Securing Tire Pressure Monitoring System

Kevin Daimi
Computer Science and Software Engineering
University of Detroit Mercy
Detroit, USA
email: daimikj@udmercy.edu

Mustafa Saed
HATCI Electronic Systems Development
Hyundai-Kia America Technical Center
Superior Township, USA
email: msaed@hatci.com

***Abstract*—Potential security attacks on vehicular networks have been ceaselessly growing. All the known wireless security attacks in addition to vehicle network specific attacks can possibly be experienced. They can target the privacy of the driver and the integrity and confidentiality of messages sent and received within the vehicle and those messages travelling outside the vehicle. One of those possible attacks can be directed at the Tire Pressure Monitoring System (TPMS) sensor. The message broadcasted by the sensor is intended for the TPMS Electronic Control Unit (TPMS ECU). This message cannot be encrypted and authenticated due to the lack of processing capabilities at the sensor side, and therefore, it could be attacked. If the attack is successful, the ID of the sensor, which is unique and transmitted in all broadcasted messages, will be invested to track vehicles, and thus, violating drivers' privacy. Furthermore, the attacker can replace the original message with a malicious one that could possibly adversely impact other Electronic Control Units. This paper attempts to secure the TPMS by suggesting the inclusion of smart sensors to replace the current sensors. Since these smart sensors possess computing power, encryption and authentication will be made possible. The original ID is replaced with an anonymous one, and the whole message including the IDs are encrypted. An unsophisticated encryption approach is used. Both the key and the anonymous ID are replaced with fresh ones after each message is received.**

Keywords—TPMS Security; Cryptography; Smart Sensors; Vehicle Security; Security Protocol; Authentication

I. INTRODUCTION

With the constantly expanding vehicular wireless network, connected vehicles, and the increasing number of vehicle Electronic Control Units (ECUs), securing vehicle assets is turning out to be more problematic. With the increasing volume of interconnections between and within vehicles, the attack rate of internal vehicle networks is rising abruptly [1]. The vehicular ad-hoc networks are decentralized dynamic networks that demand effective and secure communication requirements as a result of the vehicles being constantly in motion. Such networks are more prone to various attacks, such as Worm Hole attacks, denial of service attacks, and Black Hole Attacks [2]. To sustain the enhancements in safe vehicle technologies, it is critical to create a robust vehicle network security system, which identifies security vulnerabilities, threats, and attacks facing vehicle network [3]. Security is indispensable to the vehicle-to-anything (V2X) technology, and privacy is an intact component of V2X security that can be safeguarded with privacy preserving/anonymous authentication [4]. A key development in the automotive industry is the need to adapt proven functional safety processes and techniques for security engineering to allow vehicles to be resilient against cyber-attacks [5]. Security issues in automotive systems are obfuscated by the demand for real-time mitigation against in-field threats, and the in-field configurability and extensibility of security aspects [6]. In connected vehicles, there are different types of attacks that can target the entities vehicle, infrastructure, cloud, and mobile phone individually and the communication between them [7]. Communications of connected vehicles are subject to various security issues and result in immense concerns with respect to privacy and data confidentiality [8].

Modern vehicles utilize several busses in their networks. Among these are the Local Interconnect Network (LIN), Controller Area Network (CAN), Media-Oriented System Transport (MOST), and FlexRay buses. Connected to these buses are various ECUs. These are embedded systems controlling one or more of the vehicle's functions. They play a central role in controlling many functions in vehicles [9] – [15]. Those ECUs are vulnerable to security attacks that could be fatal and can result in casualties. Hence, there is a critical need to protect the ECUs infrastructure [16]. By equipping vehicles with cutting-edge sensors and actuators, and the growing number of formidable network of ECUs, complexity and probability of defects and security vulnerabilities increase [17]. CAN is the dominating bus in the automotive realm due to its simplicity, low cost, and robustness [18]. There is some belief that the CAN bus, to which many ECUs are attached, can be hardly compromised. Pan et al [19] discussed viable scenarios where a vehicle is no longer safe after its CAN bus is compromised by analyzing potential attacks on CAN and their effect on the safety of the vehicle driver and passengers.

One of the ECUs, the Tire Pressure Monitoring System ECU (TPMS ECU) can be attacked as a result of compromising the measurement (Pressure/temperature) broadcasted by the TPMS sensor. The attack can spread over to other ECUs as ECUs share buses. The sensor used in this system is not a smart sensor. It is capable of sending messages (measurements) but not receiving messages. They also lack computing power and storage. A smart sensor is composed of a sensing part with processing resources provided by a microprocessor. In other words, smart sensors are principal sensing parts with embedded intelligence that can provide important data to the receiver with amplified reliability and integrity [20]. Smart sensors should incorporate the following features; self-identification, self-diagnosis, time and location aware, higher order functions, and conforming to communications and protocols standards [21]. A smart sensor may include a microprocessor, a flash memory of 16 KB (8 KB for firmware, and 8 KB for other uses), a 512 B RAM, and 64 parameter registers, and 8 MHz clock [22].

The rationale for having Tire Pressure Monitoring System (TPMS) in vehicles is to warn drivers that one or more tires are substantially under-inflated, possibly creating unsafe driving conditions. The TPMS sensor will forward the tire pressure value and possibly other values, such as temperature, to the TPMS ECU. The TPMS ECU causes the low tire pressure indicator (a yellow symbol) to illuminate on the dashboard instrument panel [23]. The TPMS allows drivers to promptly realize the current status of each tire's pressure. It is made up of TPMS sensors and a TPMS monitoring device (TPMS ECU). TPMS sensors measure the pressure and the temperature of tires and transmit them to the TPMS ECU [24]. The TPMS ECU analyzes the tire information received from the TPMS sensors and reveal the tire pressure status to the driver [25].

Messages broadcasted by the TPMS sensors can be attacked. Since the message includes the unique ID of the sensor, the vehicle could be tracked, and the privacy of the driver compromised [26]. The captured message could be modified by the attacker and then broadcasted. This could impact other ECUs connected to the Control Area Network (CAN) bus [27]. Roufa et al [28] presented a privacy and security evaluation approach of wireless Tire Pressure Monitoring Systems based on laboratory experiments with separated tire pressure sensor modules and other experiments using a complete vehicle system. They concluded that eavesdropping is certainly possible at a distance of approximately 40 meters from a moving vehicle. It was further concluded that reverse-engineering of the original protocols exposed the static 32-bit identifiers and the messages to be easily tracked remotely. This fact, together with the absence of authentication and validation of the messages, will raise concerns about privacy of drivers by tracking their vehicles and allow remote spoofing of sensor messages.

Kilcoyne, Bendelac, Ernst, and Michaels [29] analyzed the cybersecurity of the TPMS wireless communications interface and proposed adopting a more secure TPMS protocol that employs a simple linear feedback shift register (LFSR) based message encryption. They used an interesting experiment that involved a TPMS and various equipment apparently in a lab setting. They encrypted the sensor ID with LFSR but left the pressure and temperature untouched. Knowing that that current TPMS sensors are one-way sensors (they send but cannot receive), and with the lack of any processing power, it is not clear how the message sent by sensor can be encrypted while the TPMS is in the tire. Furthermore, leaving the readings of pressure and temperature as plain messages will make them prone to attacks. In other words, the approach works fine in a lab setting, but it cannot be implement in reality.

This paper suggests the deployment of smart sensors instead of the current sensors and introduces a security protocol that encrypts a message by a key simultaneously created by the smart sensor and the TPMS ECU. To protect the privacy of vehicle location, an anonymous ID for the sensor is used. The remaining of the paper is organized as follows: Section II briefly explains smart sensors. The TPMS security architecture is introduced in Section III. The proposed TPMS security approach is presented in Section IV, and the security analysis is performed in Section V. Finally, the paper is concluded in Section VI.

II. SMART SENSOR SYSTEM MODULES

The smart sensor modules are briefly explained in this Section. These modules are depicted in Figure 1 below. The system has a sensor for pressure and another sensor for temperature of the tire in question. It can also contain further sensors, such as motion sensor, acceleration sensor, and load detection sensor. The module, Other Sensors, refers to these sensors. Because all the measurements detected by the sensors are analog, an Analog-to-Digital Convertor is essential. The heart of the smart sensor system is the microcontroller. It is comprised of a microprocessor, a flash memory for firmware and possibly other uses, a RAM, a register, and a clock. Communications with the TPMS ECU is accomplished through the Communication Media of the smart sensor. The Microcontroller module will play a key role in securing the communication between the smart sensor and the TPMS ECU.

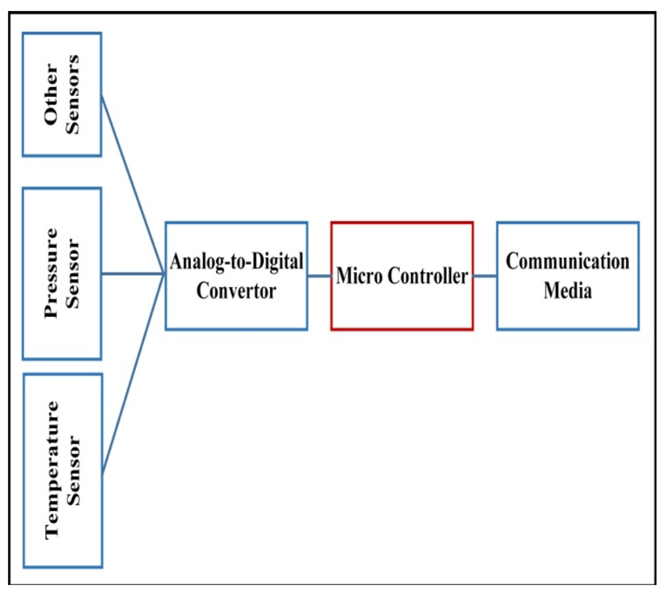

Figure 1. Smart sensor modules

III. TPMS Security Architecture

The current sensors of the TPMS are one-way (one-directional) devices. They can only transfer the readings to the TPMS ECU but cannot receive. They do not have any processing power. Therefore, the measurements forwarded to TPMS cannot be encrypted. This paper suggests replacing the currently installed sensors with smart sensors.

Each tire will be equipped with a smart sensor. All the smart sensors are connected to the TPMS ECU as with the current situation. The sensors can now send and receive data. Furthermore, their microcontroller will furnish them with the needed computing capabilities to implement the needed security functions to safeguard the broadcasted readings/measurements. The TPMS security architecture in Figure 2 reveals the following common subset of ECUs; Telematics Control Unit (TCU), Audio Control Module (ACM), Engine Control Module (ECM), Powertrain Control Module (PCM), and Body Control Module (BCM). Because different vehicle manufacturers use different ECUs, we labeled the rest as ECU1, ECU2, etc. The presented ECUs are selected to show that attacking the TPMS ECU through the non-smart tire sensors (current sensor) can impact other ECUs causing further problems and possibly casualties.

The TPMS security architecture will only try to ensure that ECUs attacks through the broadcasted messages (measurements) are prevented. Securing the ECUs against other attacks is beyond the scope of this paper. A security approach to protect the ECUs is presented in [9].

The smart sensors and the TPMS ECU agree on using Pseudo-IDs instead of the real IDs to protect privacy, cryptographic algorithms, techniques for creating and changing the key, and the order of the transferred messages. They further agree on nonce calculation to ensure the currency of the exchanged messages.

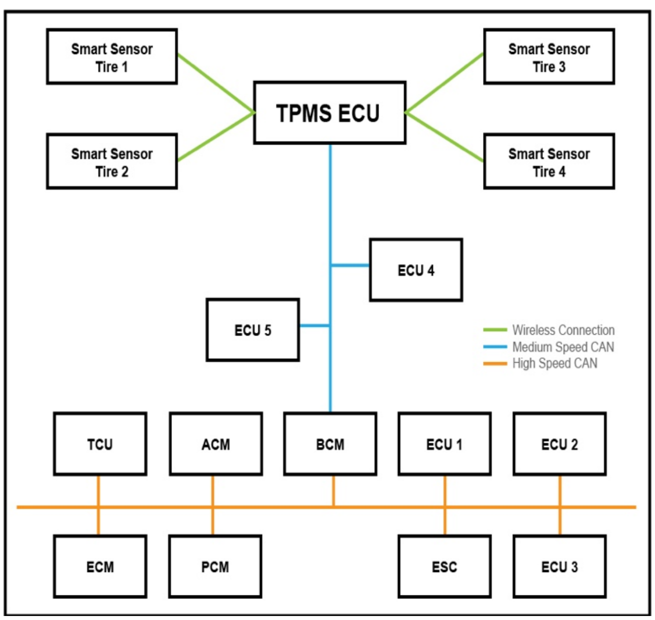

Figure 2. TPMS security architecture

IV. Proposed TPMS Security Approach

The proposed TPMS security approach is broken up into seven components. The purpose of this subdivision is to facilitate the comprehension of the suggested approach. The notations used in this approach are depicted in Table 1 below. In this security approach, a session is concluded when the messages in the security protocol below (Section F) are processed. Once the two messages are received, a new session starts.

A. Initialization

At manufacturing time, all the sensors should have their IDs (ID_1 – ID_4), 64-bit secret key, 64-bit secret value, nonce, and the ID of the TPMS ECU (ID_{TMPS}) preinstalled. The TPMS ECU will have ID_1 – ID_4, secret (symmetric) key, nonce, and secret value in addition to its ID_{TMPS} preinstalled. In addition, the MAC key, KM, is also taken care of for both the TPMS and the smart sensors at manufacturing time. For every session, the IDs will be replaced with anonymous IDs to maintain location privacy. The secret key, secret value, and the MAC key will also be replaced with freshly calculated values.

B. Secret Value Computation

The secret value, S, is deployed to further confuse the attacker. It is recalculated after each message as follows:

1. Expand A-ID to 64 bits to get S_1
2. Complement the bits of S_1
3. $S_2 = S_1 \oplus K$
4. Shift left the bits of S_2 16-bit position to get S_3
5. $S = S_3 \oplus$ A-ID

C. Counter

A 1-bit counter, *CTR-1* will be employed to control generating various values. It is initially set to zero. If it is 0, the tire pressure is used for generating the new symmetric key, secret value, MAC key, nonce, and anonymous ID. The counter is then incremented. If it is 1, the tire temperature is used instead, and the counter is incremented.

D. Keys and Anonymous IDs Generation

The subscripts n, p, and c indicate that new, previous, and current values will be used. The goal is to generate the new symmetric key (K), Mac key (KM), anonymous ID (A-ID), and nonce (N). Both the smart sensors and the TPMS ECU will perform these calculations after the measurements are sent by the sensors and received by TPMS ECU. In what follows, P/T indicates using either P or T depending on the value of CTR-1, and the addition is carried out with modulus 64.

$$K_n = (K_p \oplus K_c) + P/T$$

$$KM_n = (KM_p \oplus KM_c) + P/T$$

$$A\text{-}ID_n = (A\text{-}ID_p \oplus A\text{-}ID_c) + P/T$$

$$N_n = (N_p \oplus N_c) + P/T$$

Once the first message exchange is executed, both parties (sensors and TPMS ECU) have only one value for the variables above. In other words, they only have the current values K_c, KM_c, A-ID_c, N_c. Accordingly, the calculations above are modified as follows:

$$K_n = K_c \oplus P$$

$$KM_n = KM_c \oplus P$$

$$A\text{-}ID_n = A\text{-}ID_c \oplus P$$

$$N_n = N_c \oplus P$$

For all these calculations, A-IDs, P, T, and N need to be expanded to 64 bits. An A-ID is expanded by complementing its bits and inserting them as the leftmost 32 bits. For P, T, and N, the expansion is achieved by repeating their value (8-bit) three times to generate 32 bits, complementing them and inserting the complement as the leftmost 32 bits. Once the new values are obtained, only the right most 8 bits for N, P, and T will be used, and the right most 32 bits for A-ID will be valid.

E. Cryptographic Algorithm

Before stating the algorithm, it is essential to describe the contents of messages containing the measurements of tire pressure and temperature. This paper will rely on 64-bit messages. Larger messages can be used provided the registers' size at the smart sensors allows that. Vehicles manufacturers assign 32 bits for tire ID. Therefore, the bit distribution will be as follows:

ID	Nonce	Temperature	Pressure	MAC
32 bits	8 bits	8 bits	8 bits	8 bits

The encryption part of the proposed cryptographic algorithms XORs the message M with the key K, adds the ID of TPMS ECU to the result (modulus 64), and then XORs it with the ID of the smart sensor. This is represented symbolically as;

1. $X = M \oplus K$
2. $Y = X + A\text{-}ID_{TPMS}$
3. $C = Y \oplus A\text{-}ID_i$, i = 1 to 4

Note that C is the cipher text, and X, Y are just used to simplify the calculations.

The decryption part is the reverse of the above encryption because it is a symmetric algorithm. It is depicted below:

1. $Y = C \oplus A\text{-}ID_i$, i = 1 to 4
2. $X = Y - A\text{-}ID_{TPMS}$
3. $M = X \oplus K$

F. Security Protocol

Each smart sensor will concatenate the pressure, P, the temperature, T, and the rightmost 48 bits of the secret value, S. It then finds the MAC for them. Having done that, the ID, P, T, MAC, and N are concatenated, encrypted with the symmetric key, K, and forwarded to the TPMS ECU.

$$X = P \,\|\, T \,\|\, S$$
$$SS_i \rightarrow TPMS: E\,[K, A\text{-}ID_i \,\|\, P \,\|\, T \,\|\, N \,\|\, MAC\,(KM, X)]$$

Note that during the first message exchange, ID_i is used instead of A-ID_i. Upon receiving this message, the TPMS ECU decrypts it with K, ensures the message is current and not a replay by comparing it to its nonce, verifies the ID (A-ID_i) of the smart sensor, obtains the MAC of P || T || S and compares it to the MAC of the message. If they are equal, it retrieves the values of P and T and act accordingly.

Prior to every subsequent session, the new A-IDs are generated and exchanged. Before the encryption is applied, N || A-ID_i || MAC (A-ID_i), and N || A-ID_{TPMS} || MAC (A-ID_{TPMS}), are expanded to 64 bits by inserting 16 zeros on the right. The anonymous ID exchange is as follows:

$$SS_i \rightarrow TPMS: E\,[K, N \,\|\, A\text{-}ID_i \,\|\, MAC\,(KM, A\text{-}ID_i)]$$

$$TPMS \rightarrow SS_i: E\,[K, N \,\|\, A\text{-}ID_{TPMS} \,\|\, MAC\,(KM, A\text{-}ID_{TPMS})]$$

Both parties will decrypt the received message, make sure the message is not a replay by comparing it to their nonce, ensure the message is authentic by calculating the MAC of the ID and comparing it to the MAC in the message, and save the received IDs. All other values including the symmetric key, MAC key, nonce, and secret value need not be exchanged because they are calculated simultaneously by both parties.

G. Replacing TPMS Smart Sensor/ECU

It is possible that either the smart sensor or the TPMS ECU may malfunction and the dealership decides to replace them. In this case, the keys will not be symmetric, IDs are new and unknown to other parties, nonce cannot be verified, and secret values will not be the same. The suggested approach to deal with such a scenario is explained below.

If a TPMS smart sensor is replaced, the ID of the sensor is fed to the TPMS ECU either manually or automatically. The values ID_{TPMS}, K, KM, and N are copied from the TPMS to the new sensor. When communicating with this smart sensor, the approach of Section *D* for calculating the new K, KM, A-ID, and N when only the first message is exchanged is followed until current and previous values are available. This methodology also applies when replacing a tire with a spare tire if the TPMS does have the details of the spare tire.

When the TPMS malfunctions, the ID of the TPMS is entered into all the sensors either manually or automatically. The ID, symmetric key, MAC key, and nonce of each of the smart sensors is fed into the TPMS ECU. At this point, the communication will be treated as a fresh one for all parties.

It could be argued that those values are known by the technician at the dealership, and therefore they can be used for attacking the TPMS ECU and compromising other ECUs. This can never occur since these values will continue to change right after the vehicle is driven.

TABLE 1. NOTATIONS USED

Symbol	Meaning
P	Pressure
T	Temperature
K	Symmetric/Secret key
KM	MAC key
MAC	Message Authentication Code
S	Secret value
$ID_1 – ID_4$	ID of smart meters 1-4
SS_i	Smart sensor i, i= 1-4
ID_{TPMS}	ID of TPMS ECU
$A\text{-}ID_{TPMS}$	Anonymous ID of TPMS ECU
$A\text{-}ID_1$	Anonymous ID of ID_1
$A\text{-}ID_2$	Anonymous ID of ID_2
$A\text{-}ID_3$	Anonymous ID of ID_3
$A\text{-}ID_4$	Anonymous ID of ID_4
N	Nonce
E	Encryption
$\oplus$	Exclusive OR
$\|\|$	Concatenation
$\rightarrow$	Send to
C	Cipher text

V. SECURITY ANALYSIS

In the above protocol, only authenticated messages will be accepted. Authentication is achieved by appending the MAC of the messages; MAC (KM, (P || T || S), MAC (KM, $A\text{-}ID_i$), and MAC (KM, $A\text{-}ID_{TPMS}$) to their respective messages, calculating the MACs upon receiving the message and comparing the results. Furthermore, the confidentiality of messages is assured by encrypting the message and the MAC with the symmetric key, K. Only the party that holds K can decrypt the message.

The ID of the smart sensors and the TPMS ECU are replaced with anonymous IDs; $A\text{-}ID_i$ and $A\text{-}ID_{TPMS}$ respectively. This ensures the privacy of the vehicle location is preserved. Furthermore, the anonymous IDs are changed with every session to allow additional security with regards to the vehicle location.

The security approach above adopts the one-time pad. This is demonstrated by continuously replacing the key after each session. Each new message will retain a new key. This scheme is unbreakable.

The security value, S, is adopted to baffle the attacker by granting added security. S is also modified with every session to even further obscure the attacker.

Finally, a dynamic nonce, N, is implemented to verify the currency of the received message. The received N is compared to the N of the receiver to ensure currency. This nonce is vigorously updated using the algorithm above.

VI. CONCLUSION

Current vehicles encompass high data connectivity. There are various communication routes that have access to critical functionality of the vehicle. This obviously demands protecting vehicle infrastructure and functionalities through enforcing efficient methods, techniques, and processes to secure vehicle network. In an effort to contribute to securing vehicle network, this paper proposes a technique for protecting the communication between tire pressure/temperature sensors and the Tire Pressure Monitoring System ECU. The goal of this technique is to prevent locating the vehicle using its ID and thwart attacking other vehicle ECUs through eavesdropping on the message broadcasted by the sensors. This can occur because the receiving ECU, TPMS ECU, is connected to other ECUs through the CAN bus and other busses. If this attack succeeds, it can cause vital damage to the vehicle and the safety of drivers and passengers. For the security approach presented in this paper to work, smart sensors should replace regular sensors. The real IDs are not used after the first communication. They are replaced with anonymous IDs to prevent vehicle location attack. Security (symmetric) keys, Message Authentication Code key, nonce, secret value, and anonymous IDs are re-generated after each session. A session is made up of two communications: sending the measurements for pressure P, and temperature T by the smart sensors, and exchanging the new anonymous IDs.

Should other sensors, such motion sensor (MS), acceleration sensor (AS), and load detection sensor (LDS), be added, the approach could be easily scaled up by redistributing the bits among the measurements. If needed, the message containing the measurements could be divided into two or more messages of 64-bit each. T/P will be replaced with other measurements, such as T/P/MS/AS/LDS. The size of the counter CTR-1 need to be increased correspondingly.

REFERENCES

[1] P. Mundhenk, A. Paverd, A. Mrowca, S. Steinhorst, M. Lukasiewycz, S. A. Fahmy, and S. Chakraborty, “Security in Automotive Networks: Lightweight Authentication and Authorization,” ACM Transactions on Design Automation of Electronic Systems, vol. 22, no. 2, pp. 1-27, 2017.

[2] P. Tyagi, and D. Dembla, “Performance Analysis and Implementation of Proposed Mechanism for Detection and Prevention of Security Attacks in Routing Protocols of Vehicular Ad-Hoc Network (VANET),” Egyptian Informatics Journal, vol. 18, pp. 133–139, 2017.

[3] S. Rizvi, J. Willet, D. Perino, S. Marasco, and C. Condo, “A Threat to Vehicular Cyber Security and the Urgency for Correction,” in Proc. Complex Adaptive Systems (CAS 2017), Chicago, Illinois, USA, 2017, pp. 100-105.

[4] Y. Yang, Z. Wei, Y. Zhang, H. Lu, K. R. Choo, and H. Cai, “V2X Security: A Case Study of Anonymous Authentication,” Pervasive and Mobile Computing, vol. 41, pp. 259–269, 2017.

[5] G. Machera, H. Sporer, E. Brenner, and C. Kreiner, “An Automotive Signal-Layer Security and Trust-Boundary Identification Approach,” in Proc. The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017), Madeira, Portugal, 2017, pp. 490-497.

[6] S. Ray, W. Chen, J. Bhadra, and M. A. Al Faruque, “Extensibility in Automotive Security: Current Practice and Challenges,” in Proc. The 54th Annual Design Automation Conference (DAC’17), Austin, Texas, USA, 2017, pp. 1-6.

[7] E. G. AbdAllah, M. Zulkernine, Y. X. Gu, and C. Liem, “Towards Defending Connected Vehicles Against Attacks,” in Proc. The Fifth European Conference on the Engineering of Computer-Based Systems (ECBS’17), Larnaca, Cyprus, 2017, pp. 1-9.

[8] S. Tbatou, A. Ramrami, and Y. Tabii, “Security of Communications in Connected Cars Modeling and Safety Assessment,” in Proc. The 2nd International Conference on Big Data, Cloud and Applications (BDCA'17), Tetouan, Morocco, 2017, pp. 1-7.

[9] K. Daimi, M. Saed, S. Bone, and J. Robb, “Securing Vehicle’s Electronic Control Units,” in Proc. The Twelfth International Conference on Networking and Services (ICNS 2016), Lisbon, Portugal, 2016, pp. 29-34.

[10] M. Richter, “Understanding the ECU – What it Does and How it Works,” MC^2 Magazine, 2006, http://www.fes-auto.com/upload/articles/Understanding%20the%20ECU.pdf, pp. 62-65, [retrieved: May 2018].

[11] ETAS GmbH, “Electronic Control Unit (ECU) – Basics of Automative ECU,” 2014, http://www.scribd.com/doc/268828296/20140121-ETAS-Webinar-ECU-Basics#scribd, pp. 1-30, [retrieved: May 2018].

[12] Freescale, “Future advances in Body Electronics” https://cache.freescale.com/files/automotive/doc/white_paper/BODYDELECTRWP.pdf, 2013, pp. 1-18, [retrieved: May 2018].

[13] On Semiconductor, “Basics of In-Vehicle Neworking (INV) Protocols,” http://www.onsemi.com/pub_link/Collateral/TND6015-D.PDF, pp. 1-27, [retrieved: May 2018].

[14] S. Seo, J. Kim, S. Hwang, K. Kwon, and J. Jeon, “A Reliable Gatway for In-Vehicle Networks Based on LIN, CAN, and FlexRay,” ACM Transcation on Embedded Computing Systems, vol. 4, no. 1, pp. 1-24, 2012.

[15] B. Zou, M. Gao, and X. Cui, “Research on Information Security Framework of Intelligent Connected Vehicle,” in Proc. The 2017 International Conference on Cryptography, Security and Privacy (ICCSP '17), Wuhan, China, 2017. pp. 91-95.

[16] M. Kang, and J. Kang, “Intrusion Detection System Using Deep Neural Network for In-Vehicle Network Security,” PLOS ONE Journal, pp. 1-17, 2016.

[17] A. Lima, F. Rocha, M. Völp, and P. Esteves-Verissimo, “Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems,” in Proc. The 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC’16), Vienna, Austria, 2016, pp. 59-70.

[18] M. Lukasiewycz, and P. Mundhenk, S. Steinhorst, “Security-Aware Obfuscated Priority Assignment for Automotive CAN Platforms,” ACM Transactions on Design Automation of Electronic Systems, vol. 21, no. 2, pp. 1-27, 2016.

[19] L. Pan, X. Zheng, H. X. Chen, T. Luan, H. Bootwala, and L. Batten, “Cyber Security Attacks to Modern Vehicular Systems,” Journal of Information Security and Applications, vol. 36, pp. 90–100, 2017.

[20] G. W. Hunter, J. R. Stetter, P. J. Hesketh, and C. Liu, “Smart Sensor System,” The Electrochemical Society Interface, pp. 29-34, 2010.

[21] R. N. Johnson, “Applying Smart Sensor Technology to Existing Real-World (Legacy) Systems,” Telemonitor Inc., pp. 1-10, 2002, http://telemonitor.com/wp-content/uploads/2015/06/Smart-real-world-legacy-system-SmLegManu.pdf, [retrieved: May 2018].

[22] A. Yang, “TPMS,” Freescale, pp. 1-74, 2014, http://cache.freescale.com/files/training/doc/dwf/DWF14_TechDay_CN_Baoding_SEP_25_007.pdf, [retrieved: May 2018].

[23] Bridgestone Tires, “What is TPMS and How Does It Work,” https://www.bridgestonetire.com/tread-and-trend/drivers-ed/tire-pressure-monitoring-system-how-tpms-works, [retrieved: May 2018].

[24] S. Kim, C. K. Bae, Y. M. Ko, and D. J. Kim, “Communication Protocol for Bidirectional TPMS,” in Proc. The Ninth International Conference on Ubiquitous and Future Networks (ICUFN’17), Milan, Italy, 2017, pp. 791-793.

[25] H. W. Chun, "Technology and Service Trends of Smart Car," ETRI Electronics and Telecommunications Trends, vol. 27, no. 1, pp. 147-157, 2012.

[26] P. Bright, “Cars Hacked Through Wireless Tire Sensors,” Arstechnica, https://arstechnica.com/information-technology/2010/08/cars-hacked-through-wireless-tyre-sensors, [retrieved: May 18].

[27] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, H. Shacham, and S. Savage, “Experimental Security Analysis of a Modern Automobile,” in Proc. The 2010 IEEE Symposium on Security and Privacy (SP), Berkeley/Oakland, CA, USA, 2010, pp. 447-462.

[28] I. Roufa, R. Millerb, H. Mustafaa, T. Taylora, S. Ohb, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study,” in Proc. The 19th USENIX conference on Security (USENIX Security'10), Washington, DC, USA, 2010, pp. 21-36.

[29] D. K. Kilcoyne, S. Bendelac, J. M. Ernst, and A. J. Michaels, “Tire Pressure Monitoring System Encryption to Improve Vehicular Security,” in Proc. The 2016 IEEE Military Communications Conference (MILCOM 2016), Baltimore, MD, USA, 2016, pp. 34-44.