A Blockchain-Based Mutual Authentication Method to Secure the Electric Vehicles' TPMS

Author(s): Razmjoui, Pouyan; Kavousi-Fard, Abdollah; Jin, Tao; Dabbaghjamanesh, Morteza; Karimi, Mazaher; Jolfaei, Alireza

Title: A Blockchain-Based Mutual Authentication Method to Secure the Electric Vehicles' TPMS

Year: 2023

Version: Accepted manuscript

Please cite the original version:

Razmjoui, P., Kavousi-Fard, A., Jin, T., Dabbaghjamanesh, M., Karimi, M. & Jolfaei, A. (2023). A Blockchain-Based Mutual Authentication Method to Secure the Electric Vehicles' TPMS. *IEEE Transactions on Industrial Informatics*. https://doi.org/10.1109/TII.2023.3257294

A Blockchain-Based Mutual Authentication Method to Secure the Electric Vehicles' TPMS

Pouyan Razmjoui, Abdollah Kavousi-Fard, *Senior Member, IEEE*, Tao Jin, *Senior Member, IEEE*, Morteza Dabbaghjamanesh, *Senior Member, IEEE*, Mazaher Karimi, Alireza Jolfaei

***Abstract*— Despite the widespread use of Radio Frequency Identification (RFID) and wireless connectivity such as Near Field Communication (NFC) in electric vehicles, their security and privacy implications in Ad-Hoc networks have not been well explored. This paper provides a data protection assessment of radio frequency electronic system in the Tire Pressure Monitoring System (TPMS). It is demonstrated that eavesdropping is completely feasible from a passing car, at an approximate distance up to 50 meters. Furthermore, our reverse analysis shows that the static *n*-bit signatures and messaging can be eavesdropped from a relatively far distance, raising privacy concerns as a vehicles' movements can be tracked by using the unique IDs of tire pressure sensors. Unfortunately, current protocols do not use authentication, and automobile technologies hardly follow routine message confirmation so sensor messages may be spoofed remotely. To improve the security of TPMS, we suggest a novel ultra-lightweight mutual authentication for the TPMS registry process in the automotive network. Our experimental results confirm the effectiveness and security of the proposed method in TPMS.**

***Index Terms:* Cybersecurity, Blockchain, Electric Vehicle, TPMS, Authentication.**

Nomenclature

Indices	
SQN_R	Random number created by RF receiver
SQN_S	Random number created by WE sensor
SQN_P	Random number created by TPMS Receiver
UID_N	Present session pseudonym
UID_O	Previous session pseudonym
SK_N	Present session secret- key (SK)
SK_O	Pseudonym for latest session secret –key (SK)
$hash$	SHA(256)

I. Introduction

Vehicle protection is progressively troubling, as cars become more dependent on computer technology. These technologies not only complement the conventional mechanical component functionality but also retrieve telemetry data and assist with the policy process by drivers. Recent studies have revealed many dimensions of these issues, such as encrypted computer machinery and software design [1], protection and security of the vehicle transmission network [2], and efforts to adversely measure the automotive contact systems [3]. In this way, the implementation of message delivery system by radio frequency, which comprises in-vehicle networks and vehicle contact networks, is of special importance [4,5]. In addition, much attention has been paid to vehicle-to-vehicle and vehicular systems communications [6,7]. One of the early built-in mobile connections of transportation systems is basically a network device in the vehicle, called the tire pressure monitoring system (TPMS) [8]. Although the cyber-threatening substances are all cellular control units, TPMS is of specific importance since it is a requirement of the National Highway Traffic Safety Administration (NHTSA) [9]. NHTSA released a study on the future regulatory requirements on TPMS for most cars weighing less than 10,000 pounds in 2001-2002[8]. Radio Frequency Identification (RFID) is a methodology for transmitting cellular data in order to identify and evaluating data unique to vehicles carrying a special transponder named the RFID tag [9]. One promising idea is to use RFID techniques to construct cost-effective wireless sensor nodes [10,11]. While both direct and indirect measuring instruments are usable, just direct types have the reliability of the Transportation Recall Enhancement, Accountability and Documentation (TREAD) laws and are afterward the only measurements to be used. In this way, if any tire is significantly slightly deflated or overinflated; either passenger cars, trucks, or multipurpose passenger vehicles; TPMSs uninterruptedly quantify air pressure interior and notify drivers.

The majority of cars are fitted with direct TPMSs. In order to measure tire pressure, these structures depend on battery-operated-powered pressure sensors within the tire and communicate their message signal through a radio frequency (RF) transmitter. In response, the tire pressure control unit processes the data and can transmit command signal over the Controller Area Network (CAN) for example to the Central Control Unit (CCN) to activate an alert message on the dashboard of the vehicle. This paper focuses on direct TPMSs due to the security weaknesses and the consequences for the drivers. Direct TPMSs usually are an easy target because of the failure of cryptography frameworks. Technically, TPMS communication protocols are based on simple protocols and common modulation schemes.

Reversing the data frame format can possibly lead to hacking the TPMS sensors. By penetrating into the wireless module, the attacker can eavesdrop on the TPMS sensors communication. The TPMS sensors measure tire parameters and transmit radio packet signal that includes two segments. The first one is the preamble of frame format and the second one is the tire data that include the information such as the temperature, pressure, TPMS sensor ID and cyclic redundancy check (CRC bits). By

Corresponding Authors: (Prof. Tao Jin email: jintly@fzu.edu.cn and Prof. Abdollah Kavousi-Fard email: abdollah.kavousifard@gmail.com)

P. Razmjoui is with the Department of Electrical Engineering, Fuzhou University, Fuzhou, Fujian China 350116. (Pouyanrazmjouei@irantvt.ir and)

A. Kavousi-Fard is with the Department of Electrical Engineering, Fuzhou University, Fuzhou, Fujian China 350116 and also with the Electrical Engineering Department, Shiraz University of Technology, Shiraz, Iran. (abdollah.kavousifard@gmail.com)

T. Jin is with the Department of Electrical Engineering, Fuzhou University, Fuzhou, Fujian China 350116. (jintly@fzu.edu.cn).

M Dabaghjamanesh is with R&D Department, Electric Reliability Council of Texas, Taylor, TX 76574. (morteza.d@ieee.org)

M Karimi is with the School of Technology and Innovations, University of Vaasa, Wolffintie 34, 65200 Vaasa, Finland. (mazaher.karimi@uwasa.fi)

A Jolfaei is with the Cybersecurity and Networking at Flinders University, Australia. (alireza.jolfaei@mq.edu.au)

comparison, the automotive network system architecture appears to have a mutual smart contract in all messages received and provides little evidence of critical security protocols such as the authentication mechanism. Simple malicious behaviors can cause TPMS malfunction.

By considering the restricted sensor resources and the importance of user-friendly design, developing a bullet-proof protocol to protect TPMS communications is impractical. Asymmetric cryptographic techniques and even certain symmetric encryption algorithms are beyond the computation abilities of these wireless sensors. Even so, a huge amount of work was needed to analyze their concerns regarding privacy and protection. RFID systems [12,13], mainstream marketplace UbiComp devices [14], residential robots [15] and implantable medical products [16] are the devices being tested.

Authors in [17] proposed a model to secure the charging system in the electric vehicles. To this end, it suggests a mutual authentication using Burrows–Abadi–Needham logic. In relation to the prevailing distribution, authors in [18] suggested a random key pre-distribution strategy, in which every single node preserves a series of keys arbitrarily from the maximum allowable secret key. At least one key will be exchanged by any two adjacent nodes with a high probability, and the shared key is used to build on-demand pairing keys among sensors. In addition, an *n*-composite pre-distribution random key scheme is proposed in [19] wherein *n* general keys are transmitted instead of just one by any two neighboring nodes. TESLA [20] is a well-known authentication protocol used by wireless sensor networks (WSNs) to validate the broadcaster. Usually, validating a transmitted sender involves the use of asymmetric cryptographic algorithms (e.g., RSA), which is not really sufficient for resource-restricted sensor networks. TESLA uses symmetric cryptographic algorithms, but by exploiting temporal variations, it achieves asymmetric properties. With TPMSs, these key management systems do not function well, as sensor nodes in automotive network are concerned with setting keys among a big numbers of sensors, whereas TPMSs concentrate on setting keys among only four sensors and the Electrical Control Unit (ECU). Therefore, our stable protocol needs fewer resources (for example, space or energy estimation). Therefore, this paper assesses the cyber security concerns over the TPMS system. It also suggests to implement a shared ultralightweight RFID authentication mechanism for inclusion in a blockchain-enabled TPMS to guarantee the data security. The implementation itself is a new concept and the suggested technique gives additional strong security benefits toward potential attacks like spoofing, replay, and man-in-the-middle, making sure the privacy of the information are been written to the public ledger of the blockchain. The performance of the proposed secured model is assessed on a practical electric vehicle system.

The rest of the paper is organized as below: section II describes the TPMS system. Section III provides a security and privacy analysis. Section IV proposes a blockchain enabled ultralightweight method for TPMS. The cyber attack modeling is presented in section V. the simulation results are discussed in section VI. Finally, the main paper output are presented in section VII.

II. TPMS SYSTEM

The air specifications such as pressure and temperature of all 4 road wheels are supervised by TPMS. As an RFID transponder, the wheel-mounted tire pressure detectors transmit data to the TPMS electronics module via radio frequency signals. The TPMS module is a radio receiver that collects the air pressure and temperature data from each tire sensor. The information is then transmitted via CAN-BUS to the TPMS Receiver Unit in which a specified pass/fail criterion is defined. Fig. 1 displays all elements of the tire surveillance system.

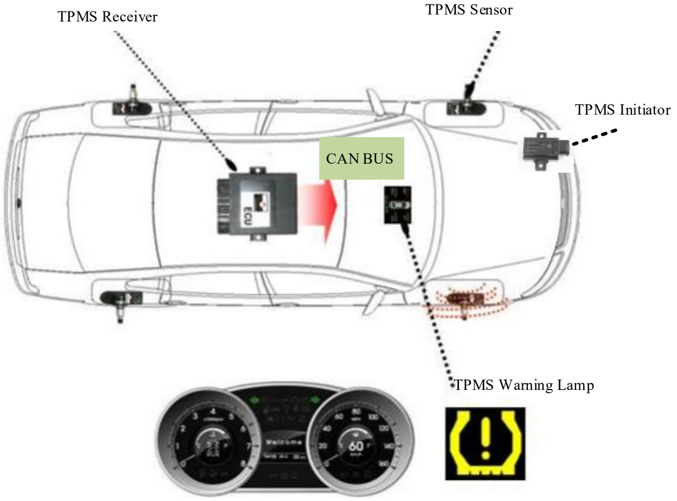

Fig.1. TPMS component

When the vehicle's speed reaches 32 km/h (20 mph), the TPMS sensors periodically send radio signal data every 60 seconds. The TPMS Receiver evaluates any transmitting data of TPMS sensors according to a low-pressure threshold set point. If it is recognized that the tire pressure drops below the set point, this is conveyed to the Instrument Panel Cluster (IPC) on the vehicle contact bus. The IPC then lights the alert indicator for TPMS.

The NHTSA specifies three forms for automotive manufacturers to enforce laws: direct, indirect, and hybrid [22]. Typically, direct TPMS involves pressure sensors mounted inside each tire to directly calculate the tire parameter inside the tire. Indirect TPMS measures velocity information gathered from wheel speed sensors of the vehicle's Anti-lock Braking System (ABS) to equate tire rotational speeds with each other to identify the air pressure of wheel. Direct systems are more precise and coherent, while for each vehicle, indirect systems would be less electronics-dependent and more powerful. The NHTSA deliberately leaves the concept of a hybrid TPMS ambiguous and indicates that such a program will be using a mix of direct and indirect approaches to satisfy regulatory requirements. Indirect TPMS, as described in Transport & Environmental (T&E) [23], is incapable to accurately calculate tire pressure in real-time. Necessary regular reconfiguration requires the vehicle to travel to operate linearly, which may cause limp home mode depending on road conditions influencing the wheels rotation and acceleration. Limp home mode is a security feature in the car which activates when each of the built-in control unit diagnoses a fault. T&E believes that indirect TPMS systems usually conform towards regulation specifications, but in many other practical circumstances during testing "display extremely weak results". The direct TPMS is the most widely used system in today's automobiles. However, their placement in the tires needs time, energy, and labor in the event that repairs or adjustments are necessary.

According to Fig. 2, when the vehicle begins moving, LF Initiator is driven through the LIN-BUS network via the RF receiver module. LF Initiator gets a specific ID that the system also utilizes to make the distinction the exact position of the tire throughout normal operating conditions. The LF Initiator emits a wake-up request to the Transponder Current sensor via a modulated signal of 125 kHz when an RF receiver signal has been received.

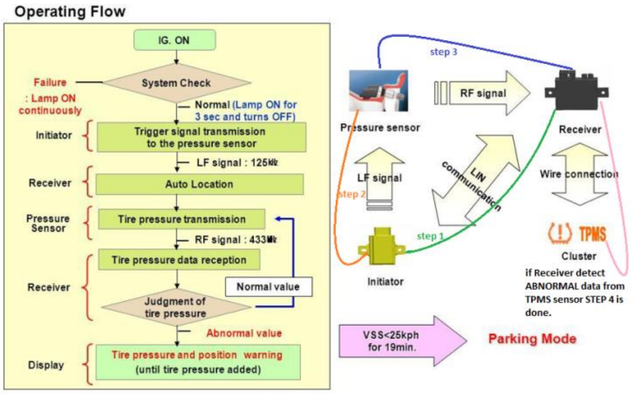

Fig.2. Operation flow of TPMS communication

Whenever the Transponder Transmitter module receives an LF (125 kHz) awaken request signal, the Analog Front End (AFE) justifies the incoming request. The microcontroller is only woken up from sleep mode after a valid signal has been received. The achievement earned by the node is specified by that of the command signal received. Normal demands assess tire strength, temperature, and acceleration. Learn Mode request labels the sensor device with a new ID for potential operations before the measurements. The RF module in the tire transponder sensor then sends the information through UHF (433.9 MHz) to the RF receiver and switches to standby mode if no further interrupts have been sensed. All tire sensors regularly broadcast the measurements of temperature and pressure along with corresponding IDs. The RF receiver module receives the packet data and performs a specific procedure before trying to send the warning light messages to the IPC. Initially, because it can begin receiving packets from nearby car sensors, it separates those packets out. Then, it conducts temperature adjustment, wherever the pressure measurements are adjusted and variations in tire pressure are evaluated. The exact implementation of the product varies considerably along with all manufacturers, especially with respect to antenna configuration and communication protocols.

There are proprietary communication protocols used by sensors and tire pressure monitoring electronic module. Nonetheless, we understand that TPMS data communication typically uses the 315 MHz or 433 MHz UHF frequencies and ASK (Amplitude Shift Keying) or FSK (Frequency Shift Keying) modulation scheme from manufacturer databases and product information. Any tire pressure sensor as RFID transponder contains a unique ID and Secret Key (SK) that are stored and encrypted in E2prom memory of tire sensor module. Just before that RF receiver can accept information collected by each of the four tire sensors, sensor IDs and wheel position on which it is mounted must be tried to configuration into the TPMS module either manual or automatically, like in many vehicles or in certain very good quality automobiles. This is usually done through the installation of the tire. Subsequently, the sensor Identifier has been the essential information that allows the TPMS module to recognize the source of data stream and to strip out the packets that other vehicles have transmitted. In order to increase the energy usage of battery in the tire transponder, tire sensors are built to be in sleep mode almost always and to wake up in two possible situations: (1) by the time the driver continues traveling at high velocity (more than 40 km/h), sensors are permitted to measure tire data such as pressure, temperature, and accelerator; (2) throughout diagnostic and initial sensor ID cycles, devices are utilized to transfer their IDs or other information. As a result, the tire sensors will wake up in sleep-mode in two trigger strategies: when a velocity of the vehicle is greater than 40 km/h or an RF switching on signal that is triggered by RF receiver.

III. Security and Privacy Analysis Goals

This paper focuses on tracking threats through listening to sensor identifiers and Denial Of Service (DOS) attacks with message spoofing risks through injecting forged data into the tire monitoring device. We would consider attacks where, by deliberately inserting forged messages, an attacker interferes with the regular operations of TPMS. For instance, an attacker can attempt to submit a low-pressure packet to cause a low-pressure alert. Likewise, the adversary can thread across a few faked low-pressure data packets and maybe a few sporadic pressure data frames, causing the low-pressure warning light to switch on and off. If feasible, such attacks could weaken the confidence of drivers in the system and possibly contribute to fully neglect TPMS-related alerts. After that, because the TPMS sensors still reply to the relevant triggering signal, an opponent who uninterruptedly emits activation signals continually causes the tire sensors to send packets, thus dramatically decreasing the TPMS's lifespan. For example, the attackers might try to transmit a low-pressure radio signal to activate a low-pressure warning lamp in the IPC. Additionally, the attacker will cycle through a few falsified low-pressure and temperature data burst and a few pressure and temperature normal bursts of data, then triggering the warning lights to switch on and off at low pressure. Even if these attacks possibly occur, they can weaken the confidence of drivers in the system and cause significant problems to fully dismiss the TPMS-related alerts. In conclusion, even though tire sensors every time react to the corresponding activation signal, an attacker who repetitively communicates activation signals can force tire sensors to transmit messages continuously, massively reducing the life of TPMS.

Being able to conduct surveillance from a path length on TPMS communication enables us to further check the potential of embedding falsified information into safety-critical in-vehicle systems. Although the TPMS is not yet an extremely important protective device, we are interested in two points: (1) whether the awareness of an RF receiver inside the car is sufficiently high to authorize spoofing from elsewhere in the vehicle or from a nearby automobile; and (2) the protection mechanisms in these structures are vulnerable to the DOS attack. In general, we are interested to know whether the tire monitoring system is rejecting suspicious packets using authentication, input validation, or filtering processes.

A real-time model can deliberately listen and trace tire sensors communication and decrypt data frame format, Fig. 3.

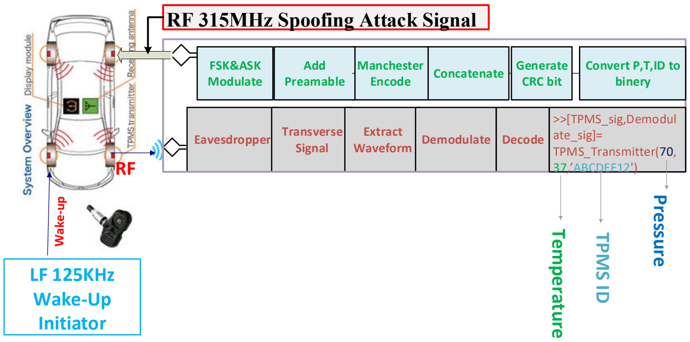

Fig.3. Spoofing attack

Frequency mixing methodology used in our experiment spoofing attack. So we used two ADF7020 daughter boards and the AD831 frequency mixer. While broadcasting a signal from one ADF7020 into the mixer's LO connection, We've been able to combine the spoofed packet from the other ADF7020 to the relevant frequency. We relayed spoofing RF 315 MHz signal to RF tire sensor receiver inside the vehicle, used a signal at 5.0 GHz. We decrypted spoofed sets of data with the FOXWELL NT1001 TPMS trigger device to evaluate our method in Fig. 4. In this figure Shows a TPMS Trigger screenshot after delivering a fake packet with the "8178E561" sensor ID and tire pressure of 240 Kpa.

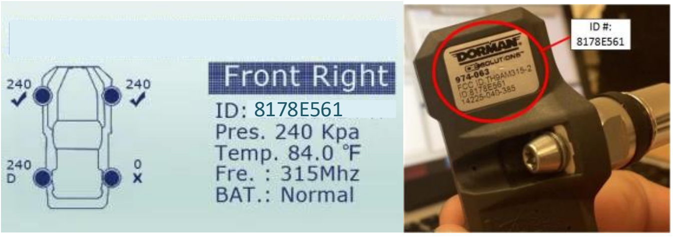
Front Right
ID: 8178E561
Pres. 240 Kpa
Temp. 84.0 °F
Fre. : 315Mhz
BAT.: Normal

Fig.4. The TPMS trigger tool displays the spoofed packet with the sensor ID: '8178E561'.

After that, we used this configuration to transmit distinct manipulated data to a target using tire sensor (A) at a rate of 60 packets per second. We initiated broadcasting one spoofed message with the front-right-tire ID and eavesdropping on the complete communication to recognize the minimum threshold of triggering the TPMS-LPW light in IPC. We found that one spoofed packet of data was not able to initiate the TPMS LPW light, and as a reply to this request, the TPMS receiver simultaneously sent two triggering signals via the antenna located near the right front tire, triggering the right front sensor to send ten packets. Thus, even though a single spoofed message doesn't really affect any alert to be displayed by the IPC, this does launch a vulnerability to a battery power attack. Besides that, we progressively exceeded the frequency of spoofed packets and observed that broadcasting five spoofed packets in a second may be enough to turn on elucidate the light of TPMS-LPW. The spoofing of the insertion signal influences the sensors to transmit packets and enables the tracking of attacks. Because the activation signals are very basic, a limited amount of bits can be transmitted. So that, using just lengthy data packages with encryption and digital signatures is not appropriate, so we propose that the few bits that can be transmitted be used as a sequencing sector, in which sequencing implements a one-way function chain in some kind of pattern similar to one-time signatures. Therefore, it would be the function of the RF module and TPMS Receiver to preserve the one-way function chain, and the TPMS sensor would actually hash the sequence number detected and equate it with the prior serial number. This would have a convenient way to anomaly detection and filter out the false triggering signals. In conclusion, the lack of authentication methods and insufficient validation mechanisms would open several vulnerabilities for attackers to exploit for a more innovative attack. Nevertheless, a simple and reliable RFID protocol is required that could be applied to the automotive network.

IV. ULTRALIGHTWEIGHT PROTOCOL FOR BLOCKCHAIN

Technically, the protocols for in-vehicle communication are classified based on their characteristics, and application type. To shortly name, the available security solutions for in-vehicle communication are **machine learning-based methods**, **port-centric techniques** and **cryptography concept**. Although the machine learning techniques have shown good accuracy to secure the vehicle, but the current available RAM and CPU existing in the vehicles are not appropriate for running high computations. In other words, these techniques are not applicable for the current vehicles and need more time to be used in the future vehicles. In the second group, port-centric techniques exist which suggest to focus on the security of data at the point of entering ports. This means that any data entering the vehicle needs to be first analyzed and checked by appropriate security methods and then used in the vehicle. For sure, this can make a big delay in the system due to the high computational costs. Moreover, these protocols perform based on a fixed value during the whole process. Hence, an adversary can easily conduct a tracking attack to monitor the movement of the RFID tag built-in TPMS based on this value. In order to overcome the shortcomings of the first two groups, cryptography methods were suggested which could gain high popularity in recent years. These methods are not much time consuming and can provide high security and privacy by converting the data into unreadable codes. This paper addresses vehicular security as opposed to the TPMS data confidentiality, because the TPMS message confidentiality is of relatively low security risk in its application (as described in Section III). What affects the security of the cryptography depend on the encryption and decryption process.

Adoption of new technologies which plays an important role not only in ensuring the reliability of IoT, but mostly in creating new administration potential for blockchain [24],[25], can resolve the above disadvantages. Blockchain was launched in 2008 and was initially intended to fix problems with the existing economy [26], Not only has the technology allowed its users to make purchases without third-party intermediaries involved, but it has proven to become more versatile than just a means of consolidating control of resources [27, 28]. In addition to the automotive network, the other most convincing blockchain technology use cases include digital identity, healthcare, and energy markets. Blockchain is a decentralized distributed database scheme that is operated jointly by all nodes in the blockchain network. It consists of a number of data items generated based on the cryptography technique, and inside the blockchain, each data block is a block. In order to create a chain of data according to the order in which they were created, blocks are connected in an ordered manner. The block relation is confirmed via the hash value of the block header data. The blockchain uses this hash value as the individual identifier number for all blocks, and by the root block hash values determined in the block header, the unique related block can be found in the blockchain. For this process, each node linked to its parent block hash value chain creates a string from the last block to the first block, providing a connection like data format for entirely blocks, as seen in Fig. 5.

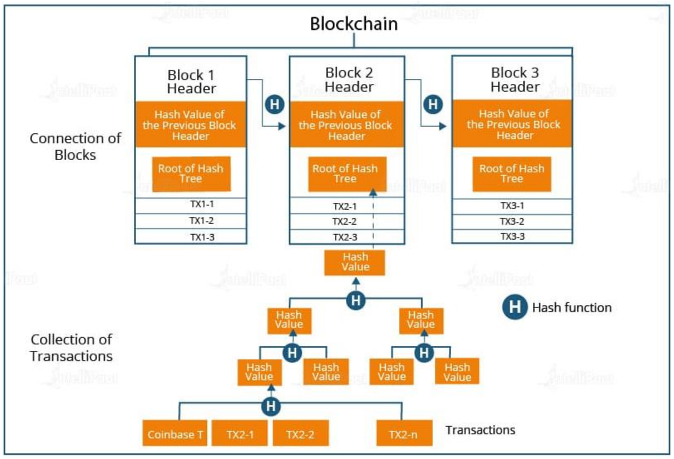

Fig.5. Existing blockchain system and block content simplified

All tire sensors are used as peer nodes in paper to create a blockchain network and transmit on-road messages to vehicles. The blockchain network basically keeps record of two different types of information, one of which is WE sensors vehicle identification information that contains the pseudonym, the public key of the RFID transponder and the mapping connection among the pseudonym as well as the origenal identity. The other is the declaration of the hash value for legal vehicles. The blockchain actually cannot be used to store vast volumes of data, but we only save in the blockchain the index value of the declarations of which the blockchain data storage burden and the difficulty of preserving data integrity are held.

The following parties are involved in the protocol: RFID-tag in TPMS sensors, RF receiver, and chain node. Bitwise XOR and rotation operations are used to implement the proposed method because the low priced IoT device is computationally limited. Yet there are no computational limits to the chain node. More stringent computing operations can also be performed, like creating the SHA-256 hash function and verifying the history of the commodity regarding the data contained in the blockchain. SHA-256 hash function is used to encrypt IDS and K hidden data before finally assigning it to a block header. Then these stored values may be used for all supply chain nodes during the authentication process.

An analysis assumes where the channel of communication between the chain node and the receiver is safe while the channel of communication between the receiver and a tire sensor is insecure. However, because of the existence of a distributed ledger, the set of values stored in the blockchain is believed to be stable. The technique is considered to secure the transmitted messages among the reader and the tag over the communication channel. Fig. 6. summarizes the operations that take place between the TPMS Receiver node, RF receiver, and tire sensors during the authentication process, followed by a detailed description of any stage. Notes used in the proposed protocol will be listed in nomenclature. The ultralightweight protocol suggested is described:

1. In order to start a communication, the RF receiver transmits a 125KHz wake-up message and a RN SQN_R to all the WE sensors.

2. Next both of the messages were received, the WE sensor calculates frame messages S_1, S_2 using its stored ID, SK produced random number SQN_S, in addition received random number SQN_R . The WE module transmits the calculated data S_1, S_2 to the RF receiver.

$$\begin{aligned} S_1 &= ROT(ID \oplus SQN_R, SQN_{S_{HW}}) \\ S_2 &= ROT(SK \oplus SQN_R, SQN_{S_{HW}}) \oplus ROT(ID, SQN_{R_{HW}}) \end{aligned} \tag{1}$$

3. The RF receiver forwards messages of SQN_R ,S_1, and S_2 to the TPMS Receiver as a automotive network chain node.

4. The TPMS Receiver node extracts ID, SK by creating hamming weight SQN_S that named SQN^*_{S-HW} and executes the following operations till a corresponding $hash(ID \parallel SK)$ is obtained from permissioned blockchain. Since SQN_S is 96 bits, we have SQN^*_{S-HW} between 0 and 96.

$$\begin{aligned} ID' &= RROT(\mathrm{S}_1, SQN'_{S_{HW}}) \oplus SQN_R \\ SK' &= RROT[S_1 \oplus ROT(ID', SQN_{S_{HW}}), SQN'_{S_{HW}}] \oplus \mathrm{SQN}_R \end{aligned} \tag{2}$$

Based on the $hash(ID \parallel SK)$, the TPMS Receiver node will validate and monitor the tire environmental parameters along with the permission level. The TPMS Receiver node will verify the tire sensors if the information has a valid record of history in terms of the time stamp, position, and sensor status. Then, a unique number SQN_{pcm} and an even hamming weight of a random number is for both the write and read authorization level will be generated by TPMS Receiver; unless, an odd hamming weight of a random number is generated. The TPMS Receiver node calculates P_1 and P_2 and transmits those messages to the RF receiver. Next, the TPMS Receiver node updates ID_N and SK_N consequently. The TPMS Receiver attaches a transaction with the current one after this upgrade and verification phase $hash(ID_N \parallel SK_N)$, and previous $hash(ID \parallel SK)$ values to the blockchain.

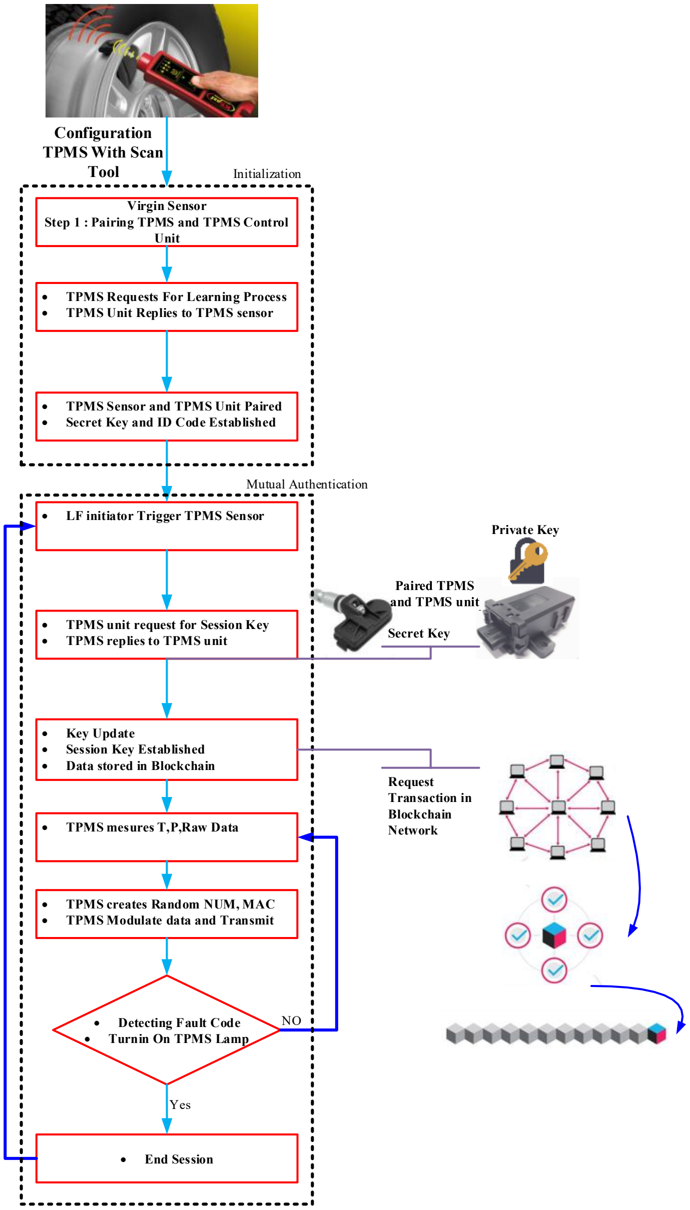
Configuration TPMS With Scan Tool
Initialization
Virgin Sensor
Step 1 : Pairing TPMS and TPMS Control Unit
TPMS Requests For Learning Process
TPMS Unit Replies to TPMS sensor
TPMS Sensor and TPMS Unit Paired
Secret Key and ID Code Established
Mutual Authentication
LF initiator Trigger TPMS Sensor
Private Key
Paired TPMS and TPMS unit
Secret Key
TPMS unit request for Session Key
TPMS replies to TPMS unit
Key Update
Session Key Established
Data stored in Blockchain
Request Transaction in Blockchain Network
TPMS mesures T,P,Raw Data
TPMS creates Random NUM, MAC
TPMS Modulate data and Transmit
Detecting Fault Code
Turnin On TPMS Lamp
NO
Yes
End Session

Fig.6. Flowchart of the ultralightweight TPMS communication protocol.

5. The RF receiver forwards messages P_1 and P_2 to the all tire sensors.

6. After receiving messages P_1 and P_2, the sensor derives random number SQN_P^* from the receiving data P_2.

$$SQN'_P = RROT(\mathrm{P}_2 \oplus ROT(SQN_R, SK_{HW}), ID_{HW}) \qquad (3)$$

The WE detector validates the RF receiver if P_1^*, which is calculated from the extracted SQN_P^* is equivalent to the received P_1 . Subsequently the confirmation, the tire sensor bring up-to-date its ID_N and SK_N if the hamming weight of SQN_P^* value that is even. If the hamming weight of SQN_P^* is an odd value, the sensors doesn't upgrade its ID_N and SK_N.

$$\begin{aligned} ID_{new} &= ROT[SK \oplus SQN_S, ID_{HW}] \oplus ROT[ID \oplus SK, SQN_R] \\ SK_{new} &= ROT[SK \oplus SQN_R] \oplus ROT[SQN_R \oplus SQN_S, \mathrm{SK}_{HW}] \end{aligned} \qquad (4)$$

To provide independence across the ID, SK updates to prevent the attacker from tracking the ID, SK , we design and implement a random scheme. The randomization updates are based on a pseudo-random generator using a ultralightweight mode with no new input plaintexts. In other words, the random output from the Randomization algorithm (providing the current ID, SK becomes the input of the algorithm for the next ID, SK update. Using a Randomization algorithm, the output corresponds to the randomized ID, SK for the TPMS communication header ID_{new}, SK_{new} where i corresponds to the TPMS transmission time index. This output then becomes the input for the next communication. At time $t+1$, ID, SK is the input of the Randomization algorithm, i.e., $ID_{new}, SK_{new} = Randomization\left(ID, SK\right)$: The ID, SK for driving the pseudo-random generator Randomization is fixed, and is generated when the TPMS sensor is deployed on the EVs, e.g., the WE sensor gets replaced.

V. Cyber Attack Models

The hypotheses are used in the study of two potential spoofing attacks on the suggested technique:

1. An attacker has the power to start communication with the receiver and with a WE sensor.

2. An intruder will collect information, capture, interrupt, and modify messages that are transmitted when contact between the receiver and a tire sensor.

A. Spoofing attack

Spoofing attacks take place whenever an attacker collects signals shared on a chat channel and replays them in order to decrypt or obtain access to data. To explain how an opponent can attempt and fail to initiate a replay attack, some examples are illustrated below.

1. The opponent replays the recorded messages S_1 and S_2 during the previous Reader session. Nonetheless, the opponent will not be efficacious as the reader is not to be able to validate the signals as transmit by a honest tag because with each new session ID and SK are encoded with new random numbers $(SQN_R\ , SQN_S)$.

2. Attacker replays signals P_1 , P_2 taken in a previous session to the WE sensor . Once again, the opponent will not be effective because the sensor is unable to authenticate the messages because separate random numbers $(SQN_R\ , SQN_P)$ are needed for each new session to compute messages P_1 and P_2 . Since the adversary will be unable to extract any communications using one or both of the malicious schemes mentioned above from the receiver and sensor, the suggested technique will survive replay attacks.

B. MAN-IN-THE-MIDDLE ATTACK

Man-in-the-Middle (MITM) Attack happens mostly during the propagation of the signal, where the contact is eavesdropped, intercepted, and monitored by the enemy. Using many methods mentioned below, the adversary may put effort to carry out a MITM attack, which also will not accomplish:

1. Adversary data frame S_1 and S_2, and then changes them already transmitting to the RF reader device. The supply chain node is incapable to gain a identical $hash(ID \parallel SK)$, value in the blockchain since the adversary is not capable to obtain the

particular values of SQN_S, SK, and ID to calculate a result frame S_1 and S_2.

2. Adversary blocks messages P_1 and P_2 , then changes them before resending to the RFID tag in tire sensor. Because the two signals P_1 and P_2 are calculated from modernized random number SQN_{PCM}, SK, ID for each session, the adversary is not to be able to speculate on right signals of P_1 and P_2, though, the sensor is incapable to verify the fake signal, since the signals P_1^* and P_2^* calculated are not the same in comparison to the modified signals P_1 and P_2. This shows that the protocol suggested is shielded from MITM attacks.

VI. Simulation Results

The efficiency of the lightweight secure communication procedure TPMS was quantitated. We concentrated specifically on the performance of four phases: comparing the confidentiality of the encryption scheme suggested, the time of encryption and decryption, the throughput of encryption and decryption, the significant size of secrecy, and the number of confidential information.

A. PERFORMANCE ANALYSIS

The efficiency of the proposed protocol is evaluated respectively in terms of the cost of storage, computation, and communication. Due to the high computational power of the RF receiver and TPMS Receiver, the output of resource-constrained RFID transponder in each tire sensor is thus analyzed.

- *Encryption/Decryption time*

The key response time or computational time is the elapsed time between the moment when the challenge is sent by the TPMS unit and the beginning of the response from the TPMS sensor that we consider as a latency time. The computational time of cryptography technology is further divided into encryption/decryption time, key generation, and key exchange time. The computation of latency time allows us to estimate (i) how much delay could the physical-layer relay attack exploit without any practical detection being possible (ii) what is the design decision behind the maximum acceptable delays allowed by the evaluated systems. We note that the numerical differences of these two measures between EVs models are due to the hardware used as well as the implementation of the secure protocols (e.g., message size, type of encryption). In order to measure the key response time, we recorded the protocol message exchanges between the EVs and TPMS sensor at radio frequency (RF) with an oscilloscope using high sampling rate (from 20 to 50 MS/s depending on the TPMS system).

The encryption/decryption time is calculated by converting plain text (message) into ciphertext (and vice versa). The key generation time depends on the length of the key, and symmetric ciphers are different from asymmetric ciphers. The key exchange time depends on the communication channel between the sender and the receiver.

Table I contrasts the proposed model's encryption time with other models. Obviously, the suggested framework is the most time-efficient scheme, and AES&3DES&SHA-256 has a generally smaller encryption time than other versions. It is presumed that the duration of encryption is directly related to file size, i.e. for greater file size, longer encryption time is required. Table II evaluates the decryption times of the developed framework and other models. As can be seen, decryption time is shorter in the proposed model than in other models. At 97 ms, a 1 MB file that is shorter than other versions is decrypted. Therefore, it is deduced here that the model suggested works better than others. Fig. 7 compares the suggested model's average encryption/decryption time and other models for various file sizes, such as (20-1000 KB based on average).

TABLE I
COMPARISON OF ENCRYPTION TIME OF DIFFERENT MODELS

Input data frame size (kB)	**Encryption Execution Time (ms)**					
	DES&ECC&SHA Hash function	RC4&DES& SHA-256 Hash function	AES-128&RC4&SHA-256 Hash function	AES-128&DES &SHA-Hash Function	RC4&AES-128&SHA-256 Hash Function	Proposed Protocol
20	3	3	7	7	7	2
40	5	7	10	9	9	4
60	7	9	16	14	14	6
80	11	12	19	15	17	8
100	14	15	25	21	22	10
140	19	22	28	23	24	15
160	22	26	31	26	37	17
180	25	30	35	28	30	19
200	27	32	41	32	35	21
240	32	39	42	33	36	26
280	37	46	50	38	42	32
300	43	49	65	48	53	34
400	55	65	78	59	65	43
500	66	79	94	70	78	56
600	82	95	108	82	89	66
800	93	111	142	120	129	76

TABLE II
A COMPARISON OF DECRYPTION TIME OF DIFFERENT MODELS

Input data frame size (kB)	**Decryption Execution Time (ms)**					
	DES&ECC &SHA Hash function	RC4&DES& SHA-256 Hash function	AES-128&RC4&SHA-256 Hash function	AES-128&DES &SHA-Hash Function	RC4&AES-128&SHA-256 Hash Function	Proposed Protocol
20	3	3	7	7	7	2
40	5	7	10	10	9	4
60	7	9	16	13	14	5
80	11	12	19	14	17	7
100	14	15	25	16	22	9
140	19	22	28	19	24	13
160	22	26	31	22	37	15
180	25	30	35	23	30	17
200	27	32	41	27	35	19
240	32	39	42	33	36	23
280	37	46	50	35	42	27
300	43	49	65	36	53	29
400	55	65	78	46	65	39
500	66	79	94	60	78	48
600	82	95	108	74	89	59
800	93	111	142	98	129	66

- Encryption/decryption throughput

The throughput of encryption is determined according to plaintext separated by the total time of encryption. Algorithm power and efficiency are demonstrated by higher throughput. The proposed model's encryption throughput is higher than that of other models. Fig. 7 displays the proposed model's encryption throughput. The throughput of decryption is measured on the basis of plaintext divided by the total time of decryption. Decryption throughput of the proposed model is greater than other implementations. Fig. 8 indicates the proposed model's decryption throughput, which has higher performance than other models.

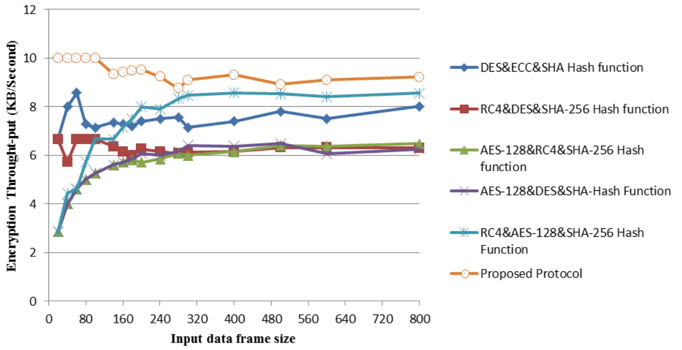

Fig.7. Encryption throughput of the proposed model and other models based on file size

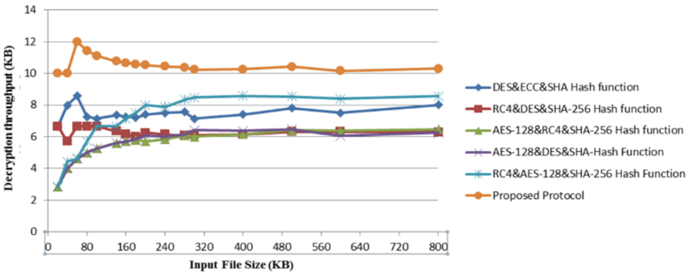

Fig.8. Decryption throughput of the proposed model and other models based on file size

- Storage Cost

This specific cost applies to the cost incurred by an RFID transponder inside each tire sensor by storing necessary data before implementation. An RFID transponder needs to store SK and ID with 96 bits length in our purposed protocol. Consequently, the total cost of storage is only the value of storing 192 bits of secret data in its memory, which would be significantly smaller than the protocols.

- Computational Cost

Let all the time necessary for the XOR operator, the hamming weight measurement time, and the time of rotate operations t_{XOR} ,t_{HW}, and t_{ROT} individually. Throughout the mutual authentication procedure inside the authentication phase, an RFID transponder in each tire sensor has a computational cost of $(7t_{XOR}+10t_{XOR}+8t_{XOR})$ and $(5t_{XOR}+7t_{XOR}+4t_{XOR})$ for upgrading of data analysis. Thus, the total computation cost, $T_{total}^{computainal}$ of tire sensor during the verification phase is assumed by $(12t_{XOR}+17t_{XOR}+12t_{XOR})$. It is concluded that only the computational cost of an OR-exclusive operation, t_{XOR}, may be overlooked as this value is significantly lower than that of using one-way hash values, $t_{hash(SHA(256))}$ and symmetric encryption, $t_{Encryption}$. However, because both hamming weight and rotation functions are bitwise operations, t_{HW}, and t_{ROT} are themselves insignificant and hence the cost function of $T_{total}^{computainal}$ is considered unimportant to the proposed protocol.

- Transmission Cost

Communication is started with a 40-bit LF wake-up and a 96-bit random-number SQN_R, which is transmit to the tire sensor from RF receiver. The suggested technique uses four messages (S_1,S_2,P_1,P_2) with 96 bits long to perform mutual authentication. The true cost of communication is also just the price of transmitting 520 bits, and is considerably lower than the protocols specified. Table III is provided for comparison between the security and performance of the proposed protocol and existing lightweight authentication protocols. Both the proposed protocols seem to be the only two that can defend RFID systems from all 5 security threats. The proposed protocol, though, as our solution demands the minimum cost of storage of all existing state-of-the-art implementations and is the only protocol built to be incorporated into the blockchain.

TABLE III
EXPECTED COST FUNCTION VALUE IN STATE OF THE ART AND PROPOSED PROTOCOL COMPARISON.

Description	purposed protocol	REF	REF	REF
Security protection from				
key	YES	no	yes	yes
replay	YES	yes	yes	no
spoffing	YES	no	no	no
Man-in-the-middle	YES	no	yes	no
tracking	YES	no	yes	yes
		PERFORMANCE		
STORAGE COST(bit)	192	384	384	424
COMPUTATIONAL COST(second)	$(12t_{XOR}+17t_{HW}+12t_{ROT})$	$(12t_{XOR}+7t_{XOR})$	$(9t_{XOR}+4t_{hash})$	$(9t_{XOR}+3t_{enc})$
COMMUNICATION COST(second)	520	616	576	512
Blockchain enable	yes	no	no	no

VII. CONCLUSION

This study describes an effective Ultralightweight RFID Secure protocol with mutual authentication that is integrated into a tire data monitoring system. TPMSs are one of the built-in wireless automotive networks which are integrated into novel electric vehicles (EVs). Like all modern vehicles, EVs are completely controlled by electronic control units embedded within networks that are exposed to cyber security threats. This paper assesses the venerable area in tire pressure monitoring systems by experimentally evaluating representatives. Our study shows that spoofing attack can disable the normal operation of the tire monitoring system. First, we reverse-engineered the TPMS communication protocols by using the USB Real-Time 10 MHz-60GHz Spectrum Analyzer, and showed that the current TPMS sensor in EVs does not utilize any secure communications technique. Also, it transmits a fixed sensor ID number in each packet data, which raises the possibility of tracking EVs through these ID numbers. Therefore, we a security mechanisms is proposed that can reduce the security and privacy concerns without unreasonable complicated of production new tires. The suggested technique is immune to three cyber attacks using both general and systematic analyses. The attacks include false relay data, man-in-the-middle data, and monitoring. It is seen that the authentication methodology of the proposed method is cost-effective in terms of storage, computation, and communication. Finally, we present a secure blockchain-based mutual authentication for integration in the EVs network.

VIII. ACKNOWLEDGMENT

This work was supported by the Chinese National Natural Science Foundation (grant number 51977039) and The central government guiding local science and technology development project under Grant 2021L3005.

REFERENCES

[1] Jiaming Shen;Laili Wang;Jialei Zhang, "Integrated Scheduling Strategy for

Private Electric Vehicles and Electric Taxis", IEEE Transactions on Industrial Informatics, Volume: 17, Issue: 3, 2021.

[2] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in Workshop on Embedded Security in Cars, 2004.

[3] A. Wright, "Hacking cars," Communications of the ACM, vol. 54, no. 11, pp. 18–19, 2011.

[4] X. Wang;S. Garg;H. Lin;MJ. Piran;J. Hu;M. S. Hossain, "Enabling Secure Authentication in Industrial IoT With Transfer Learning Empowered Blockchain", IEEE Transactions on Industrial Informatics, Volume: 17, Issue: 11, 2021.

[5] N. -W. Lo and J. -L. Tsai, "An Efficient Conditional Privacy-Preserving Authentication Scheme for Vehicular Sensor Networks Without Pairings," in IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 5, pp. 1319-1328, May 2016, doi: 10.1109/TITS.2015.2502322.

[5] S. Guo;X. Hu;S. Guo;X. Qiu;Feng Qi, "Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System", IEEE Transactions on Industrial Informatics, Volume: 16, Issue: 3, 2020.

[6] Y M. Tashtoush; D A. Darweesh; G Husari; O A. Darwish; Y Darwish; L Bani Issa; H I. Ashqar, "Agile Approaches for Cybersecurity Systems, IoT and Intelligent Transportation", IEEE Access, vol. 10, pp. 1360 – 1375.

[7] A F M Suaib Akhter, Mohiuddin Ahmed, A F M Shahen Shah, Adnan Anwar, A S M Kayes, Ahmet Zengin, "A Blockchain-Based Authentication Protocol for Cooperative Vehicular Ad Hoc Network", Sensors (Basel). 2021 Feb 11; vol 21(4), pp. 12-73.

[8] Y Tashtoush, D Darweesh, O Karajeh, O Darwish, M Maabreh, Safa' Swedat, R Koraysh, O Almousa and N Alsaedi, "Survey on authentication and security protocols and schemes over 5G networks", International Journal of Distributed Sensor Networks, Vol. 18(10), 2022, pp. 132-147.

[9] A. Subrahmannian and S. K. Behera, "Chipless RFID: A Unique Technology for Mankind," in IEEE Journal of Radio Frequency Identification, vol. 6, pp. 151-163, 2022, doi: 10.1109/JRFID.2022.3146902.

[10] BALANIS, C., AND IOANNIDES, P. Introduction to smart antennas. Synthesis Lectures on Antennas 2, 1 (2007), 1175.

[11] KOSCHER, K., JUELS, A., BRAJKOVIC, V., AND KOHNO, T. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond. In Proceedings of the 16th AC conferences on Computer and communications security (2009), pp. 33 42.

[12] S. Chabbi and C. Araar, "RFID and NFC authentication protocol for securing a payment transaction," 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS), 2022, pp. 1-8, doi: 10.1109/PAIS56586.2022.9946661.

[13] SAPONAS, T. S., LESTER, J., HARTUNG, C., AGARWAL, S., AND KOHNO, T. Devices that tell on you: privacy trends in consumer ubiquitous computing. In Proceedings of USENIX Security Symposium (2007), USENIX Association, pp. 1–16.

[14] DENNING, T., MATUSZEK, C., KOSCHER, K., SMITH, J. R., AND KOHNO, T. A spotlight on security and privacy risks with future household robots: attacks and lessons. In Ubicomp '09: Proceedings of the 11th international conference on Ubiquitous computing (2009), pp. 105–114.

[15] HALPERIN, D., HEYDT-BENJAMIN, T. S., RANSFORD, B., CLARK, S. S., DEFEND, B., MORGAN, W., FU, K., KOHNO, T., AND MAISEL, W. H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of IEEE Symposium on Security and Privacy (2008), IEEE Computer Society, pp. 129–142.

[15] NARTEN, T., DRAVES, R., AND KRISHNAN, S. RFC 4941 - privacy extensions for stateless address auto configuration in IPv6 Sept 2007.

[16] Y. -D. Yao, X. Li, Y. -P. Cui, J. -J. Wang and C. Wang, "Energy-Efficient Routing Protocol Based on Multi-Threshold Segmentation in Wireless Sensors Networks for Precision Agriculture," in IEEE Sensors Journal, vol. 22, no. 7, pp. 6216-6231, 1 April1, 2022, doi: 10.1109/JSEN.2022.3150770.

[17] Kim M, Park K, Yu S, Lee J, Park Y, Lee SW, Chung B. A Secure Charging System for Electric Vehicles Based on Blockchain. Sensors (Basel). 2019 Jul 9;19(13):3028.

[18] R. Eletreby and O. Yağan, "Connectivity of Wireless Sensor Networks Secured by Heterogeneous Key Predistribution Under an On/Off Channel Model," in IEEE Transactions on Control of Network Systems, vol. 6, no. 1, pp. 225-235, March 2019, doi: 10.1109/TCNS.2018.2808141.

[19] Perrig, A., Canetti, R., Tygar, J. D., and Song, D. The tesla broadcast authentication protocol.

[20] Gruteser, M., and Grunwald, D. A methodological assessment of location privacy risks in wireless hotspot networks. In Security in Pervasive Computing, First International Conference (2003), pp. 10{24.

[21] Jiang, T., Wang, H. J., and Hu, Y.-C. Preserving location privacy in wireless lans. In MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services (2007), ACM, pp. 246{257.

[22] Greenstein, B., McCoy, D., Pang, J., Kohno, T., Seshan, S., an Wetherall, D. Improving wireless privacy with an identifier-free link layer protocol. In Proceeding of Mobile systems, applications, and services (MobiSys) (2008), ACM, pp. 40{53.

[23] Lee, C.-H., Hwang, M.-S., and Yang, W.-P. Enhanced privacy and authentication for the global system for mobile communications. Wireless Networks 5, 4 (1999), 231-243.

[24] S. Nakamoto, ``Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: http://satoshinakamoto.me/2008/11/01/bitcoin-p2pe- cash-paper/ and http://www.bitcoin.org/bitcoin.pdf

[25] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," IEEE Access, vol. 4, pp. 22922303, 2016.

[26] A. Dua, N. Kumar, A. K. Das, andW. Susilo, ``Secure message communication protocol among vehicles in smart city," IEEE Trans. Veh. Technol.,vol. 67, no. 5, pp. 43594373, May 2018.

[27] V. Odelu, A. K. Das, K.-K. R. Choo, N. Kumar, and Y. Park, ``Efficient and secure time-key based single sign-on authentication for mobile devices," IEEE Access, vol. 5, pp. 2770727721, 2017.

[28] Sattar Shojaeiyan, Taher Niknam, Mehdi Nafar, "A novel bio-inspired stochastic framework to solve energy management problem in hybrid AC-DC microgrids with uncertainty", International Journal of Bio-Inspired Computation, vol. 18, no. 3, pp. 165-175, 2021.

Pouyan Razmjouei received a B.S degree in Electronic Engineering from Azad university Fars, Iran, in 2009; the M.S degree in Control Engineering from Azad university Garmsar, Iran, in 2014; He is currently an automotive instructor in vocational and technical school from 2015 to 2020. His current research interests include automotive security, automotive embedded and software developer, and application of machine learning in the field of electric vehicles (EVs) and battery technology.

Abdollah Kavousi-Fard (SM'19) Prof. Kavousi-Fard (M'15, SM'19) is Associate Professor of Electrical Engineering and AI at Shiraz University of Technology. He is the director of the AI in electrical systems laboratory in SUTech since 2022. He was a Postdoctoral Researcher at the University of Michigan, Mi, USA in 2016-2018. Dr. Kavousi-Fard was a researcher with the University of Denver, Denver, Colorado, USA in 2015-2016 conducting research on renewable energy sources and their impacts on the human society. He has been honored to the 1% highly-cited scientists in the world in 2019-2022 based on the SCI reports. Dr Kavousi-Fard has been a key figure in the development of renewable energy in the South of Iran, leading several research projects in the area. He has published more than 140 papers on AI application in renewable energy and green policy making in international journals and has presented his research at a number of conferences and symposia. He has also been involved in a number of initiatives to promote the use of renewable energy in Iran, including the establishment of the first renewable energy park in the country. He has also been a key figure in the development of policies and regulations to support the growth of renewable energy in Iran. Dr Kavousi-Fard has been recognized for his work in the field of renewable energy and AI in power system, receiving several awards and honors, including the Best Paper Award in 2013 in Renewable Energy Journal and 2014 in Energy Journal. He is also a Senior Member of IEEE. Dr. Kavousi-Fard is an Editor in IEEE Transactions on Industrial Applications and also in Springer, ISTE journal. He has served as the GE in several SIs including the IEEE Transactions on Industrial Informatics, IEEE Transactions on Intelligent Transportation Systems, IET GTD Journal, IET RPG Journal, IJEPES Journal, and *Sustainable Cities and Society* Journal. His current research interests include advanced machine learning, artificial intelligence, cyber security of power system, operation and management of power system, strategic decision making for sustainable development of society, microgrid, smart city, electric vehicles as well as the regulation policy making in the public management.

Tao Jin (FIET, SMIEEE) received B.S. and M.S. degrees in electrical engineering from Yanshan University, Qinhuangdao, China, in 1998 and 2001, respectively, and the Ph.D. degree in electrical engineering from Shanghai Jiaotong University, Shanghai, China, in 2005. From 2005 to 2007, he worked as a post-doctor with Shanghai Jiaotong University. From 2008 to 2009, he held research scientist position with Virginia Tech, Blacksburg, VA, USA. In 2010, he joined Imperial College London, London, U.K., as European Union Marie Curie Research Fellow, where he focused on electrical technologies related to smart grid. He is currently a Professor with the College of Electrical Engineering and Automation, Fuzhou University, Fuzhou, China. He has authored about 200 articles. Dr. Jin is a member of the IEEE Power and Energy Society and the IEEE Industrial Electronics Society, and a Special Committee Member of the Chinese Society of Electrical Engineering and the China Electrotechnical Society. He currently serves as Co-Editor-in-Chief of ESTA, and Associate Editorsfor MPCE, PCMP, China Measurement and Testing Technology, and other journals.

Morteza Dabbaghjamanesh (SM'19) received the M.Sc. degree in electrical engineering from Northern Illinois University, DeKalb, IL, USA, in 2014, and the Ph.D. degree in electrical and computer engineering form Louisiana State University, Baton Rouge, LA, USA in 2019. Currently, he is a Senior R&D Engineer at the Electric Reliability Council of Texas (ERCOT), Austin, TX, USA. Before joining ERCOT, he was R&D and research policy engineer at Midcontinent Independent System Operator (MISO) Energy. Dr. Dabbaghjamanesh serve/served as associate editor in multiple journals including IEEE Transactions on Smart Grids, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Industrial Informatics, International Journal of Electrical Power & Energy Systems, Solar Energy Journal, and Sustainable Cities and Society. His current research interests include reliability, resiliency, renewable energy sources, cybersecurity analysis, big data, machine/deep learning, smart grids, and microgrids.

MAZAHER KARIMI (Senior Member, IEEE) received the Ph.D. degree in electrical energy and power system from the University of Malaya, Kuala Lumpur, Malaysia, in 2013. He has worked as a Research Associate with The University of Manchester, from 2016 to 2017. From 2017 to 2020, he was an Assistant Professor at Gonbad Kavous University, Iran. He is currently an Assistant Professor with the School of Technology and Innovations, University of Vaasa, Vaasa, Finland. His current research interests include smart grid applications, widearea monitoring, protection, and control, distributed generation, and power system stability.

Alireza Jolfaei is an Associate Professor of Cybersecurity and Networking at Flinders University. He received his PhD degree in applied cryptography from Griffith University. His research background is in cyber-physical systems security. He received the IEEE Australian council award for his research in the design of a geometric crypto primitive, published in the IEEE Transactions on Information Forensics and Security. He provides industry consultations and offers proof-of-concept pen-testing on industrial automation and control systems, an example of which is his recent work on the security of water quality management systems under a Defence pre-accelerator program named D.Start, which also received an international award from the Sydney Water Innovation, the Smart City Shark Tank. Dr Jolfaei provides leadership through IEEE publications, standards and educational activities as the Chair of the Security and Privacy Technical Committee of the IEEE Consumer Technology Society and as the Editor-in-Chief of the IEEE Consumer Technology Society's World eZine.