Secure Controller Area Network (CAN) Transceiver With Embedded Authentication Support

Weizhong Chen, *Member, IEEE*, Xianshan Wen, *Member, IEEE*, Can Hong, *Student Member, IEEE*, Theodore W. Manikas, *Senior Member, IEEE*, Mitchell A. Thornton, *Senior Member, IEEE*, and Ping Gui, *Senior Member, IEEE*

***Abstract*— The growing number of security threats and vulnerabilities in automotive and industrial control systems motivates the design of Controller Area Network (CAN) bus components with enhanced security measures while maintaining compatibility with existing standards and allowing for interoperability with non-enhanced systems. We present such an enhancement that is implemented by replacing standard CAN bus transceivers with a new transceiver that permits automatic authentication of CAN frames. The theoretical basis of our approach is based on incorporating a secondary communications channel in a virtual manner that simultaneously transmits an authentication signature with each CAN frame. To implement the authentication mechanism, a new backward-compatible transceiver is described, designed and validated that implements the virtual channel through selectively delaying the rising edges in a Non-Return-to-Zero (NRZ) waveform that encodes a CAN frame at the physical layer. Novel aspects of the CAN transceiver include the use of use of authentication signature generators and comparators, rising edge time-based modulator/demodulator circuitry, and phase-preserving rail converters. The mixed-signal transceiver circuit was fabricated using a 0.18μm CMOS process and operation was validated over PVT corner cases and with non-secure transceivers to demonstrate backward compatibility.**

***Index Terms*— Automotive security, CAN transceiver, frame-level authentication, message authentication code generation, phase-preserving dual–rail converter.**

I. Introduction

MODERN, automobiles comprise an increasing number of environmental sensors and other subsystems that are configured as Electronic Control Units (ECU). This large and growing number of ECUs communicate with one another using an embedded network with the most predominant network standard being the Controller Area Network (CAN) [1], [2]. Coincident with the continually increasing number of ECUs is a corresponding increase in the attack surface area. Automotive cybersecurity vulnerabilities have gained significant attention over the past decade, driven by numerous cyberattack experiments, as illustrated in Fig. 1. In 2014, researchers demonstrated a remote exploitation of a vulnerability in the Uconnect infotainment system, allowing internet-based access to a Jeep Cherokee [3]. Similarly, in 2016, Keen Security Lab successfully hacked a Tesla Model S by exploiting vulnerabilities in its firmware and web browser. In 2018, they remotely compromised a BMW vehicle by targeting vulnerabilities in their infotainment and telematics systems [4]. Additionally, keyless entry relay attacks—enabling attackers to unlock and start vehicles by intercepting signals between key fobs and keyless entry systems—and CAN Bus injection attacks, where malicious messages are directly inserted into a vehicle's CAN bus, have become prominent topics in recent research. Consequently, an automobile's vulnerability to cyber-attacks is of significant concern. And CAN network plays an important role as the most well-known communication bus system between sub systems in modern vehicles.

Received 17 November 2024; revised 15 January 2025; accepted 28 January 2025. Date of publication 25 February 2025; date of current version 30 July 2025. This article was recommended by Associate Editor H. Jiang. *(Corresponding author: Ping Gui.)*

Weizhong Chen, Xianshan Wen, Can Hong, Mitchell A. Thornton, and Ping Gui are with the Department of Electrical and Computer Engineering, Lyle School of Engineering, Southern Methodist University, Dallas, TX 75205 USA (e-mail: weizhongc@smu.edu; xianshanw@smu.edu; canh@smu.edu; mitch@smu.edu; pgui@smu.edu).

Theodore W. Manikas is with the Department of Computer Science, Lyle School of Engineering, Southern Methodist University, Dallas, TX 75205 USA (e-mail: manikas@smu.edu).

Digital Object Identifier 10.1109/TCSI.2025.3538844

A. CAN Network in Modern Automotive Application

In the 1980's timeframe, CAN was developed as a wired bus-based system to reduce system cost and complexity as compared to P2P approaches. The CAN communications protocol specifies a Protocol Data Unit (PDU) referred to as a "frame." To further reduce cost, weight and complexity, CAN frames are encoded with asynchronous bit-serial signaling at the physical layer. Noise immunity in the harsh automotive environment is enhanced through use of dual-rail signaling that enables common-mode rejection.

From an architectural point of view, the CAN bus connects ECU subsystems or nodes that typically comprise one or more sensors and/or actuators, a microcontroller (MCU) and an interface to the physical communications bus. Fig. 2 contains a diagram that illustrates a subset of the various ECUs common to many automobiles including the Anti-Braking System (ABS), driver's instrument panel, and a generic sensor that could represent a vehicle's anti-collision radar.

Each ECU or CAN node in Fig. 2 comprises the host subsystem, a controller and a transceiver. The controller often comprises a microcontroller and associated interfaces, sometimes referred to as the MCU.

The CAN transceiver, in its simplest form, is only responsible for receiving and translating CAN control and data frames from other ECUs and for translating data frames provided by the controller into corresponding physical layer signals that it drives onto the CAN wireline communications medium.

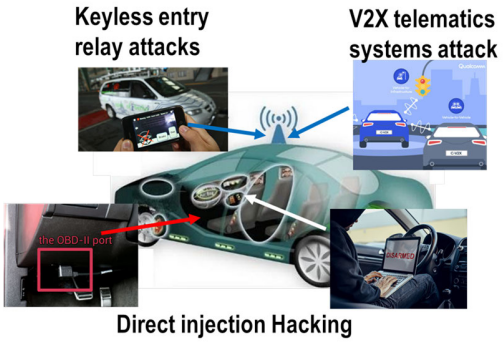

Fig. 1. Illustration of cyber-attack methods real-world scenarios.

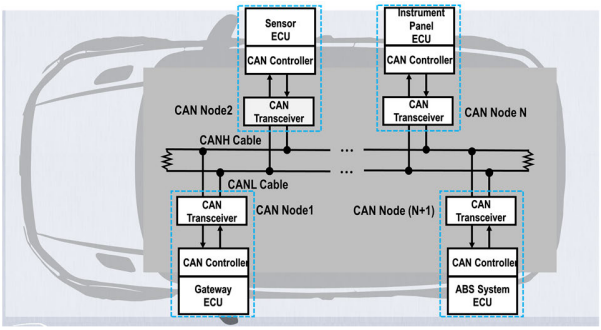

Fig. 2. (a) CAN bus network in automotive application with multiple ECUs.

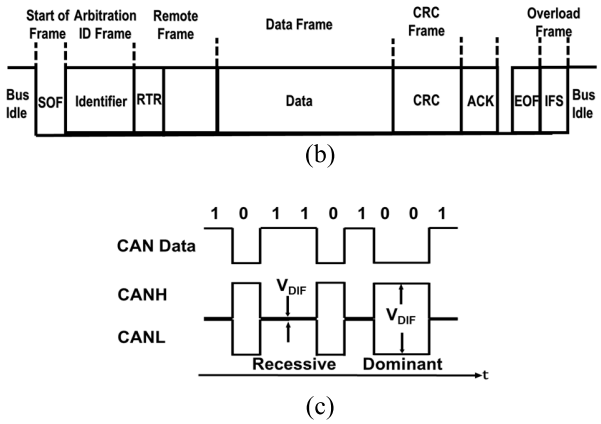

Fig. 3. (a) A standard CAN message frame structure, and (b) dual–rail voltage–mode signals on CAN transmission medium.

CAN is specified as a broadcast–based, message–oriented protocol that ensures data's integrity and prioritization by allowing device of the highest-priority to transmit when multiple devices try to send data simultaneously, while lower–priority devices hold off. This is accomplished at the physical layer through the clever use of dominant/recessive signaling levels in conjunction with the arbitration bit field that immediately follows the Start-Of-Frame (SOF) bit at the beginning of each CAN frame. Due to the dominant/recessive voltage range definitions and the means in which the CAN bus is terminated, priority is granted to frames with lower-valued identifier bit-fields when collisions occur. Since frame arbitration is implemented at the physical layer, all ECUs receive all frames and thus CAN is a frame-broadcast schema.

Fig. 3(a) illustrates a standard CAN message frame structure that consists of the SOF, the arbitration ID (identifier, represents the priority) frame, remote frame including Remote Transmit Request (RTR) code, control frame including Data Length Code (DLC), data frame, CRC (Cyclic Redundancy Check) frame and overload frame including Inter–Frame Spacing (IFS).

The reliability of the CAN protocol is further strengthened by converting the single –rail serial message frame signal into differential signals and transmitting through two –wire cables, which helps enable common–mode noise cancelation and minimize the effects from crosstalk and Electromagnetic Interference (EMI). Fig 3(b) shows the CAN bus data transmission with dual rail signals that are commonly named CANH and CANL. V_{DIF} is defined as the voltage difference between CANH and CANL. When V_{DIF} is close to zero, this bit is defined as recessive bit (0'), and when V_{DIF} is larger than a certain threshold it is defined as dominant bit (1').

B. Security Challenges for CAN Network in Modern Automotive Application

Although the CAN bus protocol has been proven to be reliable in harsh noisy environments and has been used in automotive applications for over 30 years, its original design did not account for the current cyber-security threat landscape.

Several reasons cause the CAN bus to be easily attacked in today's environment [3]. First, the CAN bus system is a broadcast-based communication system, thus all connected nodes receive all frames on the bus. An attacker can easily access the network traffic and read data frame by penetrating any of the many external sensors present in modern automobiles. Second, the CAN protocol does not include any means for frame authentication. An attacker can easily inject a malicious control frame by using any node's identifier. Third, the CAN protocol only specifies a simple Cyclic Redundancy Code (CRC)-checking capability to determine whether a received frame has been modified. A fake or maliciously injected message that only contains modifications to the data payload portion of the frame may not be detected. Fourth, as previously discussed, CAN uses a very simple arbitration scheme for colliding frames that results in frames with the highest priority (*i.e.*, lowest-valued identifier field) always wins arbitration. Exploiting the arbitration scheme by repeatedly injecting frames with low-valued identifier fields can result in a Denial-Of-Service (DOS) attack whereby an adversary can continually send high-priority frames that overwrite legitimate frames sent by other lower-priority ECUs thus starving the other ECUs by preventing them from receiving legitimate frames.

The bus-off attack is one of the widely used DOS attack methods [5], [6]. The attacker periodically injects attack message that spoof a victim node. This causes the CAN error handler to repeat until the victim node is deceived into "thinking" that it is faulty, which causes the node to enter the "bus-off" state.

The lack of built–in message or frame authentication and encryption in CAN protocol renders it susceptible to various other types of cyberattacks, all of which can jeopardize vehicle safety and data integrity.

C. Prior CAN Transceiver Security Enhancement Schemes

Multiple strategies to enhance the security of the CAN bus system were presented in prior research. Cryptographic based solutions are the most widely used method. In [7], all ECUs and gateways get an initiate authentication and encryption keys at the start point and keep updating the key periodically by derivation. This cryptographic approach truly achieves a high security level, at the cost of being backward incompatible and increasing the payload 50%. In [8], a hardware –based identification hopping (IDH) technique is implemented. The IDH controller breaks the direct data link between ECUs and CAN network, thus filtering the bad message for ECUs. An App_ID represents the ID of a CAN message in the application software. Before transmission, the App_ID is converted into a physical layer ID frame, appended to the message data payload by the transmitter, and then extracted and compared with an ID hopping table by the receiver to complete the authentication verification process. This authentication method enhances ECU security by incorporating an ID frame and performing authentication verification at the hardware layer without requiring software modifications in the ECUs. However, this approach requires adding an additional message frame to the payload of the CAN data frame, making it incompatible with conventional CAN networks.

In [9], an additional co –channel carries the underlay watermark for identification verification is integrated into the original CAN data frame. This is implemented by raising the absolute voltage levels of the dual CAN signal (V_{CANH} and V_{CANL}). The watermark voltage $V_{Watermark}$ can be expressed as:

$$V_{Watermark} = V_{CANH} + V_{CANL} - 2V_{Recessive} \quad (1)$$

The authors assert that this method minimally impacts the original CAN frame data while providing a high level of security. However, the dual-rail CAN network is prone to noise, and the absolute voltage levels are easily influenced. This method is sensitive to the cable bus environment and may lose its watermark characteristics after extended lossy bus transmissions.

Intrusion Detection System (IDS) is another widely used mechanism which scans the bus nodes for abnormal or suspicious activity and compares it with the attack scenario database. In [10], an IDS that detects the time domain feature is described. The feature utilized for intrusion detection is clock skewing. This refers not to the actual clock skew of the CAN message frame but to a calculated estimate of the data frame's clock skew. The estimation of this clock skew $Skew$ can be represented as:

$$Skew = (NBT * n - S)/S \quad (2)$$

where NBT refer to nominal bit time, n represents the number of bits and S is the measured length of the CAN message frame. NBT is the reciprocal of the CAN bus bit rate, and n is determined based on the bit rate during the frame duration. The estimated data frame clock skew is calculated by taking the difference between the measured received frame length and the computed ideal data frame length, then dividing it by the duration of the data frame. The controller simulates the clock skew to obtain the ideal skew value and performs timing measurements to identify discrepancies between the ideal skew and the actual skew for intrusion detection. Unlike conventional intrusion detection systems (IDS), this method avoids interference with the data-link layer. However, for high accuracy, the ideal skew value must be calibrated under varying environmental conditions.

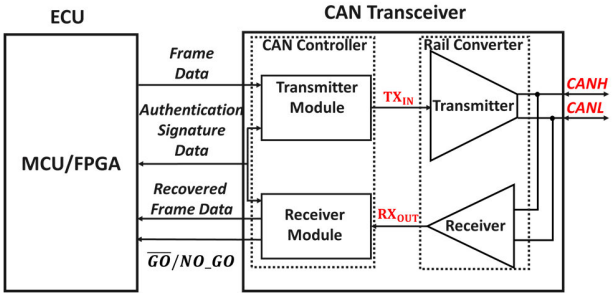

Fig. 4. Block diagram of the proposed CAN transceiver with phase modulation/extraction modules and enhanced rail converter.

In [11], a covert channel for cryptographic authentication is implemented using the timing characteristics of CAN frame transmissions. Most CAN traffic is cyclic, with messages sent repeatedly at regular intervals, which simplifies the authentication process. Authentication data is encoded in the delays between the arrival timings of CAN frames over the transmission duration. The system employs three distinct delays (10, 20, and 50 ms) to represent the timing between messages. A unique sequence of delay timings for a single CAN message frame during cyclic traffic serves as the authentication signature. However, in real-world scenarios, the inter-transmission times of cyclic traffic are noisy, often deviating significantly from expected timings. Additionally, this method does not embed authentication features directly into the message frame, making it easier for hackers to access the message data.

D. Proposed CAN Transceiver With Embedded Authentication Support

We propose a new authentication approach for enhanced security CAN transceiver. A virtual data channel is embedded within the CAN frame data stream by modulating its time domain (phase) feature. The block diagram of the CAN transceiver is illustrated in Fig. 4. The phase of the CAN frame data is modulated according to the authentication signature on the transmitter (TX) side and the phase information is extracted on the receiver (RX) side for authentication. The proposed method expands upon our previous work [12], [13], to allow for 16 bits of authentication data. The CAN bus transmission speed is 1 Mb/s. For synchronization and authentication purposes, the TX and RX operate at 25 MHz to provide a time resolution of 40 ns, which is also defined as one–time quanta (T_Q).

The embedded authentication data channel offers several advantages. First, without the correct extraction method, attackers cannot access the data. Second, the authentication information is not only within the ID frame but also included

TABLE I
SYMBOL AND NOTATION

Feature	Description
TX_{IN}	Serials CAN message data with authentication feature.
RX_{OUT}	Rail receiver recovered serials CAN message data with authentication feature.
$\overline{GO}$/NO_GO	Authentication verification result signal.
CANH/CANL	Dual rail CAN network buses.

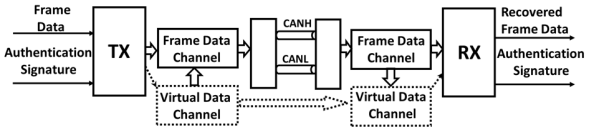

Fig. 5. Embedded authentication support with frame data channel and virtual data channel.

in other frames, ensuring that all frames in the CAN message are verified and any manipulations by the attackers are easily detected. This detection method is simpler than previous IDS methods. Third, because the authentication information is embedded in the CAN frame data stream, the data payload is not increased, and the proposed CAN transceiver remains compatible with existing systems without needing to modify the original CAN bus protocol.

Moreover, the dual-rail data transmission feature of the CAN bus protocol necessitates the use of a rail converter for data conversion, which is an integral part of the proposed CAN transceiver with embedded authentication in the data frame. This paper introduces an enhanced rail converter is designed to handle the bus–off attack mentioned earlier. The proposed authentication approach is fully implemented within the CAN bus transceiver circuit, eliminating the need for additional hardware at the data-link layer.

The rest of this paper is organized as follows: Section II explains the working principle of the embedded authentication method and the overall transceiver architecture and circuit that support this method. Section III introduces the detailed circuit implementation of the TDC, the rail transmitter and the rail receiver. Furthermore, some nonideal effects are discussed. Finally, the experimental results are discussed in Section IV, and the conclusion is presented in Section V.

II. THE PROPOSED CAN TRANSCEIVER WITH EMBEDDED SIGNATURE AUTHENTICATION

A. Virtual Channel for Frame Authentication Signatures

A virtual data channel allows each CAN bus data frame to carry a unique signature that enables the authentication of received data frames by verifying the correct signature on the concurrent virtual channel as depicted in Fig. 5. This is achieved through architectural modification within the CAN bus transceiver circuitry. Specifically, the authentication signature channel is embedded into the CAN frame data stream by modulating the phase information of the CAN frame data, inspired by our previous work in [12]. The authentication

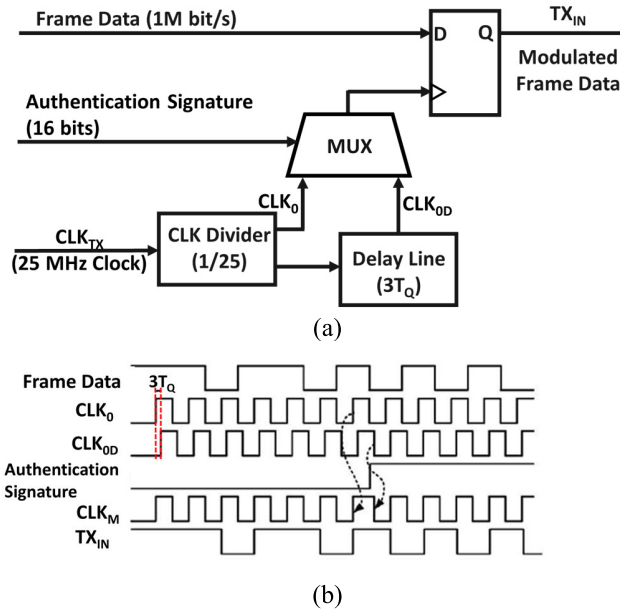

Fig. 6. (a) Block diagram of the data transmitter module, and (b) timing diagram of phase modulation operation.

signature is transmitted and received concurrently with the CAN frame data stream over the virtual authentication signature channel, facilitating authentication at the receiver end. The transceiver recovers both the frame data and extracts the authentication signature from the frame data and compares it the known signature, based on which it can generate a '$Go/NoGo$' signal to indicate whether the received data frame is trustworthy.

B. Transmitter With Frame Data and Embedded Authentication Signature

In the data transmitter module, the phase of the CAN frame data is modulated based on the authentication signature. The virtual channel was created by modulating the edge transitions within the data frame. A slight delay in the edge transition indicates a logic one (with phase modulation), while no delay indicates a logic zero (without phase modulation). Fig. 6(a) includes a block diagram of the data transmitter module design, which is capable of edge/phase–modulating the single–rail voltage signal of the CAN message frame, thereby integrating the virtual channel to carry the frame authentication signature [12].

Fig. 6(b) provides an example timing diagram illustrating the edge modulation process. Each data bit can utilize up to 25 –time quanta (T_Q) to achieve finer time resolution (i.e., 40ns for a typical 1 Mb/s CANBUS) for synchronization. To implement phase modulation, three T_Q are chosen as the phase difference in the CAN frame data bits, determined by whether the authentication signature is '1' or '0'.

A 25 MHz local clock serves as the system clock, which is divided by 25 to produce the 1MHz clock CLK_0, synchronizing with the 1 Mb/s CAN frame data. CLK_{0D} is generated by delaying CLK_0 by 3 T_Q, or 120ns. Depending on whether the authentication signature is '1' or '0', the D

flip –flop selects either CLK_0 or CLK_{0D} to resample the CAN frame data and generate the modulated CAN frame data TX_{IN}. Due to the CAN bus protocol request, no more than five consecutive '1' or '0's are allowed. Accordingly, the frequency of the authentication signature is chosen to be five times lower than that of the CAN frame data, ensuring at least one data transition in every five CAN frame data bits. This allows the authentication signature to be recovered in the RX side phase extraction by detecting the phase of the bit transitions. Additionally, to simply the detection process, this prototype uses the first 16 bits of the CAN frame data as the authentication signature, though more sophisticated signature generators can be implemented for on –chip authentication in operational versions.

C. Receiver Recovering the Frame Data and Extracting the Embedded Authentication Signature

The data receiver module demodulates received CAN frames to recover not only the actual CAN frame data but also the authentication signature by extracting the phase information embedded in the CAN frame data. To synchronize the communication between two transceiver nodes, clock synchronization is applied. The data receiver module consists of a CAN frame data recovery path, a clock synchronization block and an authentication signature recovery path, as depicted in Fig. 7(a). To synchronize with the modulated CAN frame data, a clock synchronization block synchronizes the local clock with the CAN frame data to generate a synchronized clock CLK_1, which is used to trigger a D flipflop to recover the modulated CAN frame data. In the authentication signature recovery path, a time–to–digital converter (TDC) measures the time difference between CLK_1 and the extracted data RX_{OUT}. The phase information of RX_{OUT} is extracted from the TDC output, allowing for the recovery of the authentication signature (the authentication signature). The recovered authentication signature (the authentication signature) of RX_{OUT} is compared with the expected authentication data to perform frame authentication. The authentication status signal '$\overline{GO}/NO\_GO$' uses positive-true logic and is asserted when the expected frame signature differs from the extracted frame signature. '$\overline{GO}/NO\_GO$' is a single-rail internal status signal that provides frame authentication status to the ECU that defaults to a low voltage under normal conditions when received frames are authenticated and where it is asserted to a high voltage when a received frame fails authentication. Fig. 7(b) shows the timing diagram of the CAN frame data recovery and authentication signature recovery process.

Fig. 8(a) displays the block diagram of the clock synchronization block, which includes a hard synchronization path for coarse alignment of the local clock and a soft synchronization path to generate the finely synchronized CLK_1. Fig. 8(b) illustrates the timing diagram of the hard synchronization and soft synchronization process. The hard synchronization is performed first. A clock divider and a delay line are utilized to generate 25 × 1MHz clocks. When the start of frame (SOF) is detected, which is the first '1' to '0' transition in the data package, TDC1 begins sensing the time difference between CLK_{REC} and RX_{OUT}, then updates the hard synchronization logic block to select one of the 25 clocks whose falling edge is closest to the edge of RX_{OUT}. After the hard synchronization process, a soft synchronization utilizing a different data bit will be performed. TDC2 with 40 ns resolution detects the time difference between CLK_{REC} and RX_{OUT}, adjusting a delay line via a soft synchronization logic block to align CLK_1 with RX_{OUT} at the optimal sampling point and for authentication signature recovery. This hard and soft synchronization process ensures that the rising edges of CLK_1 are optimal for sampling RX_{OUT} and extracting the embedded authentication information.

D. Hardware Security Modules

Hardware security modules (HSM) are present in both the transmitter and the receiver modules of the CAN transceiver. The transceiver was purposely designed in a manner that users of the device easily substitute a variety of HSM modules with varying and customized internal architectures since knowledge of the internal HSM architecture is likely to be maintained in a proprietary manner for security reasons. Both the transmitter and the receiver contain separate HSM modules that serve different purposes. The purpose of the transmitter HSM is to generate a message authentication code (MAC) to be used as an authentication signature word, S_T, that is combined with each frame using the modulation approach previously described. The receiver HSM generates the expected signature, S_X, that is compared to the extracted signature, S_R, of each received CAN frame. The authentication approach is based on a comparison of the extracted signature, S_R, obtained from a received CAN frame with the expected signature, S_X, that is generated by the receiver's HSM. The comparison of the extracted signature with the expected signature is performed in a comparison circuit described more fully in the following paragraph. Since both the transmitter and receiver modules use the same HSM design, this eliminates the need for storing authentication signatures in a separate database.

Although a variety of different HSM modules may be implemented, we chose relatively simple HSM architecture for the purpose of evaluating the CAN transceiver as shown in Fig. 9. The HSM is initialized by serially loading an initial seed value into the linear feedback shift register (LFSR) and a nonce value into the nonce combiner (nonce). The LFSR is a shift register that generates specific sequences using feedback mechanisms, utilized in this study for generating authentication signatures. A nonce is a one-time random number used in cryptography to enhance security. During operation, new authentication signatures, depicted as signals S_8 and S_{16}, are produced whenever a rising edge occurs on the control signal, *MAC_refresh*. Our HSM provides the capability of generating either 8-bit or 16-bit signatures depicted as S_8 and S_{16} in Fig. 9. The signature word size is selected by the input control signal, $MAC\_16/\overline{8}$. The HSM is capable of receiving new LFSR seeds and nonce values during the operation of the transceiver. When $\overline{UART\_load}$ is asserted, the LFSR seed and nonce value is updated by serially loading the values on $UART\_data$ input port.

The electrical physical layer CAN signal is in a dual-rail non-return to zero (NRZ) form when it is transmitted

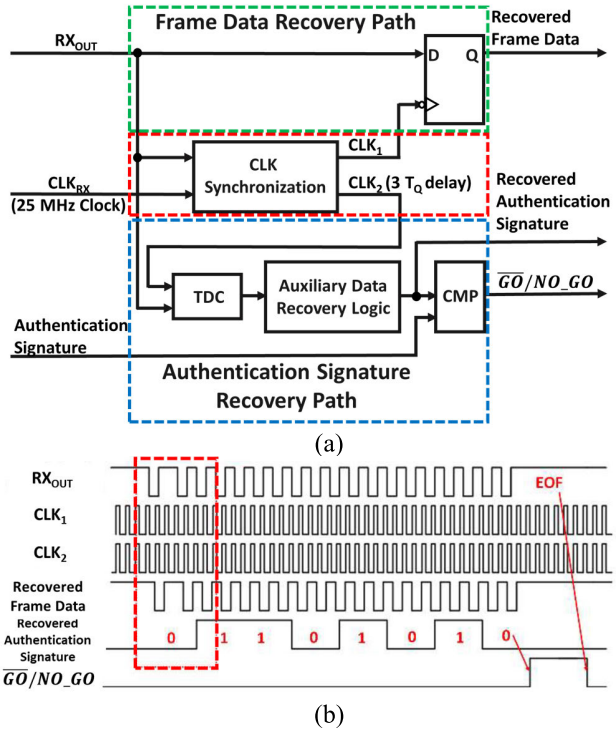

Fig. 7. (a) Block diagram of the phase extraction module including primary data recovery path, clock synchronization module and auxiliary data recovery path, and (b) timing diagram of phase extraction operation.

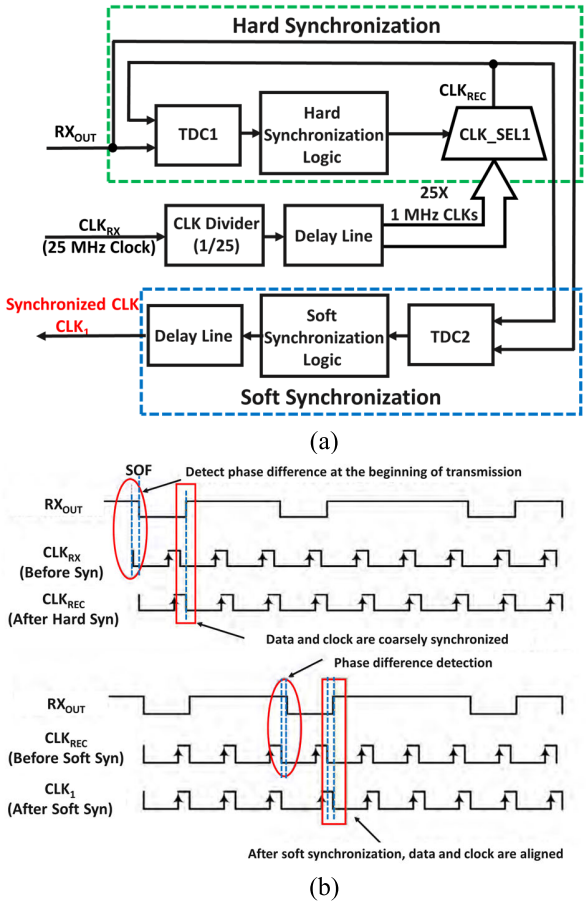

Fig. 8. (a) Block diagram of clock synchronization, and (b) timing diagram of hard synchronization and soft synchronization.

through a CAN cable. However, when dual-rail signals are input to the transceiver, the IC pin buffers perform dual- to single-rail NRZ conversion before the authentication signature is extracted. Likewise, when a frame is being prepared for transmission, it is also in NRZ single-rail form. The authentication signature is transmitted by selectively delaying the rising edges of the single-rail NRZ signal comprising each CAN frame when the signature bit is a "1," or by not delaying a rising edge when the signature bit is a "0." All rising edges of a single-rail signal representing a CAN frame may be modulated with the exception of the leading arbitration field and the trailing dominant acknowledgement bit. Neglecting the arbitration and acknowledgement bits, the shortest possible CAN frame comprises approximately 40 bits as depicted in Fig. 2. The CAN standard describes the bit stuffing rule that limits the longest possible sequence of consecutive frame bits of the same value to a maximum of five. Using the shortest frame size while considering the worst-case frame content in the form of subsequent blocks of five bits of the same value, it is guaranteed that 40/5=8 rising edges are present. Thus, any standard CAN frame can support an authentication signature, S_8, that is eight bits in length. Our transceiver also supports the use of 16-bit authentication signatures, S_{16}, for increased security when larger frame sizes compliant with the CAN-FD specification are employed [2].

Initialization of the HSM in Fig. 10 results in loading the LFSR with a seed value and storing the nonce and signature word size select flag in internal registers. The LFSR register is combined with the nonce value via a bit-wise XOR operation and the resulting value, in turn, is hashed to produce the authentication signature, either S_8 or S_{16}, in a cryptographically secure manner depending on the $MAC\_16/\overline{8}$ flag. The hash function was designed to comply with the avalanche criterion. Specifically, when the Hamming distance among any two input words to the CHS block is unity (*i.e.*, the two input words differ by only a single bit), the associated two hash values have a Hamming distance of at least one-half the word size.

The level of desired security can be controlled by the frequency with which the $MAC\_refresh$ control signal toggles from a low to high voltage. A rising edge on the $MAC\_refresh$ control input causes the LFSR to increment. In this manner, each CAN frame may have a unique authentication signature. The LFSR only increments when the MCU asserts the $MAC\_refresh$ control signal and not via the local clock signal, $CLOCK$. Thus, system synchronization is maintained since the controlling MCU dictates when the LFSRs increment.

The LFSR is implemented with feedback taps corresponding to a primitive polynomial to ensure that maximal length sequences are generated. The HSMs are specified using the Verilog HDL and, in particular, the LFSR is specified with a set of programmable feedback taps enabling the primitive polynomial to be easily changed or updated.

The transmitter HSM is responsible for the generation of frame signatures, S_T, to be modulated into the

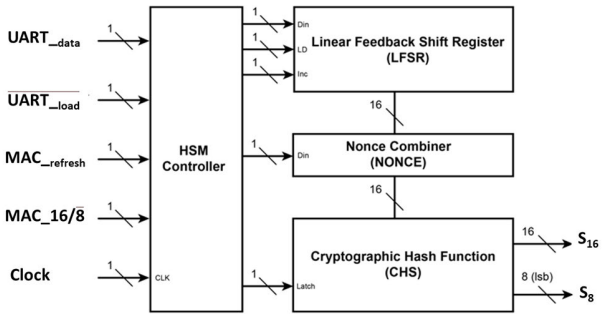

Fig. 9. Block diagram of hardware security module (HSM).

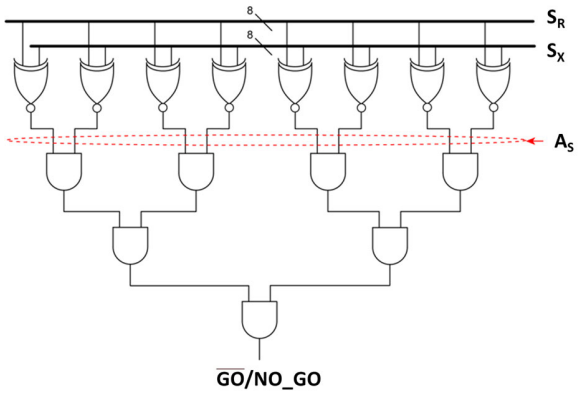

Fig. 10. $\overline{GO}/NO\_GO$ generation circuit with authentication syndrome shown.

NRZ physical-layer signals in the transmitter block of the transceiver by delaying rising edges by 3 TQ for a signature bit that is 1-valued and by adding zero delay to rising edges when the signature bit is 0-valued. The receiver HSM is used to generate the expected signature, S_X, of each received frame. CAN frame authentication occurs by providing the demodulated, or extracted, signature of a received CAN frame, S_R, and the expected signature, S_X, to the $\overline{GO}/NO\_GO$ generation circuit. Authentication is implemented by forming an "authentication syndrome," A_S, using parallel bit-by-bit comparator circuits of S_X and S_R as $A_S = S_X \oplus S_R$. The $\overline{GO}/NO\_GO$ status signal is asserted high when the Hamming weight of the authentication syndrome is non-zero, as shown in Fig. 10.

It is noted that the HSM module implemented in the transceiver as described here is exemplary only. More sophisticated means of generating authentication signatures can be implemented through the use of alternative HSM architecture. More sophisticated attack and error handling could be implemented using the authentication syndrome to pinpoint the portion of the CAN frame signal that caused authentication to fail. Enabling the signature generation to be defined independently of the overall CAN transceiver allows different CAN bus system users to implement their own processes as well as maintaining confidentiality. In terms of handling authentication failures, the status signal, $\overline{GO}/NO\_GO$, could be used to simply drop frames that are not authentic, or alternatively, to issue one or more error frames when authentication fails.

HSM synchronization can likewise be implemented in a variety of different ways and the particular synchronization

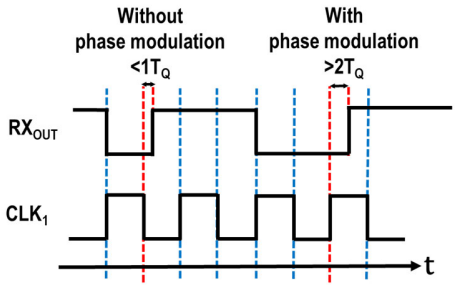

Fig. 11. Phase detection with $1T_Q$ tolerance. Phase difference less than 1 T_Q is considered bit without phase modulated, over 2 T_Q is considered bit with modulation.

method employed should be carefully considered from a cyber security point of view since losing synchronization among the HSMs within the transceiver can cause false- and positive-errors to occur with respect to the authentication process. For example, it is necessary that the expected frame signature, S_X, generated within the receiver, must match the received frame signature, S_R, in an authentic frame. Hardware-assisted synchronization can be implemented through appropriate circuits and signals within the HSMs, software-assisted synchronization can be accomplished through the implementation of special control frames that initialize the transceiver HSMs and that indicate when new frame signatures should be computed, or a hybrid hardware/software approach can be employed that comprise a combination of these two approaches as validated through our analyses.

The HSM is also designed with a compatibility test mode that enables the transceiver to operate as if no security features are present. The test mode is enabled by seeding the LFSR with the value 16'b0 thus causing no CAN frame signal rising edges to be delayed. Interoperability of the transceiver was validated by operating some transceivers in test mode while others were operating in secure mode. As expected, the test mode transceivers did result in $\overline{GO}/NO\_GO$ output signals that toggled to a high voltage indicating that the received frame had an invalid signature as expected; however, examination of the frame data indicated that it was indeed correct.

E. Phase Error Tolerance

To successfully recover the authentication signature data (i.e. the authentication signature), the phase extraction module must be capable of recovering the phase –modulated signal despite the presence of jitter or frequency drift. Since the proposed receiver is fully digital with a 40 ns (i.e. $1T_Q$) time resolution, the TDC output error caused by jitter will not exceed $1T_Q$, provided the peak –to –peak jitter of the entire transmission chain is less than 40ns, regardless of the initial phase of the modulated CAN frame data. In this design, the phase modulation index is set to $3T_Q$, ensuring that there is a $1T_Q$ tolerance for phase error from TDC, as shown in Fig. 11. The authentication signature recovery logic considers a phase difference less than $1T_Q$ as without phase modulation ($0T_Q$ in the ideal case) and a phase difference greater than $2T_Q$ as with phase modulation ($3T_Q$ in the ideal case).

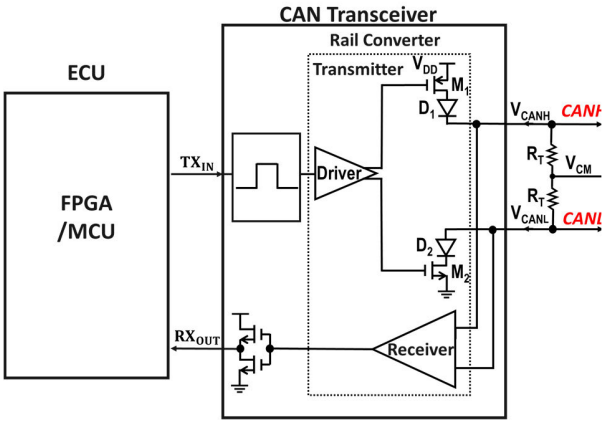

Fig. 12. Block diagram of a conventional CAN transceiver with rail converter.

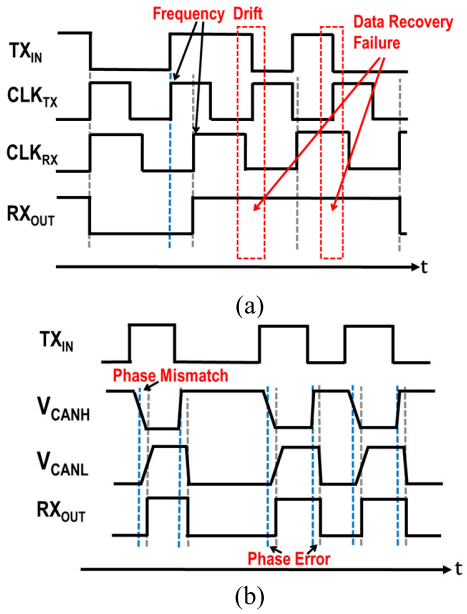

Fig. 13. (a) Frequency drift issue, and (b) phase mismatch and phase error issue.

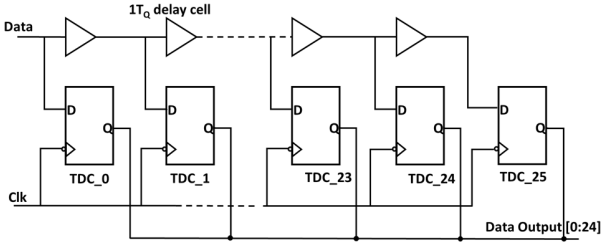

Fig. 14. TDC circuit implementation.

III. Circuit Implementation

In this section, detailed circuit implementation and design considerations are included. To overcome the drawback of conventional CAN rail converter and prevent the previously mentioned bus-off attack, a proposed CAN rail converter, comprising both a rail transmitter and a rail receiver, has been designed.

The dual-rail data transmission feature of the CAN bus protocol necessitates the use of a rail converter for data conversion. Fig. 12 illustrates the block diagram of a conventional CAN transceiver with rail converter, consisting of both a transmitter and a receiver [5]. However, the weakness in conventional CAN rail converter topology has made bus-off attacks easier to execute. The conventional transmitter is only capable of generating a dominant bit, turning on transistors M_1 and M_2 to quickly pull V_{CANH} to V_{DD} and V_{CANL} to GND. In contrast, the recessive bit is set by the termination resistors R_T, driving the bus to a common mode voltage, V_{CM}. Due to the broadband communication feature of the CAN network, the receiver continuously reads the dual–rail signal data from CANH and CANL cables and converts it into a single–rail signal, RX_{OUT}, for ECU decoding. Since the terminal resistors R_T have limited driving capability, attackers can exploit this through the attacking node to force V_{CANH} and V_{CANL} to remain in the dominant bit state by continuously activating M_1 and M_2.

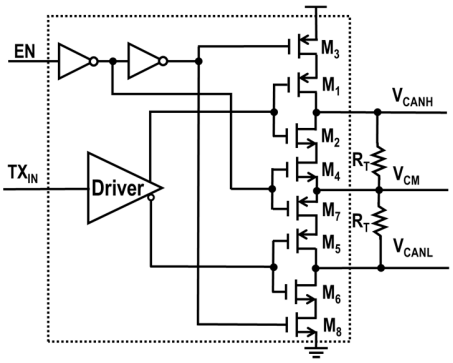

Fig. 15. The proposed dual rail transmitter with enhanced driving capability.

Moreover, the transition speed from recessive to dominant bit is controlled by M_1 and M_2, whereas the transition speed from dominant to recessive bit is determined by the termination resistors R_T. To get a fast transition, R_T is required to be as small as possible, which leads to a large constant current flowing from V_{CANH} and V_{CANL} to V_{CM} during dominant bit. This imposes a limitation on the power efficiency of the circuit.

It is important that edge transitions in the dual–ended signals remain aligned within some tolerance level (*i.e.*, phase matched), to ensure that the received single–ended signal is correct especially with the authentication signature recovery. However, certain non-ideal factors can lead to phase mismatches and phase errors, potentially resulting in transmission failure. Fig. 13(a) illustrates the jitter and frequency drift between the transmitter clock CLK_{TX} and the receiver clock CLK_{RX}. When the frequency difference between CLK_{TX} and CLK_{RX} increases beyond a certain point, the resulting phase error leads to signal recovery failure. Second, the difference in rising/falling edge time of data due to the different driving capabilities of the transmitter also results in phase error as depicted in Fig. 13(b). Third, the unequal CANH and CANL cable lengths bring extra phase mismatch.

The following section explains how the proposed rail converter can minimize phase mismatches caused by nonidealities in both transceivers and transmission cables, as well as tolerate larger phase errors.

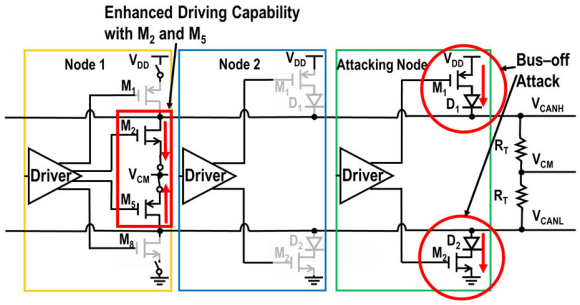

Fig. 16. Working condition of the conventional transmitter, and the proposed transmitter under bus–off attack.

A. The TDC Circuit

To address the frequency drift issue, the local clock synchronization process is important. Fig. 14 illustrates the TDC circuit used in both local clock hard synchronization and soft synchronization. The TDC is composed of two series chains: D-flip-flops and delay cells. Each delay cell introduces a 1 T_Q (40 ns) delay for the data. The data is delayed 25 times and triggers all D-flip-flops in the chain to generate a 25-bit data output [0:24]. This output is then used by the following synchronization logic module to select the clock signal with the same phase as that of the received frame data.

B. The Rail Transmitter Circuit

The main principle of bus–off attack is to use one node always overwriting the CANH and CANL cables in a dominant state. Since this attacking condition is the same as normal dominant bit state, it usually takes several bits time for CAN system with conventional CAN transceiver only to realize that the bus is under attack.

To address this issue, the proposed rail converter transmitter incorporates M_1 and M_6 for dominant bit driving, M_2 and M_5 for recessive bit driving, as depicted in Fig. 15. The presence of M_2 and M_5 for driving the recessive bit ensures that during an attack, V_{CANH} (V_{CANL}) is pulled down (pulled up) to an abnormal middle voltage between V_{CM} and V_{DD} (GND) as depicted in Fig. 16. The proposed rail converter is also back compatible with conventional CAN rail converters. When it is not transmitting message, an EN signal turns off switch transistors M3, M4, M7 and M8 fully disconnecting the transmitter from the cables, ensuring no impact on the other active nodes. This design aids in immediately detecting a bus–off attack and sends a warning signal to the ECUs to block the attacker's fake message. The EN transistor M4 and M7 can also be turned off after dominant to recessive transition to save power consumption.

The proposed rail transmitter also enables quick transitions between recessive –to–dominant and dominant–to–recessive bits without significant static power consumption. The sizes of M_1, M_6, M_2 and M_5 are carefully chosen to ensure equal rise and fall times, minimizing output phase mismatch. The proposed transmitter uses M_2 and M_5 for recessive bit driving, eliminating reliance on R_T to minimize the output phase mismatch.

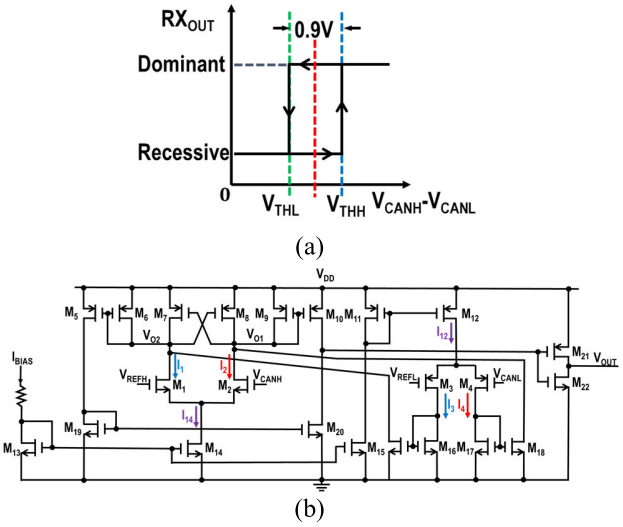

Fig. 17. (a) Hysteretic comparation with V_{THH} and V_{THL}, and (b) schematic of hysteretic dual-to-single receiver.

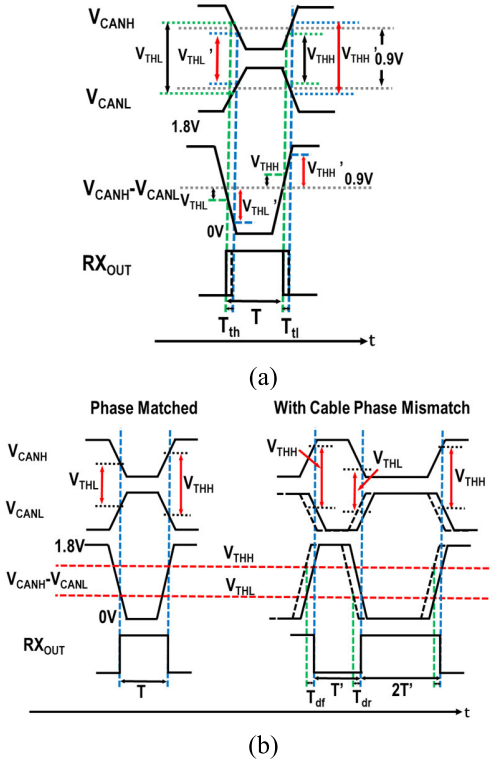

Fig. 18. (a) Phase error cancellation with symmetric V_{THH} and V_{THL}, (b) Phase error cancellation under different cable phase mismatch situations.

C. The Rail Receiver Circuit

The receiver performs a hysteretic comparison of the voltage difference between V_{CANH} and V_{CANL} with a positive trigger point V_{THH} (0.6 V in this design with a V_{DD} of 1.8 V) and a negative trigger point V_{THL} (1.2 V) as illustrated in Fig. 17(a). Hysteretic comparison is a comparison method with hysteresis that avoids false triggering by setting different threshold points, used in this study to compare voltage differences in CAN bus signals. This approach ensures that neither the dominant nor recessive bit is triggered by V_{CANH}

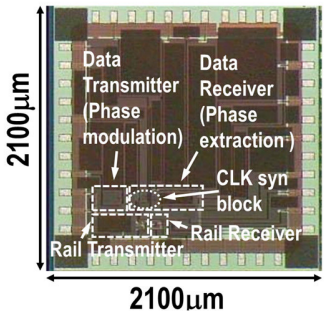

Fig. 19. Chip die photo.

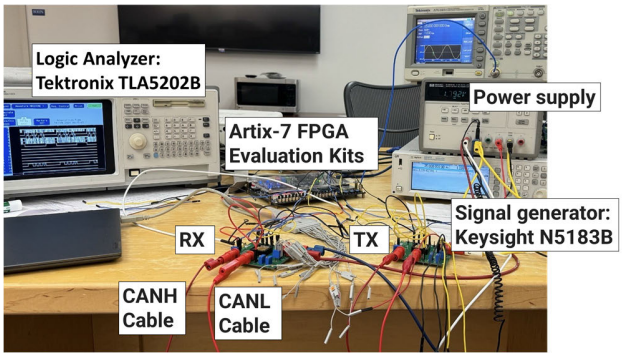

Fig. 20. CAN bus transceiver chip communication test bench setup.

or V_{CANL} alone. This design provides a sufficient voltage margin to prevent false triggering.

Fig. 17(b) illustrates the detailed circuit of the receiver. The comparator includes two input pairs: M_1 and M_2 as NMOS transistors for V_{CANH} (0.9–1.8 V), and M_3 and M_4 as PMOS transistors for V_{CANL} (0–0.9 V). Two DC common–mode voltage V_{REFH} (1.35V) and V_{REFL} (0.45V) are introduced for voltage comparison. The differential input pairs compare V_{CANH} and V_{CANL} against V_{REFH} and V_{REFL} respectively, combining the resulting differential currents to achieve hysteretic triggering. The two trigger points can be expressed as:

$$V_{THH} = V_{REFH} - V_{REFL} + V_{OS} \tag{3}$$

$$V_{THL} = V_{REFH} - V_{REFL} - V_{OS} \tag{4}$$

where $(V_{REFH} - V_{REFL})$ is 0.9 V, V_{OS} represents the hysteretic offset voltage with a nominal value of 0.3 V, determined by the sizes of M_6, M_7, M_8 and M_9 [14].

D. Nonideal Effect Analysis

Since authentication data is recovered from the receiver output RX_{OUT} by the phase extraction block, it is essential to maintain the phase (pulse width) of RX_{OUT} consistent with TX_{IN}, despite non–idealities like Process, Voltage, and Temperature (PVT) variations. With PVT–induced shifts in V_{OS}, the trigger points V_{THH} and V_{THL} can also vary, potentially causing timing errors on the rising edge T_{th} and falling edge T_{tl} of RX_{OUT}. However, because V_{THH} and V_{THL} are always symmetric around 0.9 V, any voltage variation in V_{THH} (ΔV_{THH}) is offset by an opposite variation in V_{THL} (ΔV_{THL}). With the transmitter's balanced drive strength, maintaining identical rise and fall slopes ensures that T_{th} and

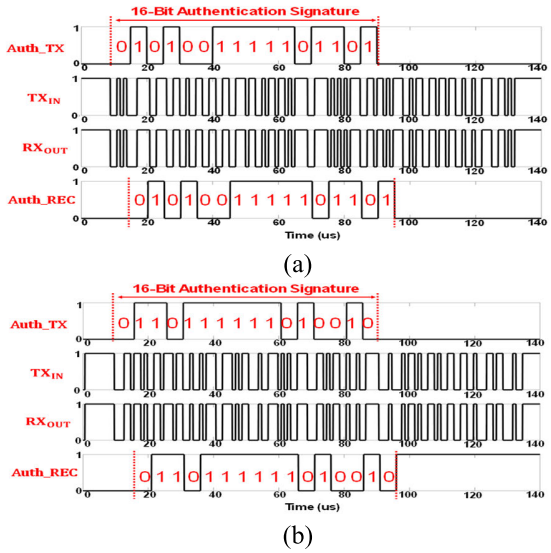

Fig. 21. (a) Measurement results with frequency drift between TX and RX (a) +0.05% frequency drift, and (b) −0.05% frequency drift.

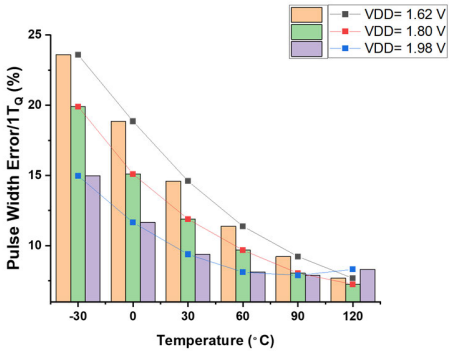

Fig. 22. RX_{OUT} pulse width error with temperature (−28.5°C to 120°C) and voltage (VDD=1.8V/1.98V/1.62V) variation.

T_{tl} remain equal, preventing pulse width errors (phase errors) in RX_{OUT}, as illustrated in Fig. 18(a).

Another non–ideal factor that may contribute to phase error in RX_{OUT} is the phase mismatch between CANH and CANL due to unequal cable lengths. When there is an additional delay on either the CANH or CANL cable, timing errors T_{dr} and T_{df} can occur on RX'_{OUT}s rising and falling edges. These errors result from the delayed triggering of the signal with the larger delay, as both differential input pairs are needed for triggering. Consequently, the bit transition in RX_{OUT} is primarily determined by the later–arriving signal in CANH/CANL, making T_{dr} and T_{df} approximately equal in the first order, as depicted in Fig. 18(b). If the ideal (phase–matched) pulse width of RX_{OUT} is T_0, the pulse width with phase mismatch can be expressed as:

$$T' = T_0 - T_{dr} + T_{df} \approx T_0 \tag{5}$$

Thus, the effect of phase mismatch on RX'_{OUT}s pulse width error (phase error) is greatly suppressed.

IV. Measurement Result

The proposed security–enhanced CAN transceiver chip was fabricated using the TSMC 180 nm process. Fig. 19 shows

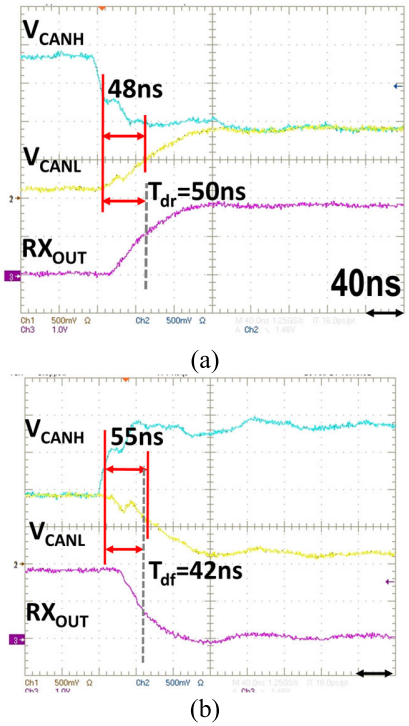

Fig. 23. Timing errors with phase mismatch between V_{CANL} and V_{CANH} (a) rising edge timing errors T_{dr}, and (b) falling edge timing errors T_{df}.

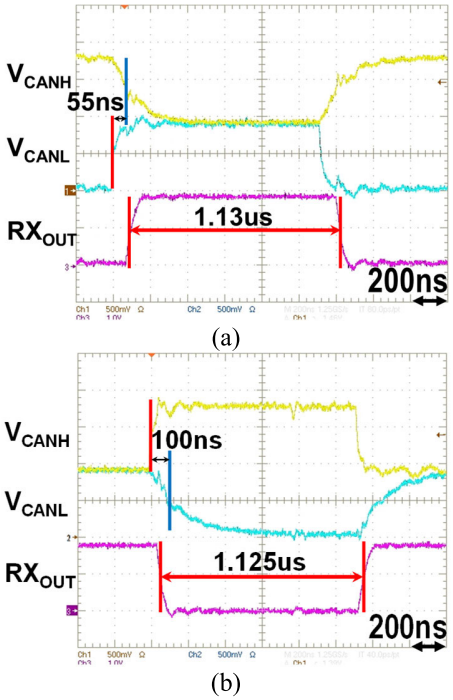

Fig. 24. Measured pulse width of RX_{OUT} with phase mismatch between CANH and CANL (a) Extra RC on V_{CANH}, (b) Extra RC on V_{CANL}.

a photo of the chip die, with a chip size of 4.41 mm^2. Ten CAN transceiver ICs were tested, all demonstrating consistent results, validating the architecture and circuits of the presented CAN bus transceiver. The measurement setup, shown in Fig. 20, illustrates the transceiver communication test setup where one chip's TX sends data frames to another chip's RX via the CANH/CANL cables. The additional cable phase mismatch is introduced by adding RC delay elements to the cables. The logic analyzer captures both the CAN frame data and authentication signature from the TX and RX outputs for comparison. The VDD is 1.8 V, recessive common voltage is 0.9 V and the TX and RX operating clock frequency is 25 MHz.

Fig. 21 shows the measurement results demonstrating the CAN bus transceiver's operation. In the real world, each CAN node has its own local clock, which brings jitter and frequency drift between the TX clock CLK_{TX} and the RX clock CLK_{RX}. When the frequency difference between CLK_{TX} and CLK_{RX} increases beyond a certain point, the resulting phase error leads to signal recovery failure. As the authentication signature is recovered by comparing the phase of bit transitions to the SOF bit, the effect of frequency drift varies with the length of the data. The phase error induced by frequency discrepancies accumulates over time during data transmission. In this CAN bus transceiver, the authentication signature length is set to 16 bits, corresponding to a CAN frame data length of 80 bits (2000 T_Q). To ensure the accurate recovery of the 16–bit authentication signature, the maximum phase error occurring at the last modulated CAN frame data bit must remain within 1 T_Q. The measured RX_{OUT} maintains the same phase as the modulated CAN frame data TX_{IN}, and the extracted 16–bit authentication signature $Auth\_Rec$ aligns with the authentication signature on the TX side ($Auth\_TX$), even with $+/-0.05\%$ frequency drift between TX and RX. Here, frequency drift is defined as $(f_{TX}/f_{RX} - 1)$. With a -0.05% frequency drift, signal $Auth\_Rec$ begins to deviate from $Auth\_TX$ after the 16-bit extraction due to accumulated phase error exceeding 1 T_Q.

The transceiver's functionality has been verified through measurements with V_{DD} varying by $+/-10\%$ (from 1.62 V to 1.98V) and temperatures ranging from -28.5 °C to 120 °C. The pulse width error of RX_{OUT}, relative to $1T_Q$ (40 ns), is illustrated in Fig. 22. Even with voltage and temperature fluctuations, the pulse width error remains below 25% of $1T_Q$.

Fig. 23 depicts the zoomed in waveforms of the rising and falling edges of the receiver output alongside $V_{CANH}(V_{CANL})$, illustrating the phase mismatch. The phase difference between V_{CANH} and V_{CANL} is 48 ns. The measured T_{dr} is 50 ns, T_{df} is 42 ns and the phase error in RX_{OUT} is reduced to 8 ns.

Fig. 24 shows the measured pulse width of RX_{OUT} in the presence of a phase mismatch between CANH and CANL. This phase mismatch is induced by adding extra RC to either V_{CANH} or V_{CANL}. The ideal pulse width of RX_{OUT} is $1\mu s + 3T_Q$ (1.12 us) due to phase modulation. The resulting error in RX_{OUT}'s pulse width is reduced to less than one–fifth of the original phase mismatch on CANH and CANL. Therefore, the impact of phase mismatch on RX_{OUT}'s pulse width is significantly minimized. It should be noted that for practical applications, if the frequency drift exceeds the specified limits, the receiver will no longer be able to synchronize the data with the local clock.

Compared to existing methods, the proposed CAN transceiver implements a hardware-based time-domain authentication technique. Unlike [8], which uses hardware-based IDH, this approach does not require an additional message frame and also provides authentication that safeguards the

TABLE II
PERFORMANCE COMPARISON OF CAN SECURITY ENHANCEMENT METHODS

	This work	[8] Access'18	[9] TVT'22	[10] Access '21	[11] TIFS '21
Topology	**Hardware-Based Time Domain**	Hardware-Based IDH	Voltage Domain	Time Domain IDS	Cycle-Traffic Timing
Computational Complexity	**Middle**	Easy	Middle	High	Easy
Data frame with Authentication feature	**Yes**	No	Yes	No	No
Additional Message	**No**	Yes	No	No	No
Backward Compatible	**Yes**	No	No	Yes	Yes

data frame. Compared to [9], which relies on absolute voltage levels, the proposed method is less sensitive to environmental factors. Additionally, in comparison to [10], which uses IDS, and [11], which employs cycle-traffic delays, this method is simpler to implement and more environmentally robust.

V. CONCLUSION

This paper proposes an enhanced CAN bus transceiver featuring embedded authentication support to improve security and an enhanced rail converter for greater reliability. An authentication signature channel is integrated into the CAN frame data transmission using phase modulation. This phase–based authentication scheme does not necessitate changes to the CAN bus protocol or additional hardware, while still ensuring backward compatibility with existing systems that lack security features. Additionally, an enhanced rail converter is implemented to facilitate single–rail to dual–rail conversion for data transmission, effectively minimizing the output phase mismatch and preventing bus-off attacks. The rail converters not only maintain the phase information of the transmitted data across various PVT variations but also possess the capability to significantly reduce phase errors arising from mismatches between the dual–rail signals, thereby enhancing the reliability of phase information for authentication. Furthermore, the proposed transmitter structure helps prevent bus–off attacks through instant detection. Compared to prior security–focused CAN transceiver designs, this design addresses the security threats in modern vehicle environment without increasing the message payload or requiring additional hardware, meanwhile maintaining backward compatibility.

REFERENCES

[1] *Controller Area Network (CAN)—Part 1: Data Link Layer and Physical Signaling*, ISO Standard 11898-1:20039, Switzerland, 2003.

[2] R. Bosch, "CAN with flexible data-rate," Robert Bosch GmbH, Stuttgart, 2012.

[3] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," Black Hat, Seattle, WA, USA, 2015.

[4] KEENLAB. (Nov. 2018). *Experimental Security Assessment of BMW Cars: A Summary Report*. [Online]. Available: https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

[5] W. Samuel, J. H. Jin, and L. D. Hoon, "A practical wireless attack on the connected car and security protocol for in-vehicle CAN," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, Apr. 2015.

[6] TI. (Nov. 2003). *TCAN1462 Datasheet*. [Online]. Available: https://www.ti.com/lit/ds/symlink/tcan1462q1.pdf?ts=1730906409819&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FTCAN1462-Q1

[7] B. Groza and P.-S. Murvay, "Security solutions for the controller area network: Bringing authentication to in-vehicle networks," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 40–47, Mar. 2018.

[8] W. Wu et al., "IDH-CAN: A hardware-based ID hopping CAN mechanism with enhanced security for automotive real-time applications," *IEEE Access*, vol. 6, pp. 54607–54623, 2018.

[9] A. J. Michaels et al., "CAN bus message authentication via co-channel RF watermark," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3670–3686, Apr. 2022.

[10] J. Zhou, G. Xie, S. Yu, and R. Li, "Clock-based sender identification and attack detection for automotive CAN network," *IEEE Access*, vol. 9, pp. 2665–2679, 2021.

[11] B. Groza, L. Popa, and P.-S. Murvay, "CANTO–covert AutheNtication with timing channels over optimized traffic flows for CAN," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 601–616, 2021.

[12] X. Wang, T. Liu, S. Guo, M. A. Thornton, and P. Gui, "A 2.56-Gb/s serial wireline transceiver that supports an auxiliary channel in 65-nm CMOS," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 1, pp. 12–22, Jan. 2020.

[13] X. Wen et al., "Controller area network (CAN) bus transceiver with authentication support," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, Austin, TX, USA, May 2022, pp. 1328–1331.

[14] W. Chen, C. Hong, X. Wen, M. A. Thornton, and P. Gui, "Controller area network (CAN) bus transceiver with enhanced rail converter," in *Proc. IEEE 67th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Springfield, MA, USA, Aug. 2024, pp. 64–67.

Weizhong Chen (Member, IEEE) received the B.E. degree in electronic science and engineering from Southeast University, Nanjing, China, in 2014, and the M.E. degree in electrical engineering from The University of Texas at Dallas, Richardson, TX, USA, in 2018. He is currently pursuing the Ph.D. degree in electrical engineering with Southern Methodist University, Dallas, TX, USA. His current research interests include high-frequency power converters and GaN drivers.

Xianshan Wen (Member, IEEE) received the B.S. degree in applied mathematics from the University of Science and Technology of China (USTC), Hefei, China, in 2015, the M.S.E.E. degree from Northwestern University, Evanston, IL, USA, in December 2016, and the Ph.D. degree in electrical engineering from Southern Methodist University, Dallas, TX, USA, in 2024.

Can Hong (Student Member, IEEE) received the B.S. degree in mathematics from Louisiana Tech University, Ruston, LA, USA, in 2020, and the M.S.E.E. degree from Southern Methodist University, Dallas, TX, USA, in 2022, where he is currently pursuing the Ph.D. degree in electrical engineering. His current research interests are high-performance and low-power analog and mixed-signal IC design.

Theodore W. Manikas (Senior Member, IEEE) received the B.S. degree in electrical engineering from Michigan State University, the M.S. degree in electrical engineering from Washington University in St. Louis, and the Ph.D. degree in electrical engineering from the University of Pittsburgh. He has been with Southern Methodist University since 2009. He is currently the Associate Chair of the Department of Computer Science. His current research interests include computer systems design, security, and testing. He is also a Licensed Professional Engineer in Texas and Oklahoma.

Mitchell A. Thornton (Senior Member, IEEE) received the Ph.D. degree in computer engineering from Southern Methodist University in 1995. He is currently the Cecil H. Green Chair of Engineering and a Professor with the Electrical and Computer Engineering Department, Southern Methodist University, and also the Executive Director of the Darwin Deason Institute for Cyber Security. Prior to joining as a Faculty Member of SMU, he was employed in industry and a Faculty Member with the University of Arkansas and Mississippi State University. His research interests include cyber security and quantum informatics. He is also a Licensed Professional Engineer and has worked in leadership positions in several IEEE committees and conferences.

Ping Gui (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Delaware, Newark, DE, USA, in 2004. She is currently the Cecil and Ida Green Chair Professor with the Electrical and Computer Engineering Department, Southern Methodist University, Dallas, TX, USA. Her current research interests include analog, mixed signal, and RF IC for a variety of applications, including high-speed wireline and wireless transceivers, analog-to-digital (ADC) converters, power management integrated circuits, and low-power and low-noise circuits for biomedical applications. She was a recipient of the CERN Scientific Associate Award from 2008 to 2010, the IEEE Dallas Section Outstanding Service Award in 2011, and the Gerald J. Ford Research Fellowship at SMU in 2015. She has served on the technical program committee (TPC) for IEEE Symposium Radio Frequency Integrated Circuits Symposium (RFIC), Custom Integrated Circuits Conference (CICC), and International Symposium of Solid-State Circuits (ISSCC).