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


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 despread.

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


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