2022-01-0119 Published 29 Mar 2022

Managing Trust Along the CAN Bus

Alan J. Michaels, Michael Fletcher, and Chris Henshaw Virginia Tech National Security Institute

Venkata Sai Srikar Palukuru and John Moore Ford Motor Company

Citation: Michaels, A.J., Fletcher, M., Henshaw, C., Palukuru, V.S.S. et al., "Managing Trust Along the CAN Bus," SAE Technical Paper 2022-01-0119, 2022, doi:10.4271/2022-01-0119.

Received: 18 Jan 2022 Revised: 18 Jan 2022 Accepted: 17 Jan 2022

Abstract

Multiple approaches have been created to enhance intra-vehicle communications security over the past three decades since the introduction of the Controller Area Network (CAN) protocol. The twin pair differential-mode communications bus is tremendously robust in the face of interference, yet physical access to the bus offers a variety of potential attack vectors whereby false messages and/or denial of service are achievable. This paper evaluates extensions of a Physical-layer (PHY) common-mode watermark-based authentication technique recently developed to improve authentication on the CAN bus by considering the watermark as a side-channel communications means for high value information. We also propose and analyze higher layer algorithms, with benefits and pitfalls, for employing the watermark as a physical-layer firewall. All of these results are backed by a software-defined radio (SDR) based hardware testbed that verifies backwards compatibility with commercial CAN transceivers and efficacy of the watermark-based authentication.

Introduction

Over the past 2.5 years, our team conceived and have implemented an improved watermark-based CAN transceiver [1, 2] that validates the potential of a time-evolving spread spectrum underlay signal that is inserted with a CAN message to help authenticate the origin of the message. This Direct Sequence Spread Spectrum (DSSS) pulse is used as an indicator that self-synchronizes to the non-synchronous CAN frame. Further, the authentication pulse is injected in the common mode path as a low-level noise signal: 1-4% of the voltage variations in the standard differential mode CAN signaling, or 25-100 mV relative to a 5V bus. This pulse is then reconstructed coherently into the original pulse via knowledge of the underlying spreading code. By virtue of the natural interference mitigation properties of DSSS signals [3], the additive DSSS signal is also effective at filtering out both common and differential mode noise during despreading.

A variety of watermark-based solutions are evident in the literature, with dominant interest in file-based or medium access control (MAC) layer techniques that are typically treated as being synonymous with *fingerprinting* [4, 5]. The proposed watermark, while performing the same authentication function, is more closely aligned with a PHY-layer wireless side channel technique, yet no prior know demonstration exploits the embedded signaling on a two-wire differential bus like CAN. Previous side-channel techniques [6] employ a variety of methods such as MAC-layer authentication using cryptographic techniques [7], one-way hash functions or signatures [8], signatures based on physically random hardware events [9], signals operating on distinct frequency bands [10, 11], exploitation of physical proximity via side channels limited to near-field communications [12], and direct fingerprinting of hardware-based nonidealities [13, 14]. More recent techniques [15] have applied structured cryptographic handshakes to ensure sufficient levels of network-wide trust for CAN.

As implemented, the watermark operates on a two-wire CAN bus, so maintains physical isolation of its *side* channel; the addition of the common mode watermark is both small relative to the primary signal and effectively filtered out by the differential receiver. It should be noted however that the common mode path has a natural disadvantage within the vehicle in that most of the ambient noise that is coupled onto the bus is mitigated to the differential receiver by virtue of twisted pair wiring between nodes, while the common mode path will inherit that full effect and thus must use a naturally interference mitigation waveform like BPSK-DSSS. A companion paper [16] describes the stress testing of the watermarking CAN transceiver, while this paper begins to narrow in on how the watermark may be adapted to yield adaptive data throughputs beyond the single authentication pulse and how the authentication decisions from individual frames may be aggregated into network-level trust metrics.

The interest in extending the data throughput of the watermark is two-fold: first is the ability to transfer high value information such as cryptographic keys in a way that is mostly imperceptible to commercial transceivers, and the second is to simultaneously integrate in secondary, yet still low latency, MAC-layer authentication such as a message hash. This excess critical, but still important device, then method 3 could be used to consciously accept messages, but only if the number of flags raised are below the second threshold set. The system would still acknowledge the messages but only until the assurance level is above the assurance threshold would it pass the messages to the host. If too many suspicious messages arrive, the device could be kicked from the CAN bus or forced to re-establish trust. For the least critical devices on the bus, method 3 could be used with the caveat of resetting the assurance level to a base line value periodically to maximize the detection of false messages. Using all of these methods in conjunction would allow the bus to have a multilayered authentication system, depicted in Figure 8.

Summary/Conclusions

Recent developments in stress testing our prototype watermarking CAN transceiver [16] presents the viability of adapting the hardware concept to implement a side-channel communications link via the watermark signal. The specific examples of data throughput in terms of cryptographic seeds and message hashes for tamper/error detection were discussed, presented as a novel information-additive approach to enable desirable security features along the CAN bus. This paper also analyzed extensions of the baseline MAC-layer design for interpreting the presence of the valid watermark, detailing advantages and disadvantages for the identified methods. In all such cases, the watermarking approach extends beyond the single authentication pulse to be aggregated into network-level trust metrics.

References

1. Michaels, A., Palukuru, S., Henshaw, C., Fletcher, M., et. al., "CAN Bus Message Authentication via Co-Channel RF Watermark," *IEEE Transactions on Vehicular Technology*, 2022. 10.1109/TVT.2022.3143708.
2. Michaels, A., Palukuru, S., Moore, J., and Lawlis, J., "CAN Bus Message Authentication via Co-Channel Common Mode Signal RF Watermark," U.S. patent application (Ford 84323375).
3. Xu, X., Zhou, S., Sun, H., Morozov, A.K. and Zhang, Y., "Impulsive Noise Suppression in Per-Survivor Processing Based DSSS Systems," 2014 Oceans - St. John's, 2014, pp. 1-5, doi:10.1109/OCEANS.2014.7003245.
4. Boreiry, M. and Keyvanpour, M., "Classification of Watermarking Methods Based on Watermarking Approaches," in *2017 Artificial Intelligence and Robotics (IRANOPEN)*, 2017, pp. 73-76, doi:10.1109/RIOS.2017.7956446.
5. Cox I.J., Kilian J., Leighton F.T. and Shamoon T., "Secure Spread Spectrum Watermarking for Multimedia," in *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, Dec. 1997, doi:10.1109/83.650120.
6. Dadam, S.R., Zhu, D., Kumar, V., Ravi, V. and, Palukuru V.S.S., "Onboard Cybersecurity Diagnostic System for Connected Vehicles," SAE Technical Paper 2021-01-1249, 2021, doi:10.4271/2021-01-1249.
7. Perazzone J.B., Yu P.L., Sadler B.M. and Blum R.S., "Cryptographic Side-Channel Signaling and Authentication via Fingerprint Embedding," in *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2216-2225, Sept. 2018, doi:10.1109/TIFS.2018.2812202.
8. Alshudukhi, J.S., Mohammed, B.A., and Al-Mekhlafi, Z.G., "An Efficient Conditional Privacy-Preserving Authentication Scheme for the Prevention of Side-Channel Attacks in Vehicular Ad Hoc Networks," *IEEE Access* 8 (2020): 226624-226636, doi:10.1109/ACCESS.2020.3045940.
9. Lee H., Juvekar C.S., Kwong J. and Chandrakasan A.P., "A Nonvolatile Flip-Flop-Enabled Cryptographic Wireless Authentication Tag With Per-Query Key Update and Power-Glitch Attack Countermeasures," in *IEEE Journal of Solid-State Circuits*, vol. 52, no. 1, pp. 272-283, Jan. 2017, doi:10.1109/JSSC.2016.2611678.
10. Calhoun T.E., Newman R. and Beyah R., "Authentication in 802.11 LANs Using a Covert Side Channel," in *2009 IEEE International Conference on Communications*, 2009, pp. 1-6, doi:10.1109/ICC.2009.5198769.
11. Goergen, N., Clancy, T.C., and Newman, T.R., "Physical Layer Authentication Watermarks through Synthetic Channel Emulation," *IEEE Symposium on New Frontiers in Dynamic Spectrum (DySPAN)* 2010 (2010): 1-7, doi:10.1109/DYSPAN.2010.5457897.
12. Matos A., Romão D. and Trezentos P., "Secure Hotspot Authentication Through a Near Field Communication Side-Channel," in *2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2012, pp. 807-814, doi:10.1109/WiMOB.2012.6379169.
13. McGinthy J., Wong L., Michaels A., Groundwork for Neural Network-Based Specific Emitter Identification Authentication for IoT, *IEEE Internet of Things Journal*, Vol. 6, Iss. 4, Print ISSN: 2327-4662, pp. 6429-6440, August 2019. doi:10.1109/JIOT.2019.2908759.
14. Chatterjee B., Das D., Maity S. and Sen S., "RF-PUF: Enhancing IoT Security Through Authentication of Wireless Nodes Using In-Situ Machine Learning," in *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 388-398, Feb. 2019, doi:10.1109/JIOT.2018.2849324.
15. Pesé M.D., Schauer J.W., Li J., and Shin K.G., *S2-CAN: Sufficiently Secure Controller Area Network* in *2021 Annual Computer Security Applications Conference (ACSAC)*, https://doi.org/10.1145/3485832.3485883.
16. Michaels, A., Palukuru, S., Fletcher, M., Henshaw, C. et al., *Robustness Testing of a Watermarking CAN Transceiver*, (SAE World Congress, 2022).
17. Fletcher M.J., Gaeddert J.D. and Michaels A.J., "Physical Layer Firewall Design using Co-Channel Underlay-Based Watermark Authentication," in *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*, 2019, pp. 453-457, doi:10.1109/MILCOM47813.2019.9020952.
18. Red Pitaya Software Defined Radios, https://redpitaya.com/.

19. NXP: "MPC574xB-C-G: Ultra-Reliable MCUs for Automotive and Industrial Control and Gateway," https://www.nxp.com/products/processors-and-microcontrollers/power-architecture/mpc5xxx-microcontrollers/ultra-reliable-mpc57xx-mcus/ultra-reliable-mcus-for-automotive-and-industrial-control-and-gateway:MPC574xB-C-G?tid=vanMPC5748G.
20. Microchip ATSAME54-XPRO: "SAM E54 Xplained Pro Evaluation Kit," https://www.microchip.com/en-us/development-tool/atsame54-xpro.
21. McGinthy J. and Michaels A., Session Key Derivation for Low Power IoT Devices, IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity), in *IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, pp. 194-203, 2018.
22. McGinthy J. and Michaels A., Further Analysis of PRNG-based Key Derivation Functions, *IEEE Access*, Dec 2019. Vol. 7, Iss. 1, pp. 95978-95986. Print ISSN: 2169-3536. DOI:10.1109/ACCESS.2019.2928768.
23. Michaels A.J., "Improved RNS-based PRNGs," In *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018)*. ACM, New York, NY, USA, Article 20, 5 pages. https://doi.org/10.1145/3230833.3232806.
24. Arikan E., "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," in *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051-3073, July 2009, doi:10.1109/TIT.2009.2021379.
25. Xiao S. and Boncelet C.G., "Efficient Noise-Tolerant Message Authentication Codes Using Direct Sequence Spread Spectrum Technique," in *2006 40th Annual Conference on Information Sciences and Systems*, 2006, pp. 1640-1644, doi:10.1109/CISS.2006.286398.
26. Nowdehi N., Lautenbach A. and Olovsson T., "In-Vehicle CAN Message Authentication: An Evaluation Based on Industrial Criteria," in *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*, 2017, pp. 1-7, doi:10.1109/VTCFall.2017.8288327.

Definitions/Abbreviations

AWGN - Additive White Gaussian Noise

BPSK - Bi-Phase Shift Keying

CAN - Controller Area Network

CAN ID - 11-symbol identifier frame near the front of a CAN message

Common Mode - Electrical signals that appear simultaneously on both the CAN-HI and CAN-LO lines of the CAN bus

COTS - Commercial Off-The-Shelf

DC - Direct Current

Differential Mode - Electrical signals that appear either on a single line of the CAN bus or that are injected in opposing directions

DSSS - Direct Sequence Spread Spectrum

EMC - Electromagnetic Compatibility

EMI - Electromagnetic Interference

FEC - Forward Error Correction

FMC - Ford Motor Company

FPGA - Field Programmable Gate Array

IoT - Internet of Things

MAC - Medium Access Control layer

NAQ - Negative acknowledgement

PHY - Physical Layer

PRNG - Pseudorandom Number Generator

Red Pitaya - Low-cost SDR platform [16]

RF - Radio frequency

SDR - Software Defined Radio

SNR - Signal-to-Noise Ratio

TRANSEC - Transmission Security.

Positions and opinions advanced in this work are those of the author(s) and not necessarily those of SAE International. Responsibility for the content of the work lies solely with the author(s).

ISSN 0148-7191