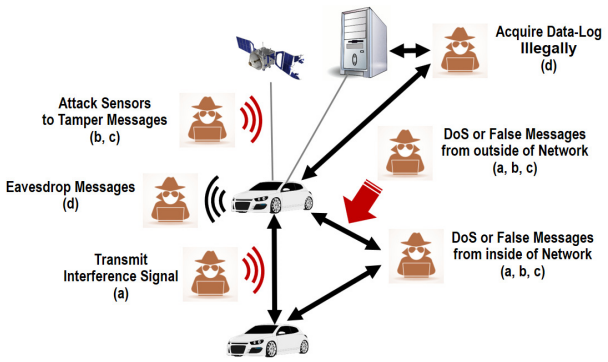

Fig. 2. Attack (surface) types on VANET

Fig. 2 describes attack (surface) types from hackers' motivations as mentioned above.

For "item a", the first attack type is radio interference to block true messages. The second type, DoS (Denial of Service), causes network congestion by flooding a huge number of false messages in order to block true messages ultimately.

There are two attack types to transmit false messages for "item b and c". The first type is to transmit false messages from the inside/outside of the network; then, the second type is to tamper with non-misbehaving vehicles' messages by manipulating sensors/devices that generate their messages. One example of this type attacks is to change vehicle locations/clocks maliciously by GPS spoofing [18].

To acquire privacy information (item d), the first attack type is to eavesdrop messages from the target vehicle locally. The second type is to acquire the driving history of the target vehicle stored on the vehicle or a server.

C. *Proposed security mechanism on VANET*

In this section, we introduce many mechanisms on the currently proposed VANET responding to cyber-risks as mentioned above.

a) Certificate from CA (Certification Authority):

To maintain the security on VANET, individual vehicles get a certificate from CA (Certification Authority), then a message sender sends a certificate prior to sending a message. On the other hand, a message receiver verifies the received certificate, then if the receiver can trust the certificate, it starts to process the messages from the trusted message senders [11, 16, 19, 20, 21, 22]. This mechanism provides the following benefits to maintain network security.

- Only certified vehicles (by CA) can transmit messages.
- Neighboring vehicles can easily identify if certified vehicles (by CA) transmitted the message.

b) Revocation list:

CA and vehicles monitor misbehaviors (e.g., suspicious certificates or messages) of neighboring vehicles. Detected misbehaviors are reported, and per necessity, reported vehicles' information is added on the CRL (Certification Revocation List); then the CRL is circulated to all vehicles in the network. Furthermore, the CRL is referenced, when the reported vehicle get a certificate [16, 19, 20, 21].

c) Privacy protection mechanism:

As mentioned above, privacy information on VANET, especially, driving history is seriously concerned, therefore, the following mechanisms have been proposed:

- Anonymity: Messages between neighboring vehicles should not include keys to identify drivers or vehicles.
- Non-traceability: Messages' IDs between neighboring nodes should be renewed at least a couple of times per day, because long logs can be used to identify owners/drivers or vehicles.
- Security/non-traceability: Message logs should be securely stored, and even once message logs stored on vehicles or servers were disclosed, these logs should not be abused.

Fig. 3 shows the mechanism to achieve the non-traceability of data log in CAs. Long-term CA manages permanent long-term certificates generated from PII (e.g., vehicle manufacturer/models/VIN-number/license-plate-number). On the other hand, short-term CA issues short-term certificates that are delivered to individual vehicles locally. In this mechanism, short-term certificates (that have clues for individual vehicles' locations/times) and long-term certificates (based on PII) cannot be linked, because long-term certificates are encrypted by one of long-term CA's asymmetric keys and cannot be

decrypted by the short-term CA which does not have long-term CA's keys [11, 16, 19, 20, 21].

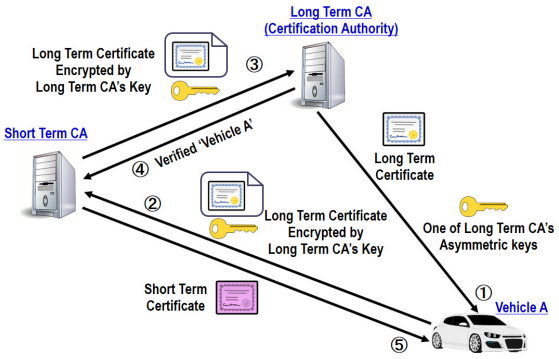

Fig. 3. Concept: Privacy protection on VANET

D. Challenges on VANET security

Next, we discuss challenges for the security mechanism as mentioned above.

a) Necessity of centralized communication:

Although not needing a communication infrastructure is the largest advantage of VANET, the abovementioned security mechanism on VANET requires the infrastructure for the centralized communication network where vehicles and CAs exchange security keys and the certificates. This is the largest challenge on the current VANET security mechanism.

b) Trade-off between safety and security:

On safety applications provided by VANET, especially for crash warning applications, excluding more nodes with minor security suspicion makes safety benefits less, therefore, we need to balance safety benefits (the original objective of these applications) and security resilience [23]. Moreover, an innocent node may be reported on a misbehavior report, by malicious or incorrect operations, therefore, the clear process rule to handle misbehavior reports should be defined.

c) Performance of encryption, decryption, and certification:

The draft of VANET (V2V communication) mandatory in the US proposes light vehicles to transmit messages at every 100 milliseconds [10]. Therefore, supposed 200 vehicles within the communication range (i.e., approximately 300 meters), an onboard device in a vehicle should decrypt 2000 messages and verify 2000 certificates, per second.

Additionally, the US has 263 million cars and trucks in 2015 [24] and each vehicle has to renew a certification minimum 2 times a day in order to avoid of being tracked maliciously, (though, some experts propose of the certificates' renewal at every 5 minutes [24]). Under this condition, CA has to issue 6000 certificates every second, though currently, the butterfly key expansion mechanism is expected to mitigate the consumption of calculation performance on CA and vehicle devices [20, 25].

d) Other challenges:

Unfortunately, all security mechanisms that include the abovementioned mechanism cannot mitigate physical attacks, such as wireless jamming, (though, jamming on the wireless spectrum allocated for VANET in both of the US and Europe, should be legally banned).

Furthermore, DOS (Denial of Services, i.e., flooding of malicious messages from malicious message senders) causes the network congestion to enlarge the latency of true messages. Additionally, DOS consumes calculation performance on receivers' devices of decrypting/certificating messages; ultimately enlarges the latency of true messages.

Other physical attacks against sensors or devices on vehicles may maliciously change messages on innocent vehicles. As one example, GPS spoofing with affordable kits [18] can easily tamper locations/clocks of innocent vehicles, and cause the miscalculation of crash timing by receiver vehicles, (though, GPS spoofing is also illegal).

As mentioned before, driving histories on VANET can be abused for secondary crimes, however, driving history can be disclosed by the combination with other methods, for example, video cameras installed in garages or tracking of drivers' mobile phones.

III. Blockchain and Its Potential

A. Blockchain

On the other hand, we, fortunately have emerging prospective security technologies mainly to be applied for financial applications; especially DLT (Distributed Ledger Technologies) utilized for blockchains can store/manage dynamic individual financial transactions on individual ledgers while preventing double spending or illegal transactions, without centralized authorities.

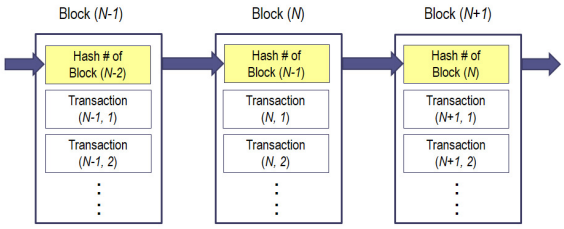

Fig. 4. Concept: Blockchain data structure

Blockchain indicates a data structure linked with multiple blocks that include the hash value of its previous blocks (with light-yellow color) and individual transaction records (Fig. 4); the linkage between consecutive blocks by hash values prevents manipulation of records [26, 27, 28].

Then, we introduce the process to create a new blockchain (includes a new additional block) by using the case of bitcoin [29], as one example [26, 27, 28] (Fig. 5):

- Individual members collect new transactions (after the previous blockchain's authorization).

- When one member successes to create a tentative new blockchain (includes a new additional block), he/she broadcasts it to all members.
- Members tentatively accept the latest blockchain broadcasted, but only if all transactions in it are valid and all necessary transactions are included in it.
- Members start to process additional transactions by using the newly authorized blockchain.

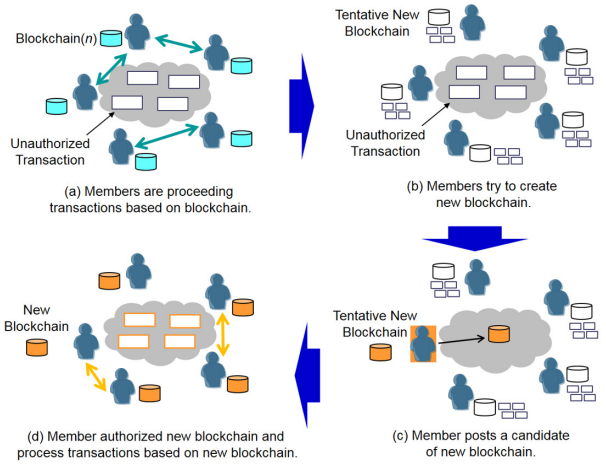

Fig. 5. Concept: blockchain's creation process (= Consensus process)

Note that, new blockchains, including new individual transactions, have been authorized by all members, not a centralized authority.

B. Blockchain's opportunities in auto industry

Blockchain can be applied to various automotive applications by utilizing its strong resistance against manipulation and lack of need of a central certification authority (nor a central data management center) [30 – 35].

a) Manufacturing and logistics:

Blockchain suits to record the information of a huge number of vehicle components, (approximately 30,000 components for ordinary vehicles [36]), such as dates/locations/persons-in-charge of shipping/inspection, and versions/lot-numbers. Blockchain; then it can record locations, materials, and machinery even for one nail.

Furthermore, it can also record vehicle locations and conditions from a factory to an end customer (vehicle owner), through a fleet company and a dealer.

b) Maintenance and inspections:

Next, blockchain can record the history of maintenance/inspections that include repairs/inspections responding to recalls. According to recent multiple industry affairs, it can also record procedure/location/person-in-charge regarding inspections prior to the vehicle shipments.

c) Ownership:

Blockchain can track the ownership of a vehicle from the first owner to the current owner through multiple owners, carefully controlling privacy issues, then it can also control the insurance related information (e.g., insurance coverages and conditions), as the extension of its ownership.

As an extension, it can also transfer the (temporary) owner permission with designating specific operations (e.g., opening doors/trunk, accessing the information of vehicle information terminals, or changing vehicle setting), in case of maintenance or valet parking.

c) Financial:

Of course, blockchain can leverage its primary natures for automotive related financial applications, such as payments for car-sharing/electric-charging [37]/parking/tolling/insurance/etc.

IV. Future VANET Security with Blockchain

In the future, VANET would expand to pedestrians or (motor-)cyclists where everyone is expected to join the network if he or she is following the community rule. (However, as we mentioned at 'Trade-off between safety and security' in the subsection D of section II, we first have to define the minimum rules and misbehavior.)

The nature of blockchain has a possibility to work in this future security mechanism (Fig. 6 (b)) where each vehicle can recognize malicious/innocent neighboring vehicles by its own distributed ledgers that include vehicles on the revocation list and/or individual vehicles' misbehaviors; then, these ledgers on individual vehicles could be authorized with the community members' consensus, without a central authority. However, at this moment, it is difficult to apply this type of technologies to VANET because of the following reasons:

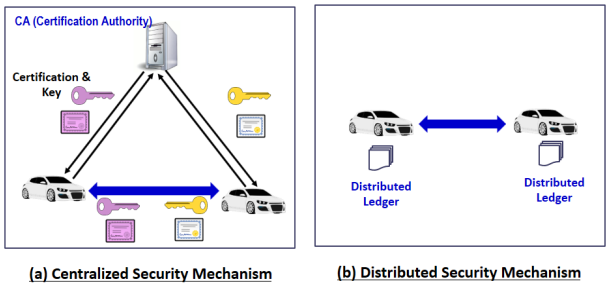

Fig. 6. Centralized and distributed security mechanism

A. Communication network

Even if we can integrate the VANET security without central authorities, by utilizing a distributed security mechanism, we still need an infrastructure for the centralized communication to synchronize individual ledgers stored in individual vehicles. As the result, VANET loses its largest advantage, i.e., not needing of a network infrastructure.

Furthermore, frequent network topology changes caused by vehicles' mobility makes the distributed security mechanism difficult to be applied on VANET. In Fig. 7, vehicle (1) leaves from the communication range of vehicle (A), on the other hand, vehicle (2) enters into the same communication range, therefore, it is difficult to synchronize distributed ledgers of

individual vehicles without a centralized network which covers all vehicles in the area.

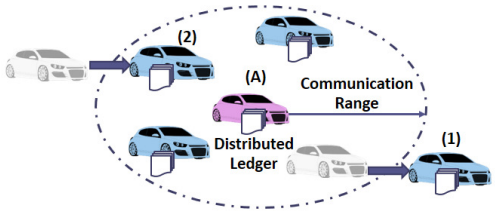

Fig. 7. Frequent network topology change on VANET

B. *Consensus process (to create new blockchain)*

In blockchain, individual participants ordinarily create new blockchains to acquire virtual currencies as a reward [26, 27, 28]. Therefore, we have to propose a new (reward) mechanism for VANET where individual vehicles desire to create new blockchains by consuming the limited calculation performance of onboard microprocessors.

Additionally, we have to investigate carefully if the time duration/delay of ledgers' synchronization is sufficient for time sensitive safety applications provided by VANET, instead of financial applications.

C. *51% issue*

Finally, we note that distributed ledgers (i.e., blockchains) are securely updated only within the condition that almost of nodes (vehicles) are not malicious [38]. When all vehicles have uniform impacts (e.g., calculation power) on the consensus process (to create a new blockchain), it is proved that we need at least 51% of innocent vehicles for the secure consensus process. However, in some consensus processes where individual vehicles' calculation performance or status of their account impact on the consensus processes, we need to be careful about the malicious manipulation on the consensus process.

Once a large number of vehicles come to be malicious intentionally or unintentionally, distributed ledgers (i.e., blockchains) can be updated maliciously for hackers' purposes.

D. *Privacy protection*

As mentioned above, privacy on VANET, especially driving histories are subject to be abused for secondary crimes, therefore, we need an appropriate privacy protection mechanism such that the current proposed mechanism implements with long-term and short-term certificates.

V. Conclusion

VANET (Vehicle Ad-hoc Network), such as V2V (Vehicle-to-Vehicle) communication is expected to take important roles in future road transportation, for example, to integrate vehicle crash warning applications, because of its short communication latency and not needing of a network infrastructure. However, VANET without passing through base stations or servers has additional difficulties to detect and exclude malicious vehicles (= nodes), besides wireless communication's inherent security vulnerabilities.

Security mechanisms for VANET currently proposed by the industry that utilize certificates from CA (Certification Authorities) will maintain VANET security, such as to maintain network security by detecting/excluding vehicles with security suspicions. Furthermore, the proposed security mechanism can protect the privacy information on VANET, such as driving logs.

However, the proposed security mechanisms have the following engineering challenges, as other ordinary security mechanisms have:

+ Trade-off between safety and security:
  In some case, even malicious vehicles should be included in the network, for safety applications, e.g., crash avoidance.
+ Calculation performance of encryption, decryption, and certification:
+ Physical-type attacks:
  - Wireless jamming.
  - Flooding of (malicious) messages.
  - Tampering messages on innocent vehicles, for example, by using GPS spoofing kits.
+ Privacy infringement with the combination of other methods: e.g., video cameras or tracking of mobile phones.

The largest technical challenge is that the currently proposed security mechanism requires the communication infrastructure to make CAs and individual vehicles exchange certificates/security-keys. In so doing, VANET would lose its largest advantage, i.e., not needing a network infrastructure.

On the other hand, DLT (Distributed Ledger Technologies) typified by blockchain which has been initially developed for financial applications are expected to be applied to various automotive applications, such as to record manufacturing/logistics and repair/maintenance, to record/manage ownership, and to handle automotive-related financial transactions, leveraging its strong resistance against manipulation and not needing of CAs.

However, DLT still has the following technical limitations to be applied for the VANET security:

- Necessity of network infrastructure to synchronize individual ledgers in individual vehicles, even if we can remove CAs.
- Appropriate consensus process (to create a new blockchain) with sufficient duration/latency for safety applications provided by VANET.
- Sufficient number of innocent vehicles for VANET security (to protect the consensus process against the malicious manipulation).
- Mechanism to protect privacy, especially driving-logs to be abused for secondary crimes.

While VANET security is a critical research topic, emerging security algorithms/mechanisms for other industries' applications, especially in the financial industry, have

possibilities to enhance VANET security. Therefore, we will continue to perform research in this domain and monitor the progress of these emerging technologies, because DLT typified by blockchain at the initial phase will see significant progress in the near future.

ACKNOWLEDGMENT

The authors express their sincerest gratitude to Mr. Richard Bishop of Bishop Consulting for his advice and review of this research report.

REFERENCES

[1] (), "Meltdown and Spectre." at meltdownattack.com (accessed in Jun. 2018).

[2] Senate, "Internet of Things (IoT) Cybersecurity Improvement Act of 2017," (S. 1691) (2017 - 18) in 115th Congress. at www.congress.gov/bill/115th-congress/senate-bill/1691.

[3] White House, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," (May 2018). at www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[4] NIST, "Framework for Improving Critical Infrastructure Cybersecurity Ver. 1.1," (Apr. 2018). at nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[5] Armor, "The Black Market Report," (Mar. 2018). at cdn.armor.com/app/uploads/2018/03/27222933/2018-Q1-Reports-BlackMarket-DIGITAL-min.pdf.

[6] H. Onishi, "Cybersecurity Updates of vehicle cyber-security in the US," (Nov. 2011), IEICE (Japan) Technical Report, IN2016-62, pp13 – 18.

[7] FCA, "Statement: Software Update:," (Jul. 2015). at media.fcanorthamerica.com/newsrelease.do?id=16849.

[8] A. Greenberg (WIRED), "This gadget hacks GM cars to locate, unlock, and start them (Updated)," (Jul. 2015). at www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/.

[9] (Reuters), "Tesla Fixes Security Bugs After Claims of Model S 'White Hat' Hack (Sep. 16)." at fortune.com/2016/09/20/tesla-security-bug-hack/.

[10] US DOT, "Federal Motor Vehicle Safety Standards; V2V Communications," (NPRM: NHTSA-2016-0126), (Dec. 2016). at www.federalregister.gov/documents/2017/01/12/2016-31059/federalmotor-vehicle-safety-standards-v2v-communications.

[11] K. Oka (ETAS), "Security Technique to ensure V2V and V2I Security," (Sep. 2015), (Japanese). at monoist.atmarkit.co.jp/mn/articles/1509/16/news009.html.

[12] P. Khani, M. Sharbaf, "Investigation of Vehicular Networks and its Main Security Issues," (2014-01-336), in SAE World Congress (Apr. 2014, Detroit, MI).

[13] NHTSA (US DOT), "Vehicle Safety Communications – Applications Final Report: Appendix Volume 3 Security," (DOT HS 811 492D), (Sep. 2011).

[14] S. Capato, L. Coconea, et al. "C-ITS security insights: a practical example of TVRA analysis," (TP0978) in European ITS Congress (Jun. 2017, Strasbourg, FR).

[15] A. Boudguiga, A. Kaiser, P. Cincilla, "Cooperative-ITS Architecture and Security Challenges: a Survey," (paper 2629) in ITS World Congress (Oct. 2015, Bordeaux, FR).

[16] P. Papadimitratos, L. Buttyan, et al. "Secure vehicular communication systems: design and architecture," pp 100 – 108, IEEE Communication Magazine (Nov. 2008).

[17] M. Amoozadeh, A. Raghuramu, et al. "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," pp 126 – 132, IEEE Communication Magazine (Jun. 2015).

[18] H. Lin, Y. Qing, "GPS SPOOFING," in DEFCON (Aug. 2015, Las Vegas, NV). at www.yumpu.com/en/document/view/53448437/gps-spoofing.

[19] L. Delgrossi, T. Zhang, "Vehicle Safety Communications," (ISBN 978-1-118-13272-2) Wiley.

[20] W. Whyte, A. Weimerskirch, et al. "A Security Credential Management System for V2V Communications," (978-1-4799-2687 -9/13), in IEEE Vehicular Networking Conference (2013).

[21] W. Whyte, "A Security Credential Management System (SCMS) for Vehicle-to-Vehicle Communications," (presentation), in ITS World Congress (Oct. 2015, Bordeaux, FR).

[22] V. Mahieu, G. Baldini, "Harmonization Task Group 6 Cooperative -ITS Security Policy," in ITS World Congress (Oct. 2015, Bordeaux, FR).

[23] H. Onishi, et al. "Approaches for Vehicle Cyber-Security in the US," (20174086), International Journal of Automotive Engineering 8 (2017) 1-6. at www.jstage.jst.go.jp/article/jsaeijae/8/1/8_20174086/_pdf.

[24] Bureau of Transportation Statistics (US DOT), "National Transportation Statistics 2017." at www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/index.html.

[25] W. Whyte, A. Weimerskirch, et al. "A Security Credential Management System for V2V Communications," in IEEE VNC 2013 (Dec. 2013, Boston, MA). at realworldcrypto.files.wordpress.com/2014/01/whyte.pdf.

[26] S. Nakamoto, A Peer-to-Peer Electronic Cash System, (Oct. 2008). at bitcoin.org/bitcoin.pdf.

[27] S. Fujimura, et al, Introduction of blockchain technologies (ISBN978-4-627-87171-7), (2017), (Japanese), Morikita Publisher.

[28] S. Sato, K. Hasegawa, et al. Textbook for blockchain, (ISBN978-4-86354-243-3), (2018), (Japanese), C&R.

[29] Bitcoin, Bitcoin is an innovative payment network and a new kind of money. at bitcoin.org/en/, (Accessed in Jun. 2018).

[30] L. Novosilska (Ignite), 10 Applications for Blockchain in Connected Car Automotive .at igniteoutsourcing.com/publications/blockchain-automotive-industry/, (accessed in Jun. 2018).

[31] (The Startup), Blockchain In Automotive .at medium.com/swlh/blockchain-in-automotive-dea04e51a079. (accessed in Jun. 2018).

[32] K. Houser (Future Society), Cars on the Blockchain? Six Ways Automakers Could Employ the New Technology, (Mar. 2018). at futurism.com/cars-blockchain-six-ways/.

[33] L. Godzik (Ginkgo), Blockchain - Technologies for the Automotive Industry, (2017). at www.ginkgo.com/wp-content/uploads/2017/06/WP_Blockchain-online.pdf.

[34] H. Kitayama, T. Fukuda, Business Service and Technology for Cars using Blockchain, (Apr. 2018) Journal of Society of Automotive Engineers of Japan Volume: 72 2018.5, Pages: 30 – 34.

[35] A. Dorri, M. Steger, S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, Volume: 55, Issue: 12, Pages: 119 – 125 (2017).

[36] (Toyota), "How many components does a vehicle have?" (Japanese) .at www.toyota.co.jp/jp/kids/faq/d/01/04/, (Accessed in Jun. 2018).

[37] N. Shimizu (Nikkei), "Implement Blockchain Lightning Network for EV Charging", (Jun. 2018) Nikkei Automotive 2018.6, Pages: 36 – 37.

[38] (Bitsonline), New Website Highlights Cryptocurrencies at Risk of 51 Percent Attack (May 2018). at bitsonline.com/51crypto-51-percent-attack/.

GENERAL REFERENCES

M. Wolf, "Security Engineering for Vehicular IT Systems," (ISBN 978-3-8348-0795-3), Vieweg+ Teubner.

Nikkei BP publisher, "Cryptography and Authentication," (ISBN 4-8222-1269-6), (Japanese), Nikkei BP publisher.