Controller Area Network (CAN) Bus Transceiver with Authentication Support

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

Ruobing Hua
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
rhua@smu.edu

Jianye Liu
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
jianyel@smu.edu

Tao Fu
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
tfu@smu.edu

Liang Fang
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
lfang@smu.edu

Xiaoran Wang
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
xiaoranw@smu.edu

Mitch Thornton
Electrical and Computer Engineering
Southern Methodist University
Dallas, United States
mitch@lyle.smu.edu

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

***Abstract*—A new CAN bus transceiver integrated circuit is described that incorporates an inherent auxiliary data channel. The auxiliary data channel enables CAN packet authentication signatures to accompany primary data payloads. The transceiver is backward compatible with the CAN protocol and thus may be used within existing networks with no modifications required. The clock edge at the transmitter is phase modulated with signature data in a manner that does not exceed clock jitter tolerances in the CAN specifications. The receiver is designed to recover the primary data and the packet signature. By comparing the received signature with the authorized packet signature, a "Go/No Go" output indicates if the received packet is properly authenticated.**

Keywords— automotive security, packet authentication, CAN bus transceiver

I. Introduction

The Controller Area Network (CAN) protocol is widely used in the automotive industry and in other control system applications. Because the CAN protocol was devised for use in systems that are physically isolated, security concerns were not emphasized. However, vulnerabilities and threats have been shown to exist in CAN-based systems [1]. In particular, the demonstration of a remote exploitation attack targeting an unaltered 2014 Jeep Cherokee increased attention regarding security vulnerabilities of the CAN bus [2].

There are several approaches being actively investigated to secure the CAN bus. Many of these approaches involve changes to the CAN bus protocol, hardware modifications and augmentations, or both. One approach is the incorporation of cryptographic methods within the CAN network such as the inclusion of HMACs or AES encryption typically requiring additional hardware resources [3][4][5]. Other approaches include software-layer approaches such as dynamic ID virtualization within the CAN bus packet structure [6], Electronic Control Unit (ECU) fingerprinting using unique characteristics of transmitted signals at the physical layer [7], CAN packet timing analyses [8][9][10][11], and authentication of ECU network nodes [12] or CAN bus packets [13][14][15][16].

A key challenge among the various methods of securing the CAN bus is to preserve interoperability with unequipped systems and to maintain compatibility with the CAN bus standard. The addition of cryptographic methods generally requires significant modifications to the hardware and/or software infrastructure that can affect overall cost and timing requirements. Timing analyses require additional processing and the use of statistical and classification approaches can result in non-zero type I and type II error rates. We describe a CAN packet authentication approach that avoids cryptographic methods, preserves interoperability with unequipped systems, and that only requires a modification to the CAN bus transceiver circuitry as inspired from earlier work in authenticating high-speed asynchronous serial data communications protocols [17].

The authentication approach in [13] requires the implementation of a hash chain data structure and a secure seed distribution method among the ECUs whereas our approach does not require such data structures or seed distribution protocols. The authentication approach in [14] is motivated by a client-server architecture and proposes incorporation of a secret key into each ECU during manufacture or at trusted facilities, such as using a physical unclonable function (PUF), with a corresponding authentication process that involves the establishment of shared keys during system initialization. The authentication approach in [15] makes use of probabilistic Bloom filters with associated hash functions. The authentication approach of [16] utilizes voltage differences among the differential CAN bus signals due to electronic

imperfections during the transition of bits from a logical "one" to "zero."

Our approach differs from the above techniques in that we do not require the incorporation of key distribution protocols, hash filters, Bloom filters, protocol modifications, or exploitation of manufacturing differences in components through the use of a PUF or voltage measurement approach. Rather, we incorporate an auxiliary data channel within the CAN protocol that maintains backward compatibility with existing unequipped systems. The auxiliary channel enables a unique signature to accompany each CAN bus packet such that each received packet can be authenticated by validating the correct signature is present on the concurrent auxiliary channel. The method is implemented through an architectural change within the CAN bus transceiver circuitry. The transceiver is thus capable of producing a "Go/No Go" signal to indicate if the received packet is trustworthy.

More specifically, an inherent auxiliary communication channel is implemented in the primary data stream by modulating the data stream in the time (phase) domain as motivated by the previous work in [17]. The authentication signature is then transmitted and received simultaneously over the inherent auxiliary channel along with the primary data stream to support authentication on the receiver end. The unique aspect of the time-domain modulated primary data is that it appears to be tolerated noise levels to unequipped receiver devices, thus rendering it operable with existing CAN transmitter and receiver devices. In contrast to the previous work in [17], we utilize a time-to-digital converter (TDC) in the packet receiver rather than a PLL-based secondary clock recovery circuit.

II. TRANSCEIVER ARCHITECTURE

The CAN message and the block diagram of proposed CAN transceiver is shown in Fig. 1. In the transmitter (TX), the phase of the primary data is modulated based on the authentication data transmitted on the secondary channel. The receiver (RX)

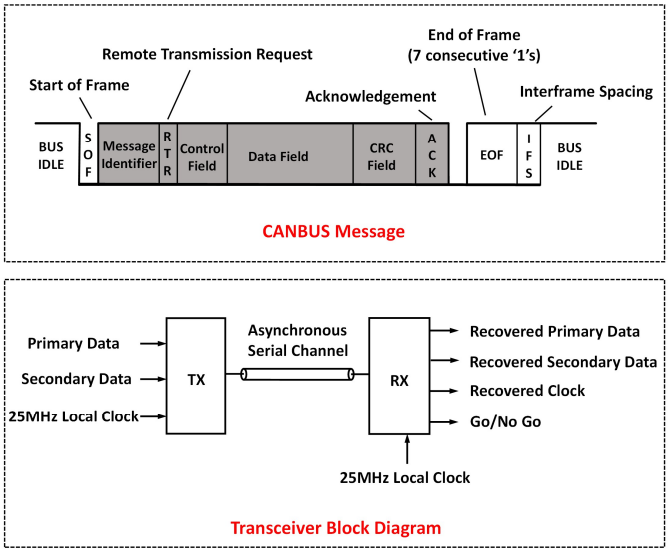

Fig. 1. CANBUS communication and transceiver block diagram

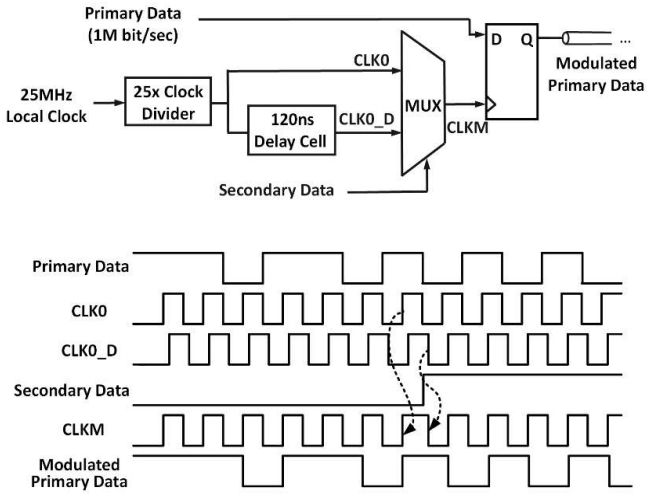

Fig. 2. CAN Bus Transmitter block diagram and timing diagram

recovers not only the primary data, but also the authentication signature by extracting the phase information in the primary data.

The serial CAN bus can operate up to 1Mb/s asynchronously. The TX block diagram is illustrated in Fig. 2. Within each data bit, up to 25 time quanta (TQ) can be chosen to provide finer time resolution (*i.e.* 40ns) for synchronization purposes within the RX. To implement phase modulation of the TX primary data, three TQs are chosen as the phase difference in the primary data bits, controlled by authentication data being '1' or '0'. A 25MHz local clock is used as the system clock that is divided by 25 to generate the 1MHz clock CLK0 that synchronizes with the 1Mb/s primary data. CLK0_D is generated by delaying CLK0 by 3 TQ, or 120ns. Based on the secondary data being '1' or '0', the D flip-flop either selects CLK0 or CLK0_D to re-sample the primary data and generate the modulated primary data as shown in the timing diagram. In the CANBUS communication protocol, the number of consecutive '1's or '0's in data cannot be more than 5. The frequency of secondary data is chosen to be 5 times smaller than

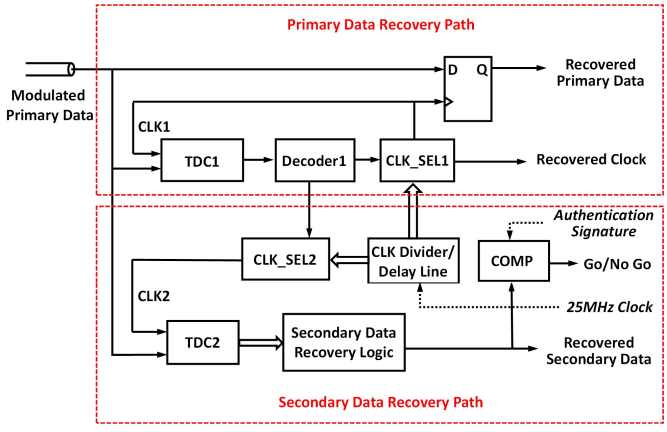

Fig. 3. CAN Bus Receiver block diagram

the primary data. so that there is at least one data transition in every 5 primary data bits. This allows the secondary data to be recovered in the RX by detecting the phase of the bit-transitions. Moreover, to avoid transmitting the signature from TX and RX, in this prototype we choose to simply use the first 8 bits of the primary data as the authentication signature, while other more sophisticated signature generators can be implemented for on-chip authentication signatures in operational versions.

The RX consists of a primary data recovery path and a secondary data recovery path, as shown in Fig. 3. In order to produce a clock for synchronization with the modulated primary data, 25 1MHz clocks with 40ns time spacing are generated by a clock divider and a delay line for clock selection. A clock selection block (CLK_SEL1) selects one of the 25 clocks and generates CLK1 to sample the modulated primary data. A TDC (TDC1) with a 40ns resolution is used to detect the time difference between CLK1 and the modulated primary data and then it adjusts CLK_SEL1 through Decoder1 to keep CLK1 at the optimal sampling point of the received data. In the secondary data recovery path, another TDC (TDC2) is implemented to detect the time difference between CLK2 and the modulated primary data. Based on the output of TDC2, the phase information of the modulated primary data is extracted, and the secondary data (the authentication signature) is recovered.

The operation of the RX is illustrated in the RX timing diagram as shown in Fig. 4. When the RX detects the start of frame (SOF), which is the first '1' to '0' transition in the data package, TDC1 starts to update CLK_SEL1 to keep the falling edges of CLK1 aligned with the edges of the modulated primary data when it detects a misalignment in between, which means the rising edges of CLK1 is good for sampling the primary data. In the secondary data recovery path, TDC2 uses CLK2 as the reference clock to extract the phase modulation on primary data, where CLK2 is generated by the CLK_SEL2 that aligns with the SOF. Once the phase modulated word serving as the authentication signature has been extracted and recovered by TDC2 and Secondary Data Recovery Logic, a comparator (COMP) compares it with the first 8 bits of the recovered primary data (which is used as the default authentication

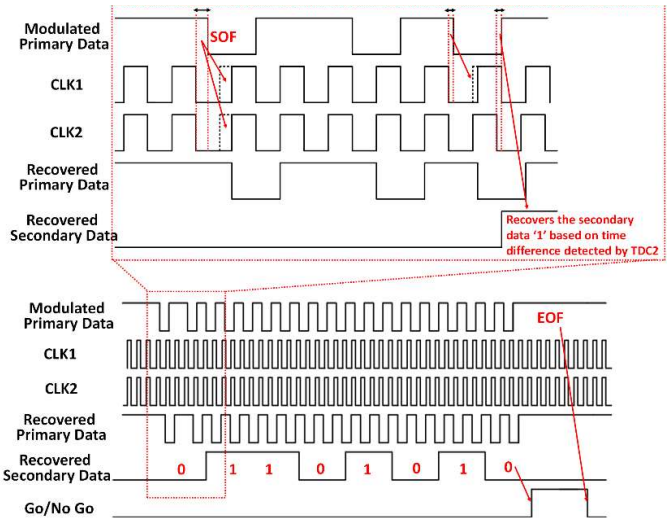

Fig. 4. CAN Bus Receiver timing diagram

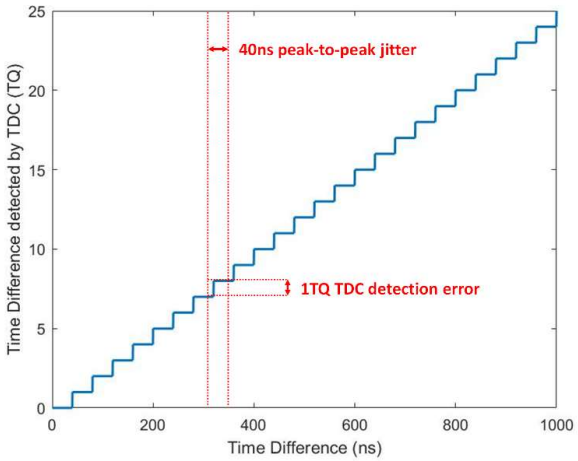

Fig. 5. Input time difference v.s. TDC detected time difference

signature in our prototype) to indicate whether the authentication is verified.

To successfully recover the secondary data, it is essential that the RX have the ability to recover the phase modulated signature in the presence of jitter. Because the proposed receiver is entirely digital with a 40ns time resolution, the error of the TDC output caused by jitter will not exceed 1TQ as long as the peak-to-peak jitter of the entire transmission chain is less than 40ns, regardless of the initial phase of the modulated primary data as shown in Fig. 5. The phase modulation index is chosen as 3TQ, so that even with 1TQ TDC detection error, the Secondary Data Recovery Logic can still properly extract the phase modulated signature word.

III. Measurement Results

The measured eye diagrams on both the TX and RX outputs are shown in Fig. 6. Different from a conventional eye diagram with eye width equal to 1us of a 1Mbit/s TX, the phase of the TX data is modulated by the secondary data, creating a 3TQ time difference, as evident in top diagram in Fig. 6. On the RX side, although the overall jitter causes 1TQ shift in the TDC detection, there is still a 2TQ spacing between different phase modulated symbols, allowing the RX to correctly extract the secondary data embedded in the primary data. The measured jitter of the modulated primary data and recovered primary data is 1.9ns and 2.0ns respectively, which are much smaller than the 40ns peak-to-peak jitter tolerance.

The transceiver is fabricated in a 0.18µm CMOS process. The core circuit occupies an area of 0.1mm^2 and consumes 3mW of power at 1.8V as shown in Fig. 7. The presented authentication transceiver scheme can be incorporated into both synchronous or asynchronous baseband data transmission schemas and still fall within the specified transceiver jitter budgets while requiring no protocol or standard modifications. The proposed security enhancing communication circuit is interoperable with non-equipped transceivers, where the primary data streams may be properly received by non-equipped devices that are pin-for-pin compatible with enhanced devices.

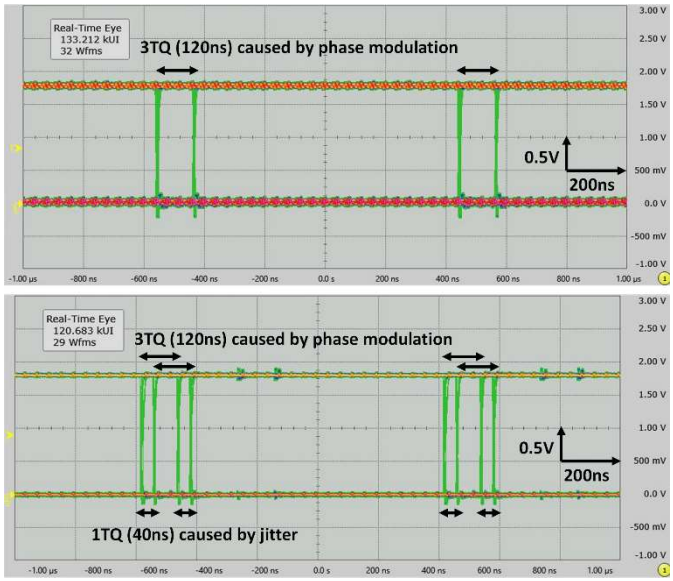

Fig. 6. Measured eye diagrams of modulated primary data (top) and recovered primary data (bottom)

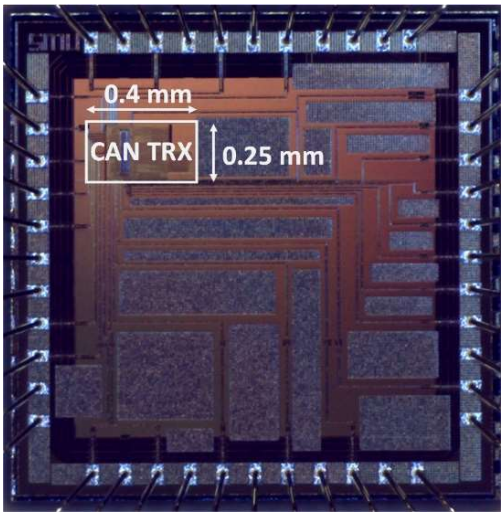

Fig. 7. Die Photograph of the secure CAN Bus transceiver

IV. Summary of Contribution

We have devised, designed, implemented, and characterized the performance of a secure CAN bus transceiver in a 0.18 µm CMOS process. CAN bus security is provided through packet signature authentication wherein an auxiliary channel is implemented by phase modulating the primary data stream. The modulation indices are chosen to remain within the phase jitter tolerances of the CAN standard, thus the technique is backward compatible with existing non-equipped systems.

References

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

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

[3] A. Maruaisap and P. Kumhom, "A hardware-based security scheme for in-vehicle CAN,"in proc., International Computer Science and Engineering Conference (ICSEC), 2016, pp. 1-5

[4] Y. Wu, Yeon-Jin Kim, Zheyan Piao, J. Chung and Yong-En Kim, "Security protocol for controller area network using ECANDC compression algorithm," in proc., IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), 2016, pp. 1-4.

[5] H. Mun, K. Han and D. H. Lee, "Ensuring Safety and Security in CAN-Based Automotive Embedded Systems: A Combination of Design Optimization and Secure Communication," IEEE Transactions on Vehicular Technology, vol. 69, no. 7, July 2020, pp. 7078-7091.

[6] H. Sun, S. Y. Lee, K. Joo, H. Jin and D. H. Lee, "Catch ID if You CAN: Dynamic ID Virtualization Mechanism for the Controller Area Network," IEEE Access, vol. 7, 2019, pp. 158237-158249.

[7] O. Avatefipour, A. Hafeez, M. Tayyab and H. Malik, "Linking received packet to the transmitter through physical-fingerprinting of controller area network,"in proc., IEEE Workshop on Information Forensics and Security (WIFS), 2017, pp. 1-6.

[8] H. M. Song, H. R. Kim and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network,"in proc., International Conference on Information Networking (ICOIN), 2016, pp. 63-68.

[9] X. Ying, S. U. Sagong, A. Clark, L. Bushnell and R. Poovendran, "Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 9, Sept. 2019, pp. 2300-2314.

[10] J. Sunny, S. Sankaran and V. Saraswat, "A Hybrid Approach for Fast Anomaly Detection in Controller Area Networks," in proc., IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2020, pp. 1-6.

[11] S. Jin, J. -G. Chung and Y. Xu, "Signature-Based Intrusion Detection System (IDS) for In-Vehicle CAN Bus Network," in proc., IEEE International Symposium on Circuits and Systems (ISCAS), 2021, pp. 1-5.

[12] K. Jeong, E. Shin, H. Kim and K. -C. Lee, "Implementation of Node Authentication Algorithm of In-Vehicle Network in Connected Car," in proc., IEEE International Conference on Industrial Technology (ICIT), 2019, pp. 1605-1609.

[13] K. Kang, Y. Baek, S. Lee and S. H. Son, "Lightweight Authentication Method for Controller Area Network,"in proc., IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA), 2016, pp. 101-101.

[14] A. S. Siddiqui, Y. Gui, J. Plusquellic and F. Saqib, "Poster: Hardware based security enhanced framework for automotives,"in proc., IEEE Vehicular Networking Conference (VNC), 2016, pp. 1-2.

[15] T. Lenard, R. Bolboacă, B. Genge and P. Haller, "MixCAN: Mixed and Backward-Compatible Data Authentication Scheme for Controller Area Networks," in proc., IFIP Networking Conference (Networking), 2020, pp. 395-403.

[16] O. Schell and M. Kneib, "VALID: Voltage-Based Lightweight Intrusion Detection for the Controller Area Network,"in proc., IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 225-232.

[17] 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 TVLSI*, vol. 28, no. 1, Jan. 2020, pp. 12-22.