Controller Area Network (CAN) Bus Transceiver with Enhanced Rail Converter

Weizhong Chen
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
weizhongc@smu.edu

Can Hong
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
canh@smu.edu

Xianshan Wen
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
xianshanw@smu.edu

Mitchell A. Thornton
Darwin Deason Institute for Cyber Security
Southern Methodist University
Dallas, United States
mitch@smu.edu

Ping Gui
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
pgui@lyle.smu.edu

2024 IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS) | 979-8-3503-8717-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/MWSCAS60917.2024.10658700

***Abstract*—This paper presents a CAN bus transceiver with phase preserving dual-rail converters to implement a secure authentication method. An inherent auxiliary data channel is embedded in the transmitted primary data via phase modulation for data authentication. The enhanced rail converters presented here are implemented to provide single-rail to dual-rail data conversion and vice versa for data transmission while preserving the phase-modulated security signatures. The rail converters not only preserve the phase information of the transmitted data across different PVT corners but also provide significant suppression of phase errors caused by the phase mismatch between the dual-rail signals.**

Keywords— Automotive Security, CAN bus transceiver, Dual-rail communication, Phase mismatch.

I. INTRODUCTION

The Controller Area Network (CAN) protocol is widely used in automotive application and industry control systems. Recently, there has been a growing attention on the possible security issues of classical CAN-based systems. Research has revealed that conventional CAN-based systems are susceptible to security threats and vulnerabilities [1]. A demonstration of a remote attack on a 2014 Jeep Cherokee was reported in [2].

Multiple strategies are applied to enhance the security of the CAN bus system. However, these strategies usually require modifications to the protocol itself or enhancement to the hardware. For instance, NXP's new secure TJA115x CAN transceiver introduces an extension ID frame into the data frame [3]. Another challenge of the modifications is that they need to be compatible with systems not equipped with the security features. A new authentication approach is described in [4] that does not require the modification of CAN bus protocol or hardware meanwhile ensuring compatibility with existing unequipped systems. The transceiver embeds an inherent communication channel within the primary data stream by modulating the data stream in the time (phase) domain that serves to authenticate CAN frames. In accordance with the authentication approach used in [4], it is necessary to include phase preserving rail converters in the transceiver to prevent corruption of the secondary authentication channel while also ensuring dual-rail transmission feature of the CAN bus standard is preserved.

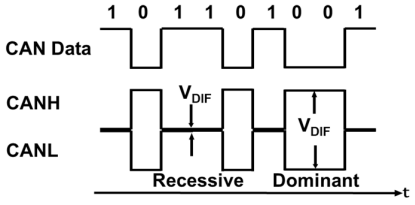


Fig. 1. Dual-rail transmission of CAN bus with recessive bits and dominant bits.

Our approach is realized through modifications to the CAN bus transceiver circuit only and the transceivers are backwards-compatible to unequipped CAN systems. We summarize the overall approach and focus on the custom designed phase-preserving rail-converter circuits that interface and drive the differential CAN cables. Circuit design details and experimental evaluation results are provided. We show that our design is tolerant to phase mismatch in the CAN cables and evaluate the bounds for allowable phase mismatch over realistic PVT corner cases.

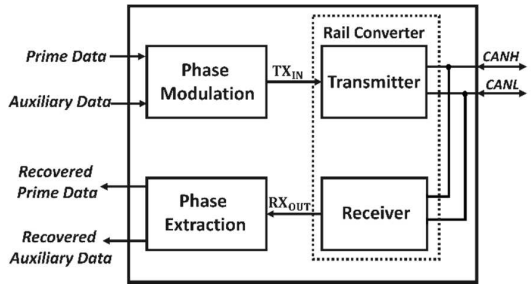


Fig. 2. The CAN transceiver block diagram.

II. CAN TRANSCEIVER

A. Overall Architecture

Phase modulation is used in [4] by incorporating an auxiliary data channel within the CAN bus protocol that provides a unique signature for each CAN frame. The CAN protocol transmits data in relatively extreme environments, such as automotive applications, and thus uses dual-rail (differential) signaling to improve signal integrity in the presence of noise, crosstalk and electromagnetic interference (EMI). To mitigate the effect of nonideal components and transmission cables, the CAN bus standard uses dual-rail signals (CANH and CANL) to transmit CAN frames. As shown in Fig. 1, 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'). In this paper, we present a CAN transceiver with rail converters that meet the CAN bus standard and provides dual-rail data transmission to demonstrate the effectiveness of using phase modulation for data authentication to enhance CAN bus security.

The block diagram of the CAN transceiver is shown in Fig. 2. The phase of the primary data is modulated according to the auxiliary authentication data on transmitter (TX) side and the phase information is extracted on the receiver (RX) side for authentication, same as in [4]. 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).

During the phase modulation on the TX side, with auxiliary data being '0' or '1', either no phase modulation or a phase modulation of $3T_Q$ is implemented accordingly, on the primary data. The rail converter converts the modulated single-rail signal (TX_{IN}) to dual-rail signals and send those signals to the CANH/CANL transmission lines.

On the RX side, the dual-rail signals on CANH/CANL are converted back to single-rail CMOS signal (RX_{OUT}) for further processing. The phase information of the received primary data bits is extracted by time-to-digital converter (TDC) in the phase extraction block. In CAN bus protocol, the number of consecutive '1's or '0's in the data packet is no larger than 5. Hence, the frequency of the auxiliary data is chosen to be one fifth of the frequency of primary data so that the auxiliary data can be recovered in RX by detecting the phase of primary data's bit-transitions. The phase of the start of frame (SOF), i.e. the first '1' to '0' transition in the data package, is detected by the TDC and stored as the initial phase of the primary data packet, and the phase of all other bit-transitions is compared against the initial phase for auxiliary data recovery. The auxiliary data recovery logic generates a '0' as the recovered authentication data when the extracted phase of the primary data bit is smaller than $2T_Q$ and generates a '1' if the extracted phase is equal to or larger than $2T_Q$. The recovered authentication data is compared against the locally generated authentication key for security.

B. Circuits Design Considerations

For proper operation, the phase errors of the primary data bit need to be suppressed within $1T_Q$ during the data transmission so that it does not affect the auxiliary data recovery. In this design, the major sources of phase error have been considered, including jitter, frequency drift between TX and RX clocks, and phase mismatch between CANH and CANL cables. Since the TDC in receiver is entirely digital with a time resolution of 40 ns, the error introduced by jitter does not exceed $1T_Q$ if the peak-to-peak jitter is less than 40 ns [4].

As the authentication data is recovered by comparing the phase of bit-transitions to SOF, the impact of the frequency drift varies with the data length. The phase error caused by frequency error accumulates with time during the data transmission. In this CAN bus TRX, the length of auxiliary data is designed as 16 bits, corresponding to a primary data length of 80 bits ($2000T_Q$). To ensure the correctness of the 16-bit auxiliary recovery, the maximum phase error which occurs at the last modulated primary data bit needs to be within $1T_Q$. Hence, the transceiver can tolerate a frequency error up to 0.05% ($1T_Q/2000T_Q$) for any combination of primary data and authentication data.

The phase mismatch can be caused by the length difference between CANH and CANL cable that results in a load (parasitic RC) mismatch. Consequently, the pulse width error may result from such phase mismatch and leads to phase error in the receiver output end. Since the phase information is important for phase extraction circuit to extract the correct auxiliary data, the rail converter has been designed to mitigate the effect of phase mismatch between CANH and CANL.

III. RAIL CONVERTER

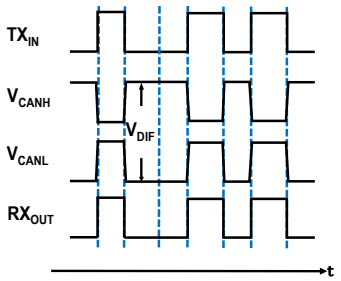


Fig. 3. Transmission waveform of CAN bus transceiver.

A CAN rail converter including a transmitter, and a receiver is introduced in this section. The single-rail CAN data (TX_{IN}) is turned into dual-rail signals V_{CANH} and V_{CANL} by the transmitter. The receiver detects V_{DIF} between V_{CANH} and V_{CANL} and generates a single-rail output RX_{OUT}, as shown in Fig. 3.

A. The Transmitter Circuit

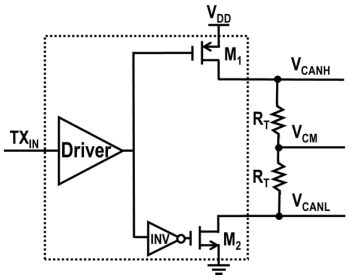


Fig. 4. Conventional CAN dual-rail transmitter.

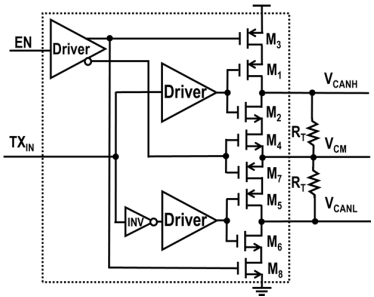


Fig. 5. The CAN dual-rail transmitter with enhanced driving capability.

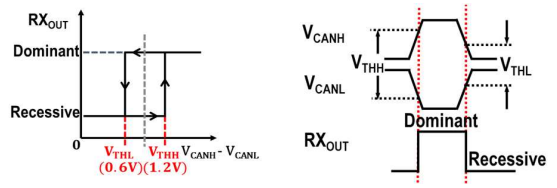
The schematic of the conventional transmitter of CAN bus transceiver is shown Fig. 4. To generate a dominant bit, the driver turns on transistors M_1 and M_2 to fast pull V_{CANH} to V_{DD} and V_{CANL} to GND, while the recessive bit is pulled by the

termination resistors to a common mode voltage V_{CM}. In this topology, the dominant to recessive bit transition speed is determined by the pull up/down resistor 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.

To overcome this limit, the presented rail converter transmitter introduces M_1 and M_6 for dominant bit driving, M_2 and M_5 for recessive bit driving as shown in Fig. 5. The M_3, M_4, M_7 and M_8 are switches controlled by enable signal EN, which disconnect the transmitter from CANH and CANL cables when no data is transmitted. With this design, both recessive-to-dominant and dominant-to-recessive bit transitions can be fast without consuming a large static power.

B. The Receiver Circuit

The receiver realizes a hysteretic comparison of voltage difference between V_{CANH} and V_{CANL} with positive trigger point V_{THH} and negative trigger point V_{THL}, as shown in Fig.6. This hysteretic comparison makes sure the dominant bit and recessive bit are not triggered only by either V_{CANH} or V_{CANL} alone and there is enough voltage margin to avoid false triggering.



(a) (b)

Fig. 6. (a) Hysteretic comparation with V_{THH}, V_{THL} (b) Realization with V_{CANH} and V_{CANL}.

The detailed circuit of receiver is shown in Fig. 7. The comparator introduces two input pairs, M_1 and M_2 in NMOS for V_{CANH} (0.9-1.8V) and M_3 and M_4 in PMOS for V_{CANL} (0-0.9V). Two DC common mode voltage V_{REFH} (1.35V) and V_{REFL} (0.45V) are introduced for voltage comparison. The two input differential pairs compare V_{CANH} and V_{CANL} against V_{REFH} and V_{REFL}, respectively, and then add the corresponding differential current together for hysteretic triggering. The two trigger points are $V_{THH} = V_{REFH}-V_{REFL}+V_{OS}$ and $V_{THL} = V_{REFH}-V_{REFL}-V_{OS}$, where ($V_{REFH}-V_{REFL}$) is equal to 0.9V and V_{OS} has a nominal value of 0.3V, which is decided by the size of M_6, M_7, M_8 and M_9 [5].

As the authentication data is extracted from RX_{OUT}, it is critical to keep the phase (pulse width) of RX_{OUT} to be the same as TX_{IN} regardless of the circuit's nonidealities such as

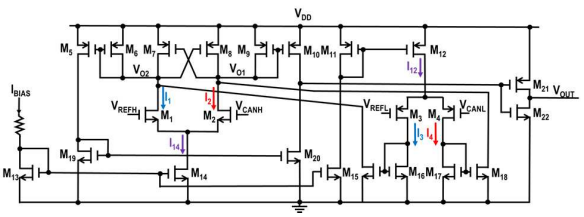


Fig. 7. Schematic of hysteretic dual-to-single receiver.

the PVT variations. With PVT variations on V_{OS}, the triggering points V_{THH} and V_{THL} also vary and may cause timing errors on the rising edge (t_{th}) and falling edge (t_{tl}) of RX_{OUT}. However, since V_{THH} and V_{THL} are always symmetric with respect to 0.9V, the voltage variation on V_{THH} (ΔV_{THH}) is the opposite of that on V_{THL} (ΔV_{THL}). Thus, with the same slope of rising/falling edge due to the balanced driving capability of transmitter, t_{th} and t_{tl} are the same and no errors on the pulse width of RX_{OUT} will be introduced, as shown in Fig. 8(a).

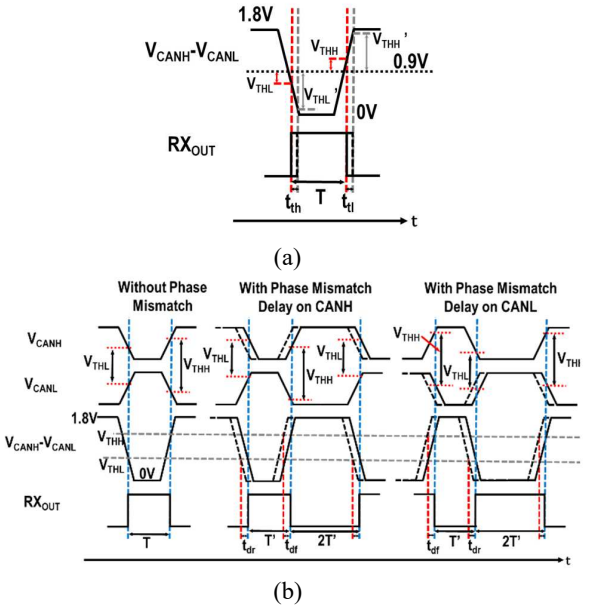
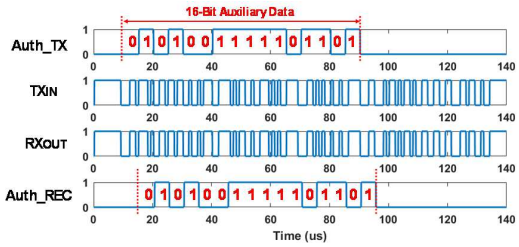


Fig. 8. (a) RX_{OUT}'s pulse width relationship with V_{THH} and V_{THL}, (b) Phase mismatch compensation under different situations.

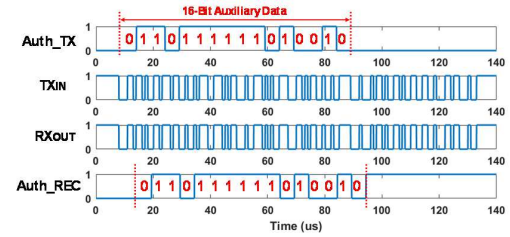
Another nonideal characteristic that may contribute to the phase error on RX_{OUT} is the phase mismatch between CANH and CANL caused by the delay difference. When there is an extra delay on either CANH or CANL line, timing errors t_{dr} and t_{df} on RX_{OUT}'s rising/falling edge are involved. These timing errors are caused by later trigging from the signal with larger delay. Because the triggering requires the corresponding current from both differential input pairs , the bit transition of RX_{OUT} are dominant by that of the later signal in CANH/CANL, resulting in that t_{dr} and t_{df} are equal in the first order. With the ideal (without phase mismatch) pulse width of RX_{OUT} being T, the pulse width with phase mismatch is $T'=T-t_{dr}+t_{df} \approx T$. Thus, the effect of phase mismatch on RX_{OUT}'s pulse width is largely suppressed.

IV. MEASUREMENT RESULTS

The presented CAN transceiver chip is fabricated in 180 nm process. The transceiver communication test is set up by using one chip's TX to send the data packets to another chip's RX through CANH/CANL cables. The measurement results that demonstrate the operation of the CAN bus TRX is shown in Fig. 9. The measured RX_{OUT} maintains the same phase information as the modulated primary data TX_{IN} and the 16-bit extracted auxiliary data (Auth_Rec) matches with the auxiliary data on TX side (Auth_TX) even with +/-0.05% frequency drift between TX and RX, where the frequency drift



(a)



(b)

Fig. 9. Measurement results with frequency drift between TX and RX (a) +0.05% frequency drift, (b) -0.05% frequency drift.

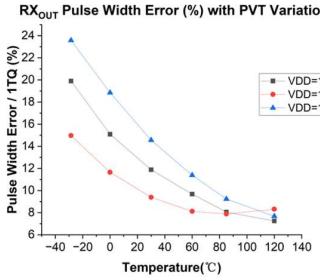
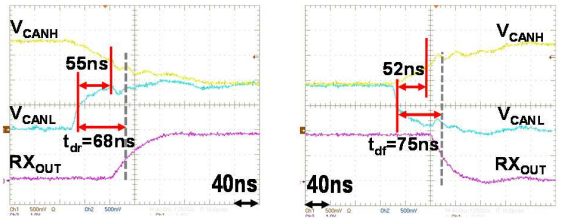


Fig. 10. RX_{OUT} pulse width error with temperature (-28.5℃ to 120℃) and voltage (V_{DD}=1.8V/1.98V/1.62V) variation.

is defined as (f_{TX}/f_{RX}-1). With -0.05% frequency drift, signal Auth_Rec starts to deviate from Auth_TX after the 16-bit extraction, as the accumulated phase error caused by the frequency error starts to exceed $1T_Q$.

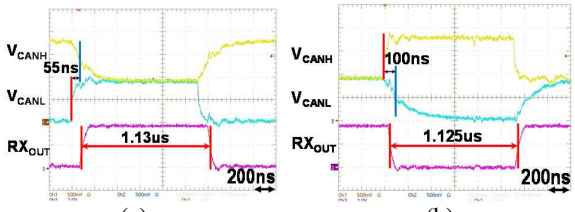
The functionality of the transceiver has been verified in measurement with V_{DD} varying by +/-10% from 1.62V to 1.98V and temperature from -28.5℃ to 120℃. The pulse width error of RX_{OUT} compared to $1T_Q$ (40 ns) is shown in Fig. 10. With voltage and temperature variations, the pulse width error maintains below 25% of $1T_Q$.

Fig. 11 shows the zoomed in waveforms of rising and falling edge of receiver output and V_{CANH}/V_{CANL} with phase mismatch. The phase mismatch between V_{CANH} and V_{CANL} is 50 ns. The measured t_{dr} is 75 ns, t_{df} is 68 ns and the phase error in RX_{OUT} is suppressed to 8 ns.



(a) (b)

Fig. 11. Timing errors with phase mismatch between V_{CANH} and V_{CANL} (a) t_{dr}, (b) t_{df}.



(a) (b)

Fig. 12. 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}.

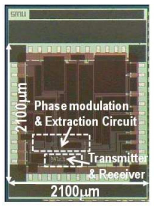


Fig. 13. Chip die photo.

Fig. 12 shows the measured pulse width of RX_{OUT} with phase mismatch between CANH and CANL. The phase mismatch is generated by adding extra RC on V_{CANH} or V_{CANL}. The ideal pulse width of RX_{OUT} is 1 us+$3T_Q$ (1.12 us) because of phase modulation. With 55 ns/100 ns phase mismatch on CANH/CANL, the error on RX_{OUT}'s pulse width is only 10 ns/5 ns. Hence, the effect of phase mismatch on RX_{OUT}'s pulse width is largely suppressed.

The chip die photo is shown in Fig. 13. A total of ten CAN transceiver ICs has been tested and they demonstrated consistent results which validate the presented CAN bus transceiver architecture and circuits. Moreover, the rail converter has been verified with delay mismatch as well as voltage and temperature variations.

V. SUMMARY

This paper presents a CAN bus transceiver with rail converters. The transceiver incorporates phase modulation to provide auxiliary data for authentication without introducing an extra data channel. The transmitter of the rail converters have enhanced rising/ falling edge and the receiver provides the capability to largely suppress the phase error caused by PVT variations of the circuit design and the phase mismatch between CANH and CANL. Extensive measurement results again PVT and mismatches demonstrates the effectiveness of the presented CAN bus transceiver architecture for secure communication within a real CAN bus system.

REFERENCES

[1] S. Checkoway et. al, "Comprehensive Experimental Analysis of Automotive Attack Surfaces," in 20th USENIX Security Symposium, August 2011, pp. 77-92.

[2] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," in Blackhat 2015, August 2015, pp. 1-91.

[3] NXP, TJA115x fact sheet "https://www.nxp.com/docs/en/fact-sheet/SECURCANTRLFUS.pdf " 2022.

[4] Wen, X., Hua, R., Liu, J., Fu, T., Fang, L., Wang, X., Thornton, M. and Gui, P., "Controller Area Network (CAN) Bus Transceiver with Authentication Support," 2022 IEEE International Symposium on Circuits and Systems (ISCAS), Austin, TX, USA, 2022, pp. 1328-1331.

[5] Phillip E. Allen, CMOS Analog Circuit Design, 3rd ed., Elsevier, 2011, pp.483–485.