Al-Rafidain Engineering Journal (AREJ) Vol. 29, No. 2, September 2024, pp. 86-98

Implementation of a Resilient Complementary Code Keying (CCK) modulation for Autonomous Vehicle (AV)

Zeina Ali M.* zinah.mohammed@uoninevah.edu.iq

Qutaiba I. Ali ** qut1974@gmail.com

* Computer and Information Engineering Department, College of Electronics Engineering, Ninevah University, Mosul, Iraq

** Computer Engineering Department, College of Engineering, University of Mosul, Mosul, Iraq

Received: Febuary 6th, 2024 Received in revised form: March 4th, 2024 Accepted: March 22th, 2024

ABSTRACT

In the realm of wireless communication, ensuring end-to-end privacy remains a critical concern in real-time applications like Autonomous Vehicles (AVs). The existing wireless protocols often need to be revised to address these privacy challenges effectively, especially when sensitive data transmission is involved. To tackle this challenge, this paper proposes a unique solution tailored to the specific requirements of each AV through the establishment of individual wireless network domains. To bolster privacy and security, a new approach called resilient modulation is introduced. This method involves integrating the Vehicle Identification Number (VIN) into the Complementary Code Keying (CCK) equation within the 802.11b network. Additionally, the proposed enhancement extends to the Wireless Controller Area Network (CAN) bus, introducing an added layer of security. Furthermore, modifications are made to the conventional CCK modulation scheme to accommodate the proposed enhancement seamlessly. By adjusting the phase angles of transmitted signals, the integrity of the CCK modulation scheme is maintained, preserving orthogonality and correlation that are crucial for effective communication. Through rigorous experimentation and analysis, The results showed that the Bit Error Rate (BER) and packet loss of the receiver Electronic Control Unit (ECU) were stable between different CCK modifications. This indicates the robustness of the basic features of CCK modification and that the extent of modifications does not affect the CCK modification scheme with respect to orthogonality and correlation properties. On the contrary, there is a significant challenge in intercepting and decoding the signal by the eavesdropping ECU, which has shown packet loss ranging from 63% to 100% across different CCK states.

Keywords:

Complementary Code Keying (CCK) modulation, Autonomous Vehicle (AV) , Controller Area Network (CAN), Vehicle Identification Number (VIN).

https://rengj.mosuljournals.com

Email: alrafidain_engjournal2@uomosul.edu.iq

==========

1. INTRODUCTION

Advanced Driver Assistance Systems (ADAS) are becoming more common in both research and commercial vehicles, which is a big step toward AVs. These technologies are meant to cut down on accidents and their severity, make it easier for disabled and older people to move around, lower pollution, and make better use of infrastructure. According to a review by the National Highway Traffic Safety Administration (NHTSA), human-related errors like distraction, fatigue, and emotional driving cause about 94% of accidents. One of the main reasons for the fast development of AV technologies is that they do not have these problems.[1]

As the world's research, testing, and use of AVs grows, the creation of standardized rules and guidelines has become very important to ensure their safe integration into society. Recently, the U.S. Department of Transportation and the NHTSA agreed to follow the international standard for automation levels set by the Society of Automotive Engineers (SAE). It has classified automated vehicles into six levels [2]. Level 0 represents vehicles where the driver has complete control, while Level 5 signifies vehicles that have complete control over all driving functions. At present, levels 2 and 3 are indeed being implemented in certain commercial vehicles, such as Tesla's Autopilot [3]. AVs incorporate advanced

features such as automatic braking, adaptive cruise control, and lane-keeping assist systems.

While there may be slight variations among different vehicle systems, they all must address the issue of autonomous navigation, which can be broadly categorized into four key components: perception, localization and mapping, path planning, and control. Perception involves the utilization of a set of sensors installed on the vehicle to detect, understand, and interpret the surrounding environment. This includes identifying both stationary and moving obstacles, such as other vehicles, pedestrians, traffic signals, road signs, and curbs. The objective of localization and mapping tasks is to precisely determine the global position of the vehicle in relation to world coordinates.

During the perception stage, ECUs collect data about the vehicle's environment and transmit it to the AV's central computing unit via the intra_vehicle_network (IVN), such as the Controller Area Network (CAN) bus. During the planning and decision-making stages, the AV's computing unit employs artificial intelligence algorithms to analyze data and make decisions about the vehicle's movements. Finally, during the control stage, the AV's control system uses the IVN to carry out the planned movements by sending commands to various components such as the engine, brakes, and steering system. The IVN is critical for enabling real-time communication between these stages, allowing the AV to function safely and efficiently [4].

In addition, several studies examine the incorporation of connected vehicle technologies [5], such as vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technologies. These technologies enable the sharing of crucial information to establish an improved cooperative driving environment, as depicted in Fig. 1. This enhanced and refined collaborative perception enables vehicles to efficiently forecast the actions of crucial environmental elements (such as obstacles, roads, ego-vehicles, environment, and driver behavior) and proactively anticipate any potentially dangerous occurrences.

The Controller Area Network (CAN) bus, a pivotal component of intra-vehicle communication networks, has its roots in the early 1980s. Initially designed to meet the automotive industry's requirements at the time, the CAN bus protocol was developed during an era when vehicles were equipped with a limited number of Electronic Control Units (ECUs) that were relatively lightweight in their data processing needs. However, as technology has advanced, the CAN bus protocol now faces several challenges [6].

In contrast, Autonomous Vehicles (AVs) represent a paradigm shift in vehicular technology.

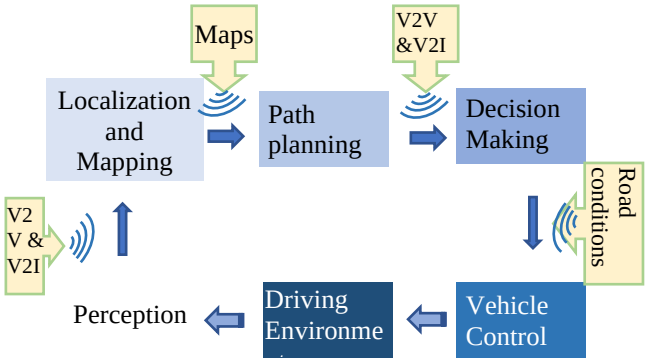

Fig. 1: Full Autonomous Navigation System. Senser Technology, Fusion Overview, V2V and V2I

AVs are computation- and networking-intensive systems, primarily due to the ever-increasing number and complexity of their ECUs, encompassing a variety of systems such as LiDAR, radar, cameras, and numerous other sensors, a number that continues to grow as more features and capabilities are added to these vehicles. This increase places a substantial demand on the vehicle's communication network, both in terms of data throughput and the complexity of managing numerous interconnected systems [7][8].

Real-time applications, such as traffic management, navigation, autonomous driving, toll collection, vehicular communication, vehicle performance review, predictive maintenance, and location-based promotion and advertising, necessitate a high data rate and bandwidth to ensure satisfactory operation and performance.

The limitations of the wired CAN bus include real-world issues, which can be summarized as follows: firstly, the spread of sensors and ECUs within the vehicle contributes to its overall complexity. Today's average vehicle can contain over 150 ECUs packed on different corners of the vehicle and round 100 million lines of code [7][9]. Secondly, the internal wiring harness has evolved into a highly composite network, adding to the complexity of the overall system. Thirdly, the choice of materials and the design considerations for the wiring layout have become increasingly sophisticated, leading to higher costs.

Additionally, the rising weight of AVs places greater demands on the driving control system, resulting in increased energy consumption. Furthermore, the utilization of wired structures for intra-vehicle communications, such as those involving steering wheel and tire components, is deemed impractical. The growing density of

components within the intra-vehicle space further accentuates the challenges. Lastly, the maintenance of these wired networks poses significant challenges, as the diagnosis and resolution of issues within the physical wiring necessitate substantial effort and resources.

Given this scenario, there is a pressing need to enhance or modify the traditional CAN bus to meet the advanced requirements of AVs. One notable solution is the move to a wireless system. As a result, a significant research challenge arises in ensuring reliability and security in a wireless environment in vehicular communication networks. The goal of this paper is to implement a hidden communication environment so that no one can listen to or detect the presence of this network. This is done by giving each AV's ECUs a unique Complementary Code Keying (CCK) modulation equation that is different from those in other AVs and from regular Wi-Fi. The effectiveness of this method will be tested using a MATLAB/SIMULINK model designed explicitly for this modified wireless enclosure.

The remainder of the content of this paper is as follows: Section 2 provides a brief overview of the IEEE 802.11b standard, while Section 3 presents the Spread Spectrum Modulator. Section 4 provides a brief review of the DQPSK modulator, while Section 5 presents the concept of CCK modulation. The research methodology is explained in Section 6. The simulation model for the modified resilient modulation and the discussion of the results are provided in Sections 7 and 8, respectively. The conclusions are finally presented in Section 9.

2. IEEE 802.11B STANDARD

The IEEE 802.11b standard offers three physical layer options: Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and Infrared. Among these, DSSS is the prevalent choice in commercial applications, primarily designed to align with the FCC regulations for operation in the 2.4GHz Industrial, Scientific, and Medical (ISM) band, a band known for its worldwide allowance for unlicensed use [10].

DSSS divides the total bandwidth into 20MHz channels. In the United States and Europe, while there are 11 available channels for DSSS, channel overlap is common. To ensure effective performance, especially when multiple Access Points (APs) are in proximity, a separation of 22MHz is recommended. Within the 83.5MHz ISM bandwidth, it is feasible to accommodate three non-overlapping channels. The IEEE 802.11b technology, embraced by most WLAN products, operates with a transmitter crafted for DSSS Phase Shift Keying (PSK) modulation, capable of data transmission speeds reaching 11Mbps. Various modulation techniques are deployed contingent on the data rate: DBPSK for 1Mbps, DQPSK for 2Mbps, and CCK for both 5.5Mbps and 11Mbps. The frame's preamble and header are invariably sent using DBPSK at 1Mbps. Conversely, the data payload may be transmitted via DBPSK, DQPSK, or CCK, depending on the chosen configuration.

Each packet transmitted within the Local Area Network (LAN) is preceded by a preamble and header that last 192 microseconds. The packet header's Signal Field specifies the type of modulation for the rest of the packet. This preamble aids the receiver in achieving initial synchronization, and the header carries vital data for establishing a physical layer connection as dictated by the communication protocol.

In compliance with FCC standards for the 2.4GHz ISM band, transmitters should operate with a nominal output of 100 milliwatts, equivalent to 20dBm. This power setting is chosen to provide adequate coverage up to a 100-meter radius while also conserving battery life.

3. SPREAD SPECTRUM MODULATOR

The modulator in the IEEE 802.11b system is capable of producing signals for DBPSK, DQPSK, and CCK spread spectrum. After the header, it can switch modulation modes for data transmission, supporting a range of 1, 2, 5.5, and 11 Mbps. All modulation types use Differential Quadra phase modulation at the baseband, with the I and Q channels unified for the 1 Mbps DBPSK mode. To diminish interference within the ISM band, spread spectrum technology is utilized, expanding the transmitted energy across a broader radio frequency spectrum, which in turn elevates the processing gain for receivers. The spreading process involves the binary data being XOR-ed with a pseudorandom binary sequence. For DBPSK and DQPSK, an 11-chip Barker sequence is employed, whereas CCK utilizes 8-chip Walsh codes [11][12].

The Signal-to-Noise Ratio (SNR) is fundamental for system analysis, indicating the energy per chip (E_c) over the noise power spectral density (N_0). SNR varies based on the chip rate, and the disparity stems from the number of bits a chip represents. N_0 is the constant power spectral density of the system's Additive White Gaussian Noise (AWGN), with a chip rate fixed at 11Mchips/s [11][12].

4. DQPSK MODULATOR

Differential Phase Shift Keying (DPSK) modulation differentiates itself from Phase Shift Keying (PSK) by not assigning a specific phase to each symbol. Instead, it detects the difference between the current phase and the previous phase, using this change in phase to indicate a change in symbol. In the simplest form of DBPSK, a phase shift of π is caused by a 1, while a 0 does not cause any phase change, or vice versa. At the receiver, the phase of each symbol is compared to the phase of the previous symbol, necessitating a one-symbol length delay in the received signal. A phase change signifies the reception of a binary digit 1, while the absence of a phase change signifies the reception of a binary digit 0 [11][12][13][14].

The IEEE 802.11b standard utilizes DPSK due to its ability to eliminate the requirement for coherent detection, which is necessary in PSK systems. In simpler terms, there is no need to estimate the carrier phase, resulting in a less complex receiver design. In terms of spectral characteristics, the DBPSK signal closely resembles a BPSK signal. However, the DBPSK signal has a processing gain advantage of 1dBm.

For DBPSK modulation, the bit error probability (P_e) in the AWGN channel is :

$$P_e = \frac{1}{2}\, exp\left(-\frac{E_b}{N_0}\right) \quad (1)$$

where E_b/N_0 is the ratio of signal energy per bit and noise density per bit.

In the case of DQPSK where M = 4, we have in effect two binary phase-modulation signals in phase quadrature and the equation is:

$$P_e = Q_1(a,b) - \frac{1}{2}\, I_0(ab) exp\left(-\frac{1}{2}(a^2+b^2)\right) \quad (2)$$

Where

$Q_1(a,b)$: Marcum Q function.

I_0(ab) :modified Bessel function of zero order.

More details about Marcum Q and the modified Bessel function can be found in [11].

The parameters a and b are defined as:

$$a = \sqrt{\frac{2E_b}{N_0}\left(1-\sqrt{\frac{1}{2}}\right)} \; and \; b = \sqrt{\frac{2E_b}{N_0}\left(1+\sqrt{\frac{1}{2}}\right)} \quad (3)$$

The 11-chip direct sequence spreading technique enhances the processing gain at the DBPSK system's receiver, calculated as 10 log(11 chips /1 bit) = 10.4 dB. In contrast, the DQPSK modulation process achieves a processing gain of 7.4 dB because it encodes 2 bits per chip. Regarding data rates, DBPSK modulation achieves 1 Megabit/second or 1 Msymbol/second , on the other hand, doubles the rate to 2 Megabits/second or 1 Msymbol/ second, with each symbol still comprising 11 chips but corresponding to two bits.

5. CCK MODULATION

The 802.11b standard utilizes a specific formula, as shown in equation 4, to derive CCK codes for transmission at a rate of 11Mbps. This formula produces a symbol by constructing 8 complex chips. This method employs a single-phase term to modulate all the chips, along with three additional phase terms to modulate different groups of chips. This approach is a more comprehensive form of the Walsh/Hadamard function, as it incorporates four phases while still maintaining an orthogonal structure [7].

$$[c0, c1, c2, c3, c4, c5, c6, c7] = \begin{bmatrix} e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)} \\ , e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)} \\ e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_4} \end{bmatrix} \quad (4)$$

where ϕi ∈ {0, π/2, π, 3π/2}. Each ci is a chip in the CCK codeword.

On the other hand, the key to CCK's efficiency is the orthogonality of the code sequences. Orthogonal codes are selected so that they do not interfere with each other when transmitted simultaneously. This characteristic allows for multiple bits to be sent in parallel, increasing the data rate. Using different code combinations, CCK can transmit at various data rates, typically 5.5 and 11 Mbps, which are the highest rates defined in the 802.11b standard. This is achieved by using 8-chip codes for 11 Mbps and 4-chip codes for 5.5 Mbps. CCK modulation is more robust to certain types of interference and multipath fading than its predecessors. This is because the spread-spectrum technique allows the receiver to recover the original data even if parts of the signal are distorted or lost [15].

The 8-bit CCK modulation splits the 8-bit stream into four 2-bit sub-streams where each sub-stream is allocated a phase as presented in Table 1. Based on the binary 2-bit sub-stream, the corresponding phase of the 2-bit sub-stream varies as shown in Table 2. The four phases associated with the 8-bit sequence are formulated in the matrix shown in equation 5 which clearly demonstrates how the elements of equation 4 are constructed [15].

$$M2 = \begin{bmatrix} \phi_1 & \phi_1 & \phi_1 & \phi_1 & \phi_1 & \phi_1 & \phi_1 & \phi_1 \\ \phi_2 & 0 & \phi_2 & 0 & \phi_2 & 0 & \phi_2 & 0 \\ \phi_3 & \phi_3 & 0 & 0 & \phi_3 & \phi_3 & 0 & 0 \\ \phi_4 & \phi_4 & \phi_4 & \phi_4 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5)$$

Table 1: Sub-Stream Phase Allocation in 8-bit CCK Modulation

Bit Sequence	a_1a_0	a_3a_2	a_5a_4	a_7a_6
Phase	ϕ_1	ϕ_2	ϕ_3	ϕ_4

Table 2: Numerical Phase Allocation in CCK Modulation

$\mathbf{a_{k+1}\ a_k}$	00	01	10	11
Phase	0	π	$\pi/2$	$-\pi/2$

Table 3: 8 bit CCK Modulation

8-bit binary data stream	0 0 1 1 1 0 1 1
2-bit sub stream	0 0, 1 1, 1 0, 1 1
Phase assignment	0, -π/2, π/2, -π/2
8 bits CCK codewords	-i , 1, -1, i, 1, i, i, 1

Inspection demonstrates that each of its elements is indeed an exponent that is powered to the sum of the phases forming columns of the matrix given in equation 4. The minus sign of the fourth and seventh elements follows the rule discussed in the generation of complementary sequences. The 8-bit CCK modulated codewords are shown in Table 3. The 8-bit CCK modulation generates 256 different codewords, whereas 64 codewords are distinctively orthogonal. This orthogonality property results in low cross-correlation and, consequently, efficient interference mitigation [16].

Fig. 2 illustrates the process of generating an 11 Mbps CCK signal, which is part of the 802.11b Wi-Fi standard [17][18]. The diagram shows the signal generation pathway for a single data packet as it is prepared for transmission over the I (In-phase) and Q (Quadrature) channels, the components are illustrated as:

1. Data Splitter: The input consists of 8 bits of data that are first split by the data splitter. Six of these bits are used to select one of the 64 CCK codes, and the remaining two bits are used for DQPSK modulation.
2. CCK Code Selection: The 6 bits from the splitter are used to choose one of the 64 unique CCK codes. Each CCK code represents a different combination of phase shifts and is used to encode the 6 bits into a symbol for transmission.
3. XOR with I and Q: The two remaining bits from the data splitter are XORed (exclusive ORed) with the in-phase (I) and quadrature (Q) components from the previous symbol's output. The I and Q components represent two orthogonal signal paths that allow for the simultaneous transmission of two bits per symbol in DQPSK modulation.
4. DQPSK Modulators: The output from the XOR operations is then fed into two DQPSK modulators, one for each of the two remaining bits. DQPSK is a phase modulation scheme that conveys data by changing the phase of the carrier wave.
5. Phase Shift: The DQPSK modulated signals are then phase-shifted, with one of them (for the Q channel) being shifted by (-pi/4) radians to ensure orthogonality between the I and Q channels.
6. Combination: The phase-shifted signals from the I and Q channels are then combined (denoted by the Σ symbol) to form the final CCK signal ready for transmission.

6. RESEARCH METHODOLOGY

Within the structure of the research methodology, there are two distinct sections: the first section pertains to the experimental setup, while the second section focuses on the numerical setup. The experimental setup involves the utilization of MATLAB to simulate work and the utilization of a ready-made model. This model consists of three ECUs: a transmitting ECU and a receiving ECU, which are modulated using the modified CCK equation. The third ECU (the eavesdropping ECU) is modulated using

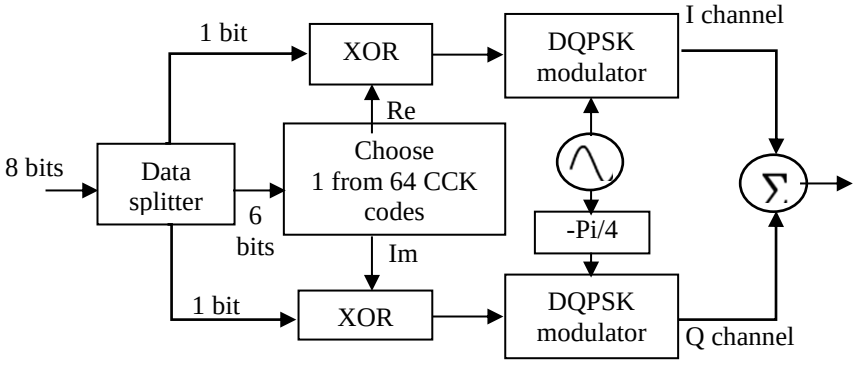

Fig.2 : 11 Mbps CCK Generation.

conventional CCK. The transmission specifications are outlined in Table 4. The numerical configuration involves integrating one of the modified modulation CCK equations with the VIN for both the transmitting and receiving nodes. The eavesdropping node, on the other hand, was modulated using the traditional CCK mentioned in Equation 4. The performance evaluation included measuring the Bit Error Rate (BER) and packet loss, as well as analyzing the signal specifications of the nodes during transmission. Next, we implement seven modification cases to the conventional equation and incorporate all equations within the transmitting and receiving nodes while still using the traditional CCK equation for the eavesdropping node. We then assess each case again.

Table 4:- Transmission Specification

Parameter	**Value**
Transmission Data Rate	11 Mbps
Transmission Technique	DSSS
Channel Bandwidth	22 MHz
Packet Size	8 Byte
Number of ECUs	3
Modulation Technique	Barker Sequence and CCK

7. THE MODIFIED RESILIENT MODULATION SIMULATION MODEL

Fig. 3 outlines a MATLAB Simulink of the modified IEEE 802.11b in terms of resilient modulation. The model is structured into segments: model parameters, channel, scope display, packet loss, and BER calculation. The Model Parameters section allows for customization of WLAN simulation parameters, such as data rate, packet size, and channel noise levels. The Channel section allows users to choose different levels of corruption generated by the channel, altering the SNR to alter the noise level. In addition, there are three ECUs. The transmitter's ECU encodes CAN data into 802.11b frames using a modified CCK modulator. The receiver ECU uses a modified CCK demodulator, while the eavesdropping ECU uses a traditional CCK demodulator.

The Wi-Fi network specifications are outlined in Table 4. The evaluation of communication systems is based on three key performance metrics: Frame Error Rate (BER) Measurement, Frame Error Rate (FER) or packet loss analysis, and Signal Characterization.

The 802.11 standard uses only three channels, 1, 6, and 11, due to their non-interfering nature. This results in a drop in 802.11b link throughput due to channel interference. However, numerous research articles [19,20,21,22,23,24] have explored modified CCK techniques to improve wireless networks' reliability, efficiency, and security.

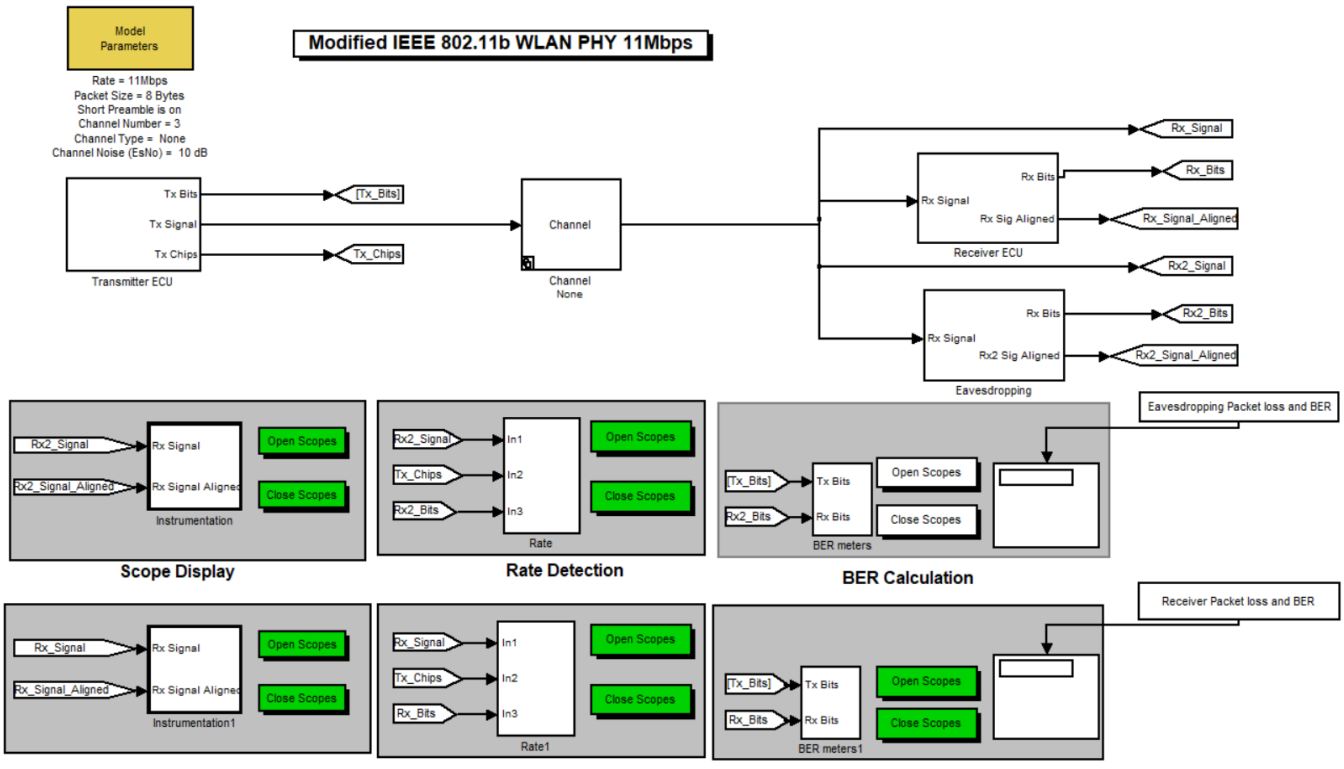

Fig. 3 :- MATLAB Simulink of Modified IEEE 802.11b in terms of Resilient Modulation

One such approach is the use of distinct and nearly orthogonal code sets for CCK modulation in neighboring Basic Service Sets. This reduces co-channel interference between Basic Service Sets [19]. Another research direction focuses on reducing the complexity of the decoder for CCK modulation by mapping complex chips to modulo-4 numbers and decomposing coded words by in-dependent angle parameters based on their properties [20]. A novel spatial block coding scheme has been proposed to exploit spatial diversity and code diversity against doubly selective fading channels. This method utilizes multiple transmit transducers and extends the traditional CCK code set to improve receiver performance [21].

The authors of [22] improved the communications reliability of CCK in IEEE 802.11b systems by proposing an overlay signaling dimension that preserves WiFi signals' underlying data rate and power spectrum characteristics. Additionally, research has been conducted to modify the code to adapt the wireless link to bandwidth by increasing the bandwidth efficiency of CCK signaling.

The study aims to create a hidden communication environment by modifying the standard CCK modulation equation with customizable parameters for each AV. These parameters include randomization to further obscure transmission and make it harder to detect and analyze. VINs, which serve as exclusive vehicle identifiers, are used to highlight a vehicle's manufacturer, specifications, and features, making them a reliable source of data in vehicle systems [25,26].

In Fig. 4, we present an intricate simulation model of transmission within an ECU. The main components of this modified CCK modulator are illustrates in Fig. 5 while Fig. 6 show the CCK modulator components.

This new approach combines modified CCK modulation techniques with the application of VINs, enhancing privacy within 802.11b networks and addressing the growing demand for confidential wireless data transmission in vehicular applications. The modified CCK adds an additional layer of privacy to the proposed wireless CAN (WCAN) bus. Fig. 7 shows the Generation Module of the modified CCK.

The flowchart in fig. 8 outlines the simulation steps for a modified CCK setup within a simulated 802.11b network environment within two scenarios. In the first scenario, the process begins with initializing the network environment, setting up transmitter and receiver ECUs using a modified CCK equation. A listener ECU is also set up using the traditional CCK equation. Network

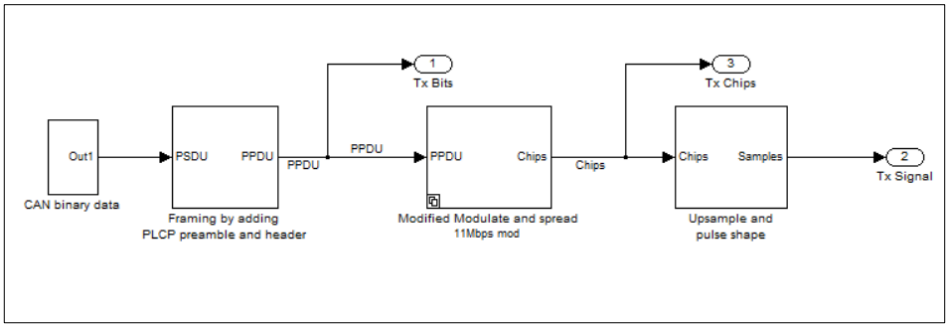

Fig. 4 :- Transmission ECU Components

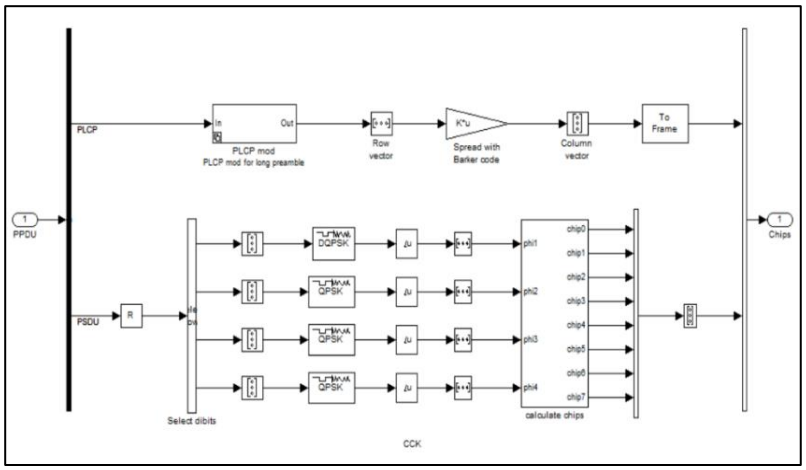

Fig. 5 :- Modulator Components of Transmiter ECU

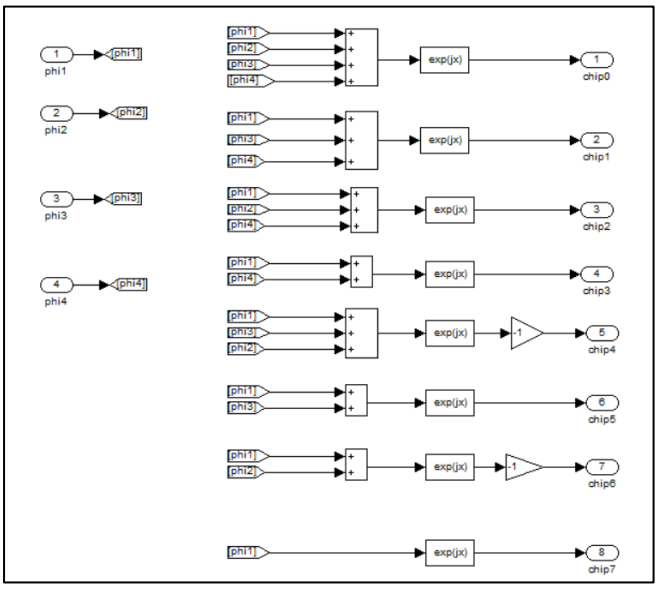

Fig. 6 :- CCK Chips Modulator Components

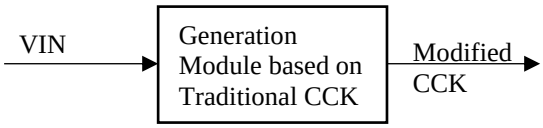

Fig. 7: Modified CCK Generation Module

performance is measured using metrics such as BER and packet loss over time. In the second scenario, modifications to the traditional CCK modulation scheme are made, including changes to the phase angles of transmitted signals. This simulation exercise demonstrates that the extent of modifications does not affect the orthogonality and correlation properties necessary for effective communication. Table 5 shows the various CCK modification cases. Performance metrics (BER and packet loss) are then repeated to ensure the modified system's performance is maintained or improved.

7.1 First Scenario Results

At 14 dB SNR levels, the transmitting ECU produced an original signal with clear binary transitions, which the receiving ECU replicated accurately. The eavesdropping ECU's inability to properly decode the signal resulted in a persistently high packet loss, ensuring data security against

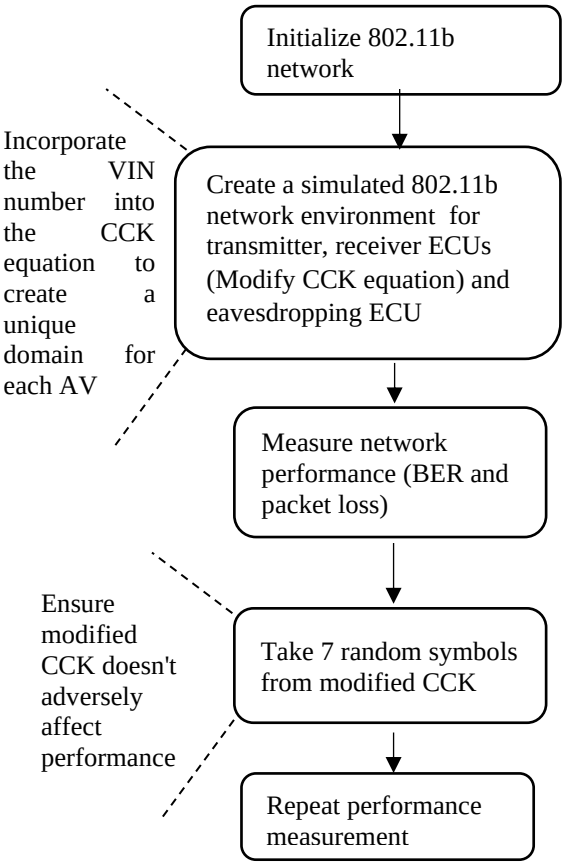

Fig. 8: Resilient Modulation Simulation Flowchart

unauthorized access. In the SNR at 12 dB and 10 dB, slight signal degradation appeared, introducing minor distortions in amplitude and shape on the receiving ECU's end. Despite this, the eavesdropping ECU's packet loss remained at 1, attesting to the durability of the system's security measures.

Challenges were more posed at lower SNR levels, where noise significantly marred the signal at 9 dB and 8 dB, increasing error susceptibility. The receiving ECU faced heightened distortion and elevated BER,

Table 5: Various CCK Modification Cases

Case number	CCK equation
Case_1	$C=\{e^{j(\pi+\pi/2+\pi)}, e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, -e^{j(\pi+\pi/2)}, e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, -e^{j(\pi+\pi)}, e^{j\pi}\}$
Case_2	$C=\{-e^{j(\pi+\pi/2+\pi)}, e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, -e^{j(\pi+\pi/2)}, e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, -e^{j(\pi+\pi)}, e^{j\pi}\}$
Case_3	$C=\{-e^{j(\pi+\pi/2+\pi)}, -e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, -e^{j(\pi+\pi/2)}, e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, -e^{j(\pi+\pi)}, e^{j\pi}\}$
Case_4	$C=\{e^{j(\pi+\pi/2+\pi)}, e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, e^{j(\pi+\pi/2)}, -e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, -e^{j(\pi+\pi)}, e^{j\pi}\}$
Case_5	$C=\{e^{j(\pi+\pi/2+\pi)}, -e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, -e^{j(\pi+\pi/2)}, -e^{j(\pi+\pi-\pi/2)}, -e^{j(\pi-\pi/2)}, e^{j(\pi+\pi)}, e^{j\pi}\}$
Case_6	$C=\{-e^{j(\pi+\pi/2+\pi)}, -e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, e^{j(\pi+\pi/2)}, -e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, e^{j(\pi+\pi)}, -e^{j\pi}\}$
Case_7	$C=\{-e^{j(\pi+\pi/2+\pi)}, e^{j(\pi-\pi/2+\pi/2)}, e^{j(\pi+\pi+\pi/2)}, e^{j(\pi+\pi/2)}, -e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, e^{j(\pi+\pi)}, -e^{j\pi}\}$
Case_8	$C=\{-e^{j(\pi+\pi/2+\pi)}, -e^{j(\pi-\pi/2+\pi/2)}, -e^{j(\pi+\pi+\pi/2)}, e^{j(\pi+\pi/2)}, -e^{j(\pi+\pi-\pi/2)}, e^{j(\pi-\pi/2)}, -e^{j(\pi+\pi)}, -e^{j\pi}\}$

particularly when handling the larger 64-byte payload. Despite these challenges, the eavesdropping ECU's packet loss continued to hold at 1, underscoring the maintained security efficacy under various SNR conditions. Across all levels, the BER and packet loss metrics for the receiving ECU escalated inversely with SNR, with lower SNR leading to higher noise and higher bit and frame errors. Conversely, the eavesdropping ECU's BER remained elevated, and packet loss consistently hit the maximum, confirming the robustness of the communication system's security against interception attempts. Table 6 and Table 7 present the BER and packet loss values.

In Fig. 9, at 10 dB SNR with an 8-byte payload, the transmitting ECU generated an original signal with binary shifts, which the receiving ECU accurately replicated with a BER of 0.0001932, demonstrating the effectiveness of the demodulation and decoding processes. On the other hand, the BER of the eavesdropping ECU was 0.2251, indicating the ability to decode the signal correctly and thus continuously lose the packet by 1, thereby protecting the data from unauthorized access.

7.2 Second Scenario Results

The BER and packet loss statistics are presented in Table 8 and Table 9 respectively. The simulation will be controlled, with SNR standardized at 12 dB across all experimental runs. This consistency is essential to ensuring that CCK modulation changes are responsible for observed variations and not environmental factors.

Table 3 shows that each case_2 through case_8 is a unique iteration of the CCK scheme, deviating incrementally from case_1. Performance indicators like BER, packet loss, and transmitted and received signals will be monitored. This simulation exercise shows that CCK modulation scheme modifications do not affect orthogonality

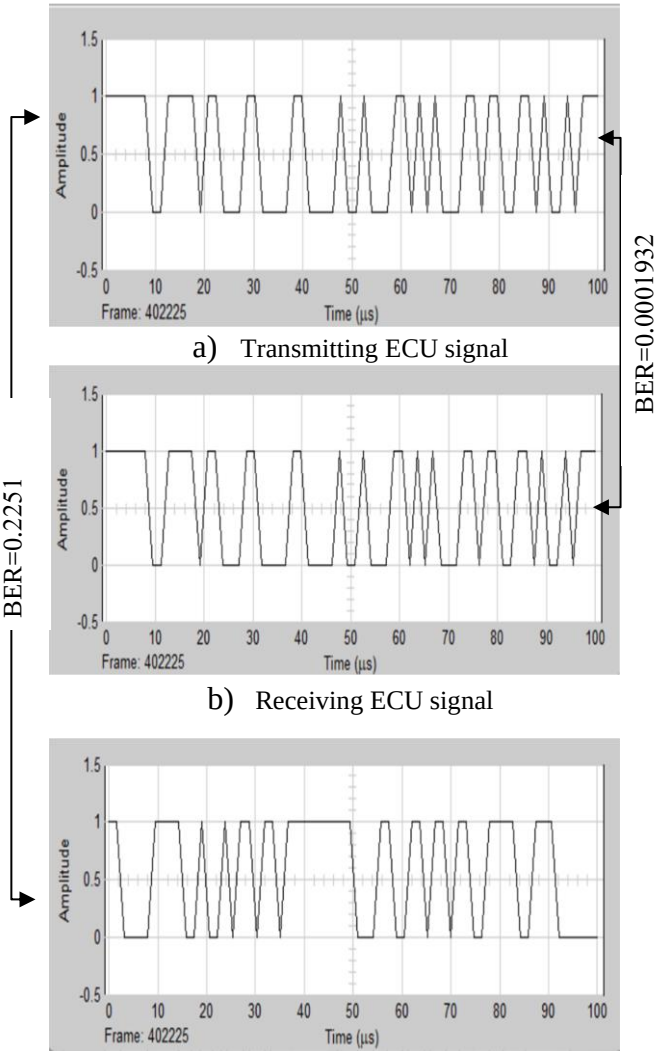

Fig. 9: Transmit, Receive and Eavesdropping Signals when SNR=10

Table 6 : BER of Receiving and Eavesdropping ECU

SNR	BER of Receiving ECU		BER of eavesdropping ECU	
	8 bytes	64 bytes	8 bytes	64 bytes
None	0	0	0.2275	0.5294
8	0.002281	0.005414	0.2188	0.5102
9	0.000733	0.001749	0.2225	0.5188
10	0.000193	0.000459	0.2251	0.5248
12	0	5.86e-006	0.2275	0.5303
14	0	0	0.2281	0.5314

Table 7 : Packet Loss of Receiving and Eavesdropping

SNR	packet loss of Receiving ECU		packet loss of eavesdropping ECU	
	8 bytes	64 bytes	8 bytes	64 bytes
None	0	0	1	1
8	0.1339	0.6741	1	1
9	0.0447	0.3104	1	1
10	0.01191	0.0921	1	1
12	0	0.001426	1	1
14	0	0	1	1

Table 8 : BER of Receiving and Eavesdropping ECU with Various Modification Cases

SNR	BER of Receiving ECU		BER of eavesdropping ECU	
	8 bytes	64 bytes	8 bytes	64 bytes
Case_1	5.534e-007	1.58e-005	5.634e-007	1.58e-005
Case_2	1.66e-006	1.399e-005	0.03746	0.0643
Case_3	3.321e-006	1.512e-005	0.1627	0.3796
Case_4	0	5.867e-008	0.2275	0.5303
Case_5	0	1.151e-005	0.1473	0.3432
Case_6	2.214e-006	7.672e-008	0.1477	0.3438
Case_7	0	1.444e-005	0.1035	0.2416
Case_8	6.088e-006	6.544e-006	0.2405	0.0568

Table 9 : FER of Receiving and Eavesdropping ECU with Various Modification Cases

SNR	packet loss of Receiving ECU		packet loss of eavesdropping ECU	
	8 bytes	64 bytes	8 bytes	64 bytes
Case_1	0.0001018	0.002851	0.0001018	0.002851
Case_2	0.0001018	0.002568	0.0001018	0.002568
Case_3	0.0003056	0.002668	0.0003056	0.002668
Case_4	0	0.001426	0	0.001426
Case_5	0	0.002709	0	0.002709
Case_6	0.0002037	0.001688	0.0002037	0.001688
Case_7	0	0.002994	0	0.002994
Case_8	0.0004073	0.001688	0.0004073	0.001688

and correlation, which are necessary for communication efficacy.

The eavesdropper and receiver in case_1 use the traditional CCK equation. The receiving ECU's BER and packet loss are extremely low, indicating that it is precisely decoding the transmitted signals. This is expected since the conventional CCK is designed for reliability and high signal decoding fidelity. Since the eavesdropper's BER and packet loss values are identical to the receiver's in Case 1, it can intercept and decode communications as efficiently as the intended receiver using the same decoding scheme. This control case confirms the expected performance of the standard CCK modulation without changes.

In Fig. 10, at case_5 with an 8-byte payload in Table 4, the transmitting ECU generated an original signal with binary shifts, which the receiving ECU accurately replicated with a BER of 0, demonstrating the effectiveness of the demodulation and decoding processes. On the other hand, the BER of the eavesdropping ECU was 0.1573, indicating the ability to decode the signal correctly and thus continuously lose the packet by 1.

The eavesdropping ECU faces significant signal interception and decoding challenges due to the high BER and packet loss that persists across CCK cases (from cases 2 to 8). This consistent challenge implies that the modified CCK schemes maintain communication security without amplifying the eavesdropper's decoding errors. The consistent error rates suggest that these modifications, while not improving security, maintain the legitimate communication channel.

CCK modulation's core attributes are robust because BER and packet loss remain stable during CCK adjustments. Orthogonality and correlation are essential for effective communication and are unaffected by the variables or parameters of the tests. This confirms that CCK modifications can secure vehicular communications without compromising performance.

8. RESULT DISCUSSION

We proposed implementing a hidden communication environment for each vehicle by introducing a unique modification for the CCK of the operating ECUs to be included in the vehicle contract modulator. The effectiveness of this method was tested using a MATLAB model in a configured simulation environment with three nodes, one AV ECU sends, another receives, and another eavesdrops, trying to penetrate the AV's wireless network while setting the SNR from 8 dB to 14 dB, the payload is specified as a simulated CAN bus at 8 and 64 byte.

The results demonstrated the integrity of the data sent between the two AV ECUs. Regarding eavesdropping, the BER reached 50% for a 64-byte payload and 22% for an 8-byte payload, resulting in 100% packet loss. Seven cases were taken to ensure that this proposed resilient modification does not affect the signal characteristics regarding orthogonality and correlation, and the SNR was set to 12 dB for all cases. The results showed that a secure connection was maintained. Between the sending and receiving vehicle's ECUs, the packet loss of the eavesdropping node ranged from 63% to 100%, thus creating a hidden communication

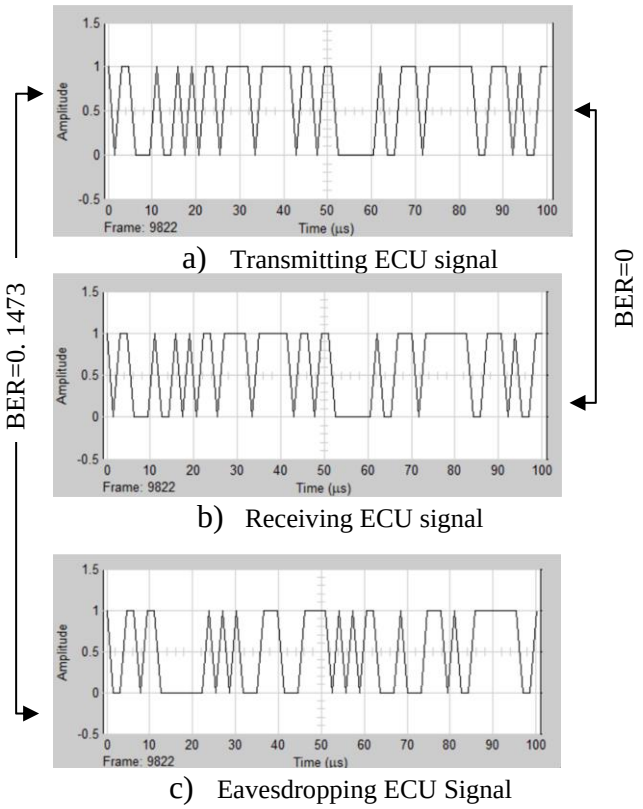

Fig. 10: Signals in case_5

environment for each vehicle.

9. CONCLUSION

Transmission security is crucial in wireless transmission, protecting data from eavesdropping and decryption. Despite the fact that spread spectrum communication provides security, transmission interception risks persist. This paper presents a resilient modulation technique that incorporates VINs into the CCK equation. The results showed the integrity of the data sent between the AV ECUs, with 100% packet loss due to the eavesdropping ECU. In addition to ensuring orthogonality and correlation are not affected by modifications, other modified CCK were implemented and the result was, the packet

loss of the eavesdropping node ranged from 63% to 100%, creating a hidden communication environment for each vehicle. This type of resilient modulation is considered a better choice for future secure wireless transmission technology. In future research, we recommend combining the modified CCK with encryption algorithms like AES or RSA to enhance data security.

REFERENCES

[1] J. Van Brummelen, M. O'Brien, D. Gruyer, & H. Najjaran, "Autonomous vehicle perception: The technology of today and tomorrow". *Transportation research part C: emerging technologies*, vol. 89, no. pp. 384-406, 2018. https://doi.org/10.1016/j.trc.2018.02.012

[2] SAE International. "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," *SAE Int*. 4970, no. 724 (2018): 1-5. [online]. Available: https://www.sae.org/standards/content/j3016_202104/

[3] Autopilot. [online]. Available: https://www.tesla.com/autopilot

[4] G. Bathla, K. Bhadane, R. Kumar Singh, R. Kumar, R. Aluvalu, R. Krishnamurthi, A. Kumar, R. N. Thakur, and S. Basheer, "Autonomous vehicles and intelligent automation: Applications, challenges, and opportunities," *Mobile Information Systems*, Vol. 2022, no. 1, 2022 (2022). https://doi.org/10.1155/2022/7632892

[5] S. Kaviani, M. O'Brien, J. Van Brummelen, H. Najjaran and D. Michelson, "INS/GPS localization for reliable cooperative driving," *In 2016 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Vancouver, BC, Canad, pp. 1-4. IEEE, 2016. https://doi.org/10.1109/CCECE.2016.7726750

[6] M. Bozdal, M. Samie and I. Jennions, "A survey on can bus protocol: Attacks, challenges, and potential solutions," *2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)*. Southend, UK, 2018, pp. 201-205. https://doi.org/10.1109/iCCECOME.2018.8658720

[7] B. Leigh, and R. Duwe, "Designing autonomous vehicles for a future of unknowns," *ATZelectronics worldwide*, Vol. 16, pp.44-47, (2021): https://doi.org/10.1007/s38314-020-0578-3

[8] R. Sharma, "Big data for autonomous vehicles," *Deep Learning and Big Data for Intelligent Transportation: Enabling Technologies and Future Trends*, pp. 21-47, (2021): https://doi.org/10.1007/978-3-030-65661-4_2

[9] M. Rumez, D. Grimm, R. Kriesten and E. Sax, "An overview of automotive service-oriented architectures and implications for security countermeasures," *IEEE access*, Vol. 8, pp. 221852-221870, (2020): https://doi.org/10.1109/ACCESS.2020.3043070

[10] Hartwich, Florian. "CAN with flexible data-rate." In Proc. iCC, pp. 1-9. Citeseer, 2012.

[11] J. G. Proakis, "Digital communications". McGraw-Hill, Higher Education, 2008. Fifth edition

[12] B. Sklar, and F. J. Harris, "Digital communications: fundamentals and applications," Pearson, 2021.

[13] S. Haykin, and M. Moher, "Introduction to analog and digital communications," *John Wiley & Sons, Inc*., 2007.

[14] M. A. Bhagyaveni, R. Kalidoss, K. S. Vishvaksenan, "Introduction to analog and digital communication". *River Publishers*, 2022. https://doi.org/10.1201/9781003338673

[15] Xiaohui Xu, Chao Zhang and Xiaokang Lin, "Using different orthogonal code sets for CCK modulation to mitigate co-channel interference among WLANs," *IEEE International Symposium on Communications and Information Technology*, 2005. ISCIT 2005.. Vol. 2. IEEE, 2005. https://doi.org/10.1109/ISCIT.2005.1567008

[16] A. H. Jafari and T. O'Farrell, "Performance evaluation of spatial complementary code keying modulation in MIMO systems," *2015 IEEE 81st Vehicular Technology Conference (VTC Spring)* , Glasgow, UK, 2015, pp. 1-5, https://doi.org/10.1109/VTCSpring.2015.7146005

[17] J. Mikulka and S. Hanus, "CCK and barker coding implementation in IEEE 802.11 b standard," *2007 17th International Conference Radioelektronika*, Brno, Czech Republic, 2007, pp. 1-4 IEEE, 2007. https://doi.org/10.1109/RADIOELEK.2007.3714844

[18] J. Mikulka and S. Hanus, "Complementary code keying implementation in the wireless networking," *In 2007 14th International Workshop on Systems, Signals and Image Processing and 6th EURASIP Conference focused on Speech and Image Processing, Multimedia Communications and Services*, pp. 315-318. IEEE, 2007. https://doi.org/10.1109/IWSSIP.2007.4381105

[19] Xiaohui Xu, Chao Zhang and Xiaokang Lin, "Using different orthogonal code sets for CCK modulation to mitigate co-channel interference among WLANs," *IEEE International Symposium on Communications and Information Technology*, 2005. ISCIT 2005.. Vol. 2. pp. 885-888, https://doi.org/10.1109/ISCIT.2005.1567008

[20] T. D. Tuyen, and T. A. Vu. "Novel Low-Complexity CCK Decoder for IEEE 802.11 b System," *VNU Journal of Science: Natural Sciences and Technology* 27.4 (2011).

[21] L. Jing, H. Wang, C. He and Z. Ding, "A novel spatial CCK modulation design for underwater acoustic communications," *IEEE Transactions on Vehicular Technology*, Vol. 68, no. 6 (2019), pp. 6192-6196. https://doi.org/10.1109/TVT.2019.2912583

[22] F. Talebi, and T. G. Pratt. "Codeset overlay for complementary code keying direct sequence spread spectrum," *In Proc. 6th Int. Conf. Mobile Ubiquitous Comput., Syst., Services Technol*., pp. 179-183. 2012.

[23] I. H. M. Ata and Qiu Pei Liang, "Using modified fast Walsh transform (MFWT) to accommodate increasing data rate of IEEE 802.11 b PHY WLAN to 22 Mbps," *In IEEE 2002 International Conference on Communications, Circuits and*

Systems and West Sino Expositions, vol. 1, pp. 534-538. IEEE, 2002. https://doi.org/10.1109/ICCCAS.2002.1180676

[24] H. Wang, L. Jing, C. He and Z. Ding, "High rate cck modulation design for bandwidth efficient link adaptation," *IEEE Wireless Communications Letters*, Vol. 8, no. 2, pp. 496-499, (2019). https://doi.org/10.1109/LWC.2018.2877648

[25] H. Shokravi, H. Shokravi, N. Bakhary, M. Heidarrezaei, S. S. R. Koloor, and M. Petrů, "A review on vehicle classification and potential use of smart vehicle-assisted techniques," *Sensors*, Vol. 20, no. 11 (2020): 3274. https://doi.org/10.3390/s20113274

[26] N. A. Ali, M. AbuElkhair and S. Bouktif, "Utilizing VIN for improved vehicular sensing," *In 2016 IEEE Wireless Communications and Networking Conference*, pp. 1-6. IEEE, 2016. https://doi.org/10.1109/WCNC.2016.7564813

تنفيذ تعديل التشفير التكميلي المرن (CCK) للمركبات ذاتية القيادة (AV)

زينة علي محمد* **قتيبة إبراهيم علي****

zinah.mohammed@uoninevah.edu.iq qut1974@gmail.com

* قسم هندسة الحاسوب والمعلوماتية , كلية هندسة الالكترونيات, جامعة نينوى,العراق

** قسم هندسة الحاسوب, كلية الهندسة, جامعة الموصل,العراق

تاريخ الاستلام: 6 فبراير 2024 استلم بصيغته المنقحة: 4 مارس 2024 تاريخ القبول: 22 مارس 2024

الملخص

في مجال الاتصالات اللاسلكية، يبقى ضمان الخصوصية الشاملة مصدر قلق بالغ، خاصة في تطبيقات الوقت الفعلي مثل المركبات ذاتية القيادة (*AV*). غالبًا ما تفشل البروتوكولات اللاسلكية الحالية في معالجة تحديات الخصوصية والأمان هذه بشكل فعال، خاصة عندما يتعلق الأمر بنقل البيانات الحساسة. ولمواجهة هذا التحدي، تقترح هذه الورقة حلاً فريدًا مصممًا خصيصًا لتلبية المتطلبات المحددة لكل مركبة ذاتية القيادة من خلال إنشاء نطاقات شبكة لاسلكية فردية. لتعزيز الخصوصية والأمان، تم تقديم نهج جديد يسمى التعديل المرن. *تعد طريقة دمج رقم تعريف المركبة (*VIN*) في معادلة* CCK *تقنية تعمل على تحسين الخصوصية في شبكات* 802.11b *. يقدم هذا التحسين مستوى إضافيًا من الأمان لناقل* WCAN *المقترحة. بالإضافة إلى ذلك، نقوم بتوسيع نطاق التحسين من خلال تنفيذ مجموعة من التعديلات على مخطط تعديل* CCK *التقليدي. يتم تغيير زوايا الطور للإشارات المرسلة لضمان عدم تأثير تعديلات مخطط تعديل* CCK *على التعامد والارتباط، وهو أمر ضروري للاتصال الفعال. أظهرت نتائج التعديل المرن أن معدل خطأ البت (*BER*) وفقدان الحزمة لوحدة التحكم الإلكترونية في جهاز الاستقبال كانت مستقرة بين تعديلات* CCK *المختلفة. يشير هذا إلى متانة الميزات الأساسية لتعديل* CCK *وأن مدى التعديلات لا يؤثر على مخطط تعديل* CCK *فيما يتعلق بخصائص التعامد والارتباط. على العكس من ذلك، هناك تحدي كبير في اعتراض الإشارة وفك تشفيرها بواسطة وحدة التحكم الإلكترونية التي تتنصت، والتي أظهرت ان فقدان الحزمة يتراوح من 63% إلى 100% عبر حالات* CCK *المختلفة.*

الكلمات الدالة :

تعديل مفتاح الكود التكميلي (CCK)، المركبة المستقلة (AV)، شبكة منطقة التحكم (CAN)، رقم تعريف المركبة (VIN).