IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 December 2023, accepted 24 December 2023, date of publication 26 December 2023, date of current version 4 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3347541

RESEARCH ARTICLE

Jitter-Based Authentication for Automotive Wireline Networks

SYDNEY LANG, (Graduate Student Member, IEEE), AND TAWFIQ MUSAH, (Senior Member, IEEE)
Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA
Corresponding author: Tawfiq Musah (musah.3@osu.edu)

ABSTRACT This paper proposes a new authentication approach targeted to wireline broadcast communication systems for automotive and industrial applications. The proposed approach leverages jitter amplification in wireline channels, that become stronger features for message-source authentication with higher data rate or channel loss, to provide a low-overhead physical layer authentication. The fundamentals of jitter amplification are reviewed and the use of it as a feature for authentication while maintaining high signal integrity is explored. Simulations using a Simulink model of an example automotive link with multiple electronic control units (ECUs) are used to show the efficacy of the proposed message source authentication scheme. The simulation results also show significant resilience of the proposed approach to noise. Measurement results using a bench-top setup show that the proposed feature detection approach has a high degree of authentication accuracy in a real-time application and provides a low-cost alternative to prevailing software-based approaches.

INDEX TERMS Authentication, broadcast networks, wireline communication, physical layer security, timing noise, wireline transceiver.

I. INTRODUCTION

The proliferation of driver assistance features and the quest for level 5, fully autonomous driving has led to a steep rise in data rate demand in automotive wireline networks. Automotive physical layer (PHY) standards are proposing 16Gbps rates in a few years, with a roadmap to 32Gbps and 48Gbps shortly thereafter [1]. Unlike the current control area network (CAN) bus which has no native security features, security on the future automotive network bus is an important consideration because of expanded potential for unauthorized safety-critical access and the extent of damage such breaches could cause [2], [3], [4], [5], [6], [7]. One option for meeting the high data rate and security requirements is to use Ethernet for its bandwidth and its native IPSec protocol for security [8]. However, this approach comes at the cost of added latency and increased computing complexity and overhead requirements for sensors and electronic control units (ECUs) that make it ill-suited to future automotive wireline networks. Moreover, the broadcast and dynamic nature of the automotive network bus makes the traditional key distribution and collision arbitration onerous to implement [9].

There has been a wide array of non-cryptographic authentication approaches using the PHY layer characteristics in the wireless space. Given the spatial diversity in wireless systems, accurate channel estimations could be used to provide message source authentication. Demonstrated channel estimation schemes include the use of pilot tones in orthogonal frequency-division multiplexing (OFDM) [10], circuit characteristics combined with channel response [11] and reconfigurable transmit antennas [12]. Other authentication approaches use deep learning [13], [14] to detect change in the channel condition and thus provide intrusion detection. However, these schemes do not translate well to wireline links because of detection complexity.

Researchers have attempted to implement intrusion detection systems (IDS) on automotive networks by focusing on extracting several inherent physical properties of the wireline signal itself using machine learning. Using existing

The associate editor coordinating the review of this manuscript and approving it for publication was Shadi Alawneh.

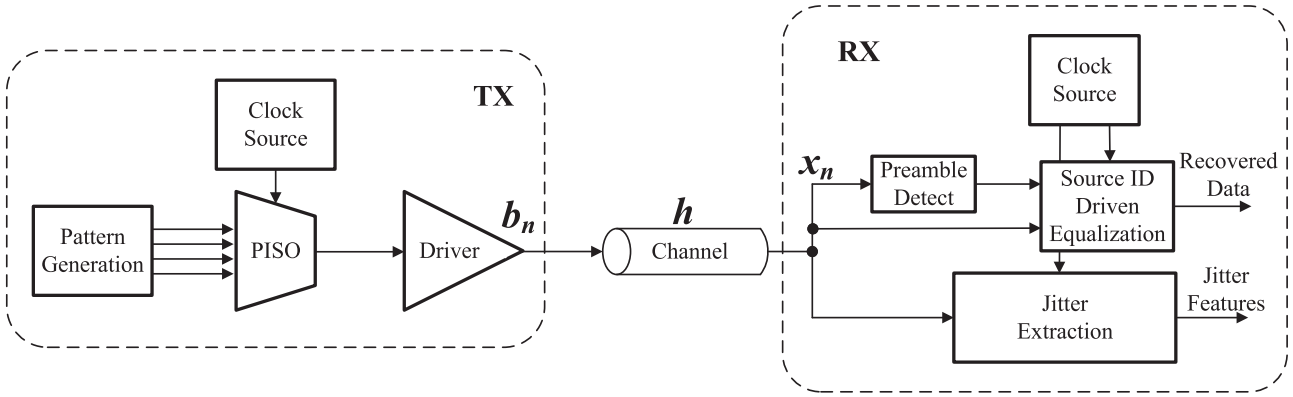

FIGURE 1. A wireline transceiver block diagram showing receiver jitter extraction using source ID driven equalization.

CAN bus, frame arrival times [15], [16], ECU clock frequencies [17] and other CAN specification parameters like worst-case response times [18] or cumulative frame arrival time residuals [19] have been used as fingerprinting signatures. Some IDS schemes have used the power spectrum of the CAN network [20] or the dominant state voltage level in addition to the rise/fall times entering and exiting the state [21], [22], [23]. Other demonstrated IDS schemes used the step response of the received signal [24], [25] and steady-state voltage of received signal [26]. All these IDS schemes have shown high accuracy when multiple features and a large number of message frames are used in the machine learning (ML) driven detection. However, more features indicate increased computation complexity while a large number of frames translates to slow detection. Moreover, these IDS approaches are not native to the CAN design and may not scale to future networks where detection speed and overhead will be critically important.

In this paper, a jitter-based authentication scheme that relies on a well-characterized feature and seamlessly integrates with the automotive wireline network with zero bandwidth overhead is proposed. The proposed approach uses device timing noise variation coupled with channel-based noise amplifications to guarantee message source distinguishability. To improve the resilience of the proposed approach to spoofing and replay attacks, a collaborative receiver authentication (CRA) approach where a couple of receivers are used in source authentication is also proposed.

The bit-wise jitter measurement enables single frame feature extraction and authentication. Thus the proposed approach is extremely fast compared to other schemes that extract features over 10s or 100s of frames. Moreover, the jitter used is predictably amplified by channel loss, making the proposed approach more sensitive to ECU locations and thus guaranteeing stronger security. This allows just a single feature to be used for message-source ID with high accuracy and lead to simple detection and low hardware overhead. Finally, the proposed CRA approach guarantees robustness against masquerade and replay attacks beyond what could be achieved with single point detection.

The paper is organized as follows. Section II reviews jitter fundamentals and its dependence on channel loss and data pattern. Section III introduces the use of jitter for message source authentication and its application for authentication in automotive wireline networks. The proposed multi-point detection scheme and its impact on authentication accuracy are discussed in Section IV. Conclusions are included in Section V.

II. JITTER IN WIRELINE LINKS

Consider the transmitter (TX) of the simplified wireline transceiver of Fig. 1. The parallel input data is serialized using the transmitter clock before being driven onto the channel. Any timing noise or jitter on the clock will be captured by the data and could lead to reduced horizontal eye margin at the receiver (RX). The received data is recovered using an embedded clock and data recovery (CDR) circuit, details of which are not shown in Fig. 1. The degree of the eye margin degradation depends on the nature of the transmit jitter, the CDR gain, CDR bandwidth and its own jitter [27]. As such wireline transceiver designers have focused on characterizing and suppressing jitter for signal integrity purposes [28], [29]. In this work, it is ensured that these signal integrity considerations for high fidelity communications are maintained by message source driven equalization, and a parallel operation at the receiver extracts the transceiver jitter to be used for message source authentication.

The two primary sources of jitter in wireline transceivers are circuit or channel induced [30]. The circuit induced jitter is from device noise sources that cause deviations of signal zero-crossings away from their ideal locations. They can be random in nature like thermal and flicker noise, or periodic like power supply or substrate noise. The magnitude of deviation of the data zero-crossing from the ideal can be expressed as a function of the bit period or data unit interval (UI). A general metric that can be used to specify jitter is the N-UI jitter, which can be expressed as [30]:

$$NUI\ Jitter = \sum_{k}^{k+N-1} (\upsilon_i - \overline{\upsilon}); k > 0 \qquad (1)$$

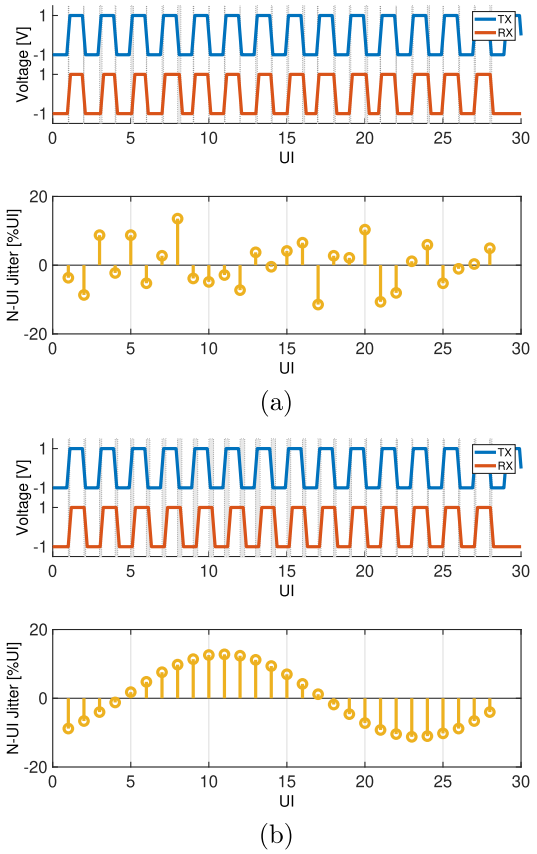

FIGURE 2. Jitter sequence examples using half-rate alternating data in which gray bars represent deviations from ideal positions for (a) random and (b) periodic noise sources.

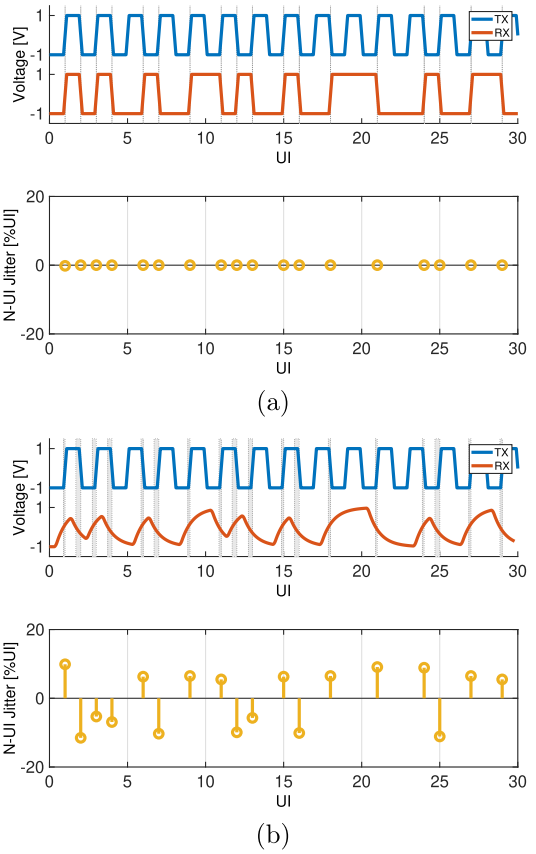

FIGURE 3. Jitter sequence examples using half-rate PRBS data showing (a) no jitter at 0dB channel loss and (b) significant jitter at 8dB of loss.

where v_i and $\overline{v}$ are the actual and i^{th} data samples, respectively, k is the trigger edge and N is the number of edges from the trigger point. The N-UI jitter illustration assuming an alternating half rate data is shown in Fig. 2 for a random and periodic jitter distribution. For the purposes of jitter quantification, standard deviation or RMS (σ) will be used for random (Gaussian) jitter (RJ) and peak-to-peak (pp) values will be used for periodic and other truncated jitter (PJ) sources.

The channel induced jitter is caused by inter-symbol interference (ISI) due to dispersion in the channel. It can also be caused by co-channel interference (CCI) in a multilane link, but this effect is considerably small in our target application. As such, only the impact of ISI is considered. To analyze the impact of channel on jitter, the translation of jitter to receiver voltage noise in the presence of channel dispersion provides good insight. Assuming transmitted symbols b_k of width T and pulse response $p(t)$ over a channel with impulse response $h(t)$, the voltage signal at the receiver can be expressed as [23]

$$x_s(t) = \sum_{-\infty}^{0} b_n g(t - kT) \tag{2}$$

$$g(t) = h(t) * p(t) \tag{3}$$

$$p(t) = \begin{cases} 1 & \text{for} \quad 0 < t \leq T \\ 0 & \text{for} \quad t \leq 0; t > T \end{cases} \tag{4}$$

The zero-crossings of the received data due to this data dependent jitter (DDJ), assuming a voltage threshold v_{th}, can be extracted by solving

$$v_{th} = x_s(t_c) = \sum_{-\infty}^{0} b_n g(t - kT) \tag{5}$$

The DDJ assuming a first-order and second-order channel response was derived and simplified in [31] to be

$$t_{c,DDJ,1} = \frac{\tau}{2} \ln\left(\frac{1+\alpha}{1-\alpha+\alpha^2}\right) \tag{6}$$

$$t_{c,DDJ,2} = -\frac{v_{th} - g(t_o + T)}{g^{(1)}(t_o + T)} \tag{7}$$

In (6) and (7), $\alpha \equiv \exp\frac{-T}{\tau}$ and represents the ratio between the bandwidth and the bit rate of the system, $g^{(1)}$ is the first derivative of g and t_o is the threshold crossing time or $g(t_o) = v_{th}$. In both cases, generally slower signals will exhibit higher DDJ. Thus, observing the DDJ, especially with a fixed sequence of data pattern, could provide strong indication of channel loss or length. The DDJ after a channel loss of 8dB loss is shown in Fig. 3 using non-return-to-zero (NRZ) pseudorandom bit sequence (PRBS). For completeness, the

circuit jitter at the transmitter will also be shaped after going through the channel. The impact of this TX jitter on the received voltage can be expressed as an additive voltage noise [32], where the total received signal is

$$x[n] = x_s[n] + x_{jit}[n] \tag{8}$$

In (8), x_{jit} is the voltage noise induced by the TX jitter. This noise can be expressed [32], [33] using Taylor's series approximation as

$$x_{jit}[n] = \sum_k q[n]s_n h_{n-k} + \frac{1}{2}\sum_k q[n]^2 s_n h^{(1)}_{n-k} \tag{9}$$

$$s_n = b_n - b_{n-1} \tag{10}$$

where $q[n]$ is the TX jitter sequence and $h^{(1)}$ is the first derivative of the channel impulse response. The voltage noise is converted back to jitter at the receiver by multiplying it with the inverse of the signal slope at the zero-crossing.

As evident from (9) and (10), the voltage noise due to the TX jitter has both a dependence on channel response and data pattern. The total jitter (TJ) observed at the receiver will therefore be a sum of all these three components at the point of observation.

$$TJ_{RX} = RJ_{RX} + PJ_{RX} + DDJ_{RX} \tag{11}$$

The TJ interaction with varying channel loss forms the basis upon which the proposed jitter-based message source authentication is realized. Transmitters at different physical distances will have different ISI that will result in different observed jitter profiles. Moreover, if the transmitted data patterns are different, this will provide an added distinguishability in the observed jitter at the receiver. Relying on central limit theorem, we will describe TJ with properties of normal distribution in subsequent discussions. It is worth mentioning that while jitter amplification due to ISI is critical for the proposed authentication approach, it implies degraded signal integrity. Thus, parallel paths for jitter extraction and equalization are used at the receiver to ensure that the security imperatives are met without penalty to bit error rate (BER) and eye margin at the receiver. Moreover, the ability to implement robust timing recovery from the received signal is assumed [27], since a receiver clock will be required as a reference for jitter measurement. The receiver clock will have its own jitter that will affect the measured TJ. However, the RX jitter is typically much lower than the TX jitter [30], [33] and thus can be treated as undesired variability whose impact on the measured target jitter has to be characterized and minimized. With increasing data rates in wireline links, ensuring that the receiver jitter is low is an important signal integrity concern and will be enough to meet the authentication accuracy requirements in the proposed approach.

III. PROPOSED JITTER-BASED AUTHENTICATION

The automotive wireline link is a broadcast network of electronic control units (ECUs) communicating with sensors and actuators as shown in Fig. 4(a). Data rates exceeding 10Gb/s have been demonstrated [34] on these links, with embedded clocking using CDRs envisioned [35]. The proposed authentication scheme will sit in each ECU transceiver (XVR). The receiver circuits will require additional circuits to extract, store and compare jitter to perform message source authentication, as shown in Fig. 5. These circuits include zero-crossing detector, time-to-digital converter (TDC), one-shot memory and statistical processing engine. No changes are needed on the transmitter side. The extra components at the receiver will add an area and power cost. However, these components will have significantly lower area and power consumption compared to main datapath circuits, hence their overhead is minimal. Further work designing and fabricating these component will allow the quantification of these additional costs. For the simulation results included in this paper, these components are realized behaviorally in Simulink and MATLAB.

A. JITTER DISTINGUISHABILITY WITH CHANNEL LOSS

The message frame structure used in the proposed authentication adopts the same one used in CAN, shown in Fig. 4(b). This is typically a 126-bit payload with 28bit section reserved for the message ID. Each message ID is unique to each ECU. This allows the use of this 28bit ID to do highly accurate message source authentication given that the unique ID will result in a unique jitter distribution with channel loss. To confirm this assertion, Simulink simulations were run over varying channel lengths (loss) and message IDs. The pulse responses for channel losses of 0dB to 12dB are shown in Fig. 6. The first simulation investigates the empirical effect of loss on the TJ assuming fixed and varying input data sequence over 200 trials. With an RJ $\sigma = 2\%$ of UI, PJ Amplitude $= 2\%$ UI and PJ period $= 100$UI added at the transmitter, the RMS value of TJ (σ_{TJ}) can be seen to increase with channel loss in Fig. 7(a). For this simulation, the input data pattern is kept constant as the channel loss is changed. Thus, it shows the effect of loss alone. As can be expected, the RJ and PJ combine to create a distribution around the expected RMS value at each loss after many trials. This makes the distributions highly distinguishable at high loss, but less so at low loss. The impact of data patterns is captured in Fig. 7(b), where the distribution at 12dB loss can be seen to be modulated by five different message IDs. Thus both the location of the transmitter and the message ID combine to generate a unique fingerprint for message source authentication.

To use the jitter profile for authentication, the mean of the RMS value of the TJ for each transmitter is stored after a secure training period. This mean distribution is then used as a reference during normal operation to authenticate transmitters in real time. To accommodate variations due to high frequency PJ and RJ, bounds are set around the mean jitter distribution to ensure appropriate true positive detection. These bounds should be set in the presence of all the noise sources, which is guaranteed in practice. The change

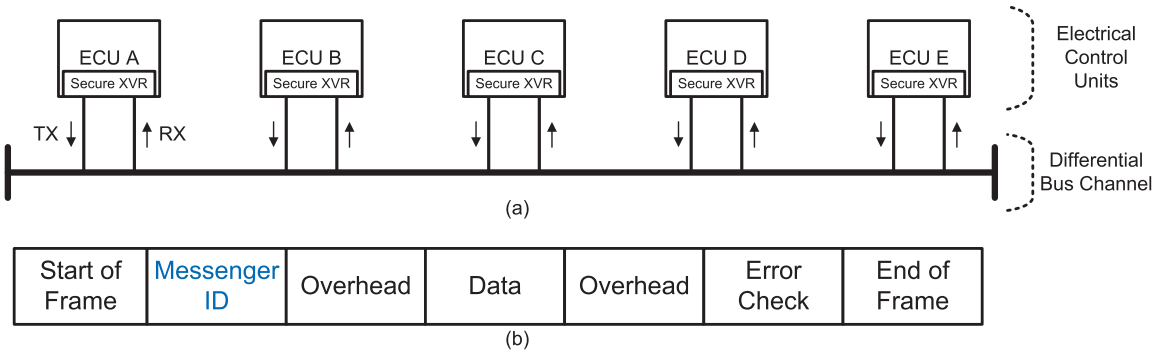

FIGURE 4. An automotive broadcast network showing (a) multiple electronic control units (ECUs) on the same bus and (b) the frame structure for communication.

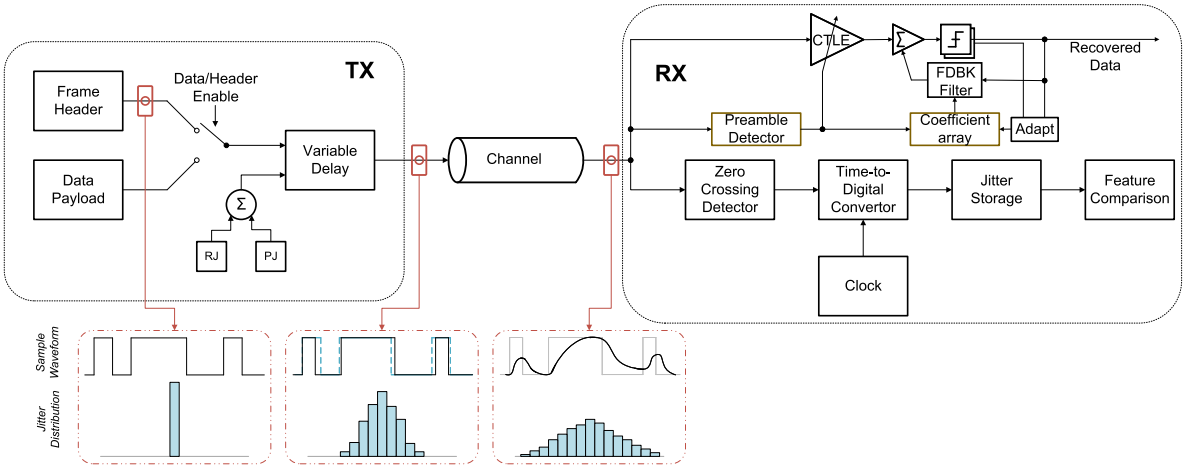

FIGURE 5. High level schematic of the Simulink testbench used to validate the message source authentication concept.

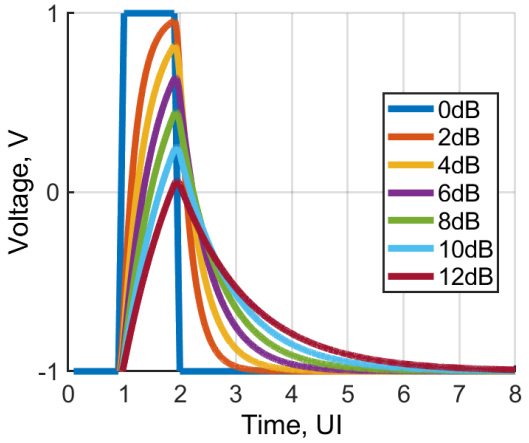

FIGURE 6. Channel pulse responses showing effect of varying channel loss.

in the mean of the RMS value of the TJ with channel loss is shown in Fig. 8. The TJ amplification with loss is evident, especially beyond 4dB of loss. The $\pm\sigma$, $\pm 2\sigma$ and $\pm 3\sigma$ bound around the mean TJ is also shown. The wider the bounds, the more accurately it will detect legitimate transmitters in the presence of noise. However, this must be balanced, as it trades off with lowering distinguishability from neighboring transmitters. The choice of detection bounds adopted in this work is discussed in Section IV.

The effect of the transmitter PJ and RJ on these bounds is shown in Fig. 9. Here the $\pm 2\sigma$ bounds are chosen for illustration purposes. Fig. 9(a) shows the impact of changing the RMS values of RJ from 0% to 4% UI. The PJ amplitude is also changed from 0% to 8% of UI in Fig. 9(b), and its period changed from 50UI to 150UI in Fig. 9(c). In all the three curves, it is evident that the RJ and PJ define the low loss bounds, but are overcrowded by the DDJ at high loss. This has good implication for distinguishability at low loss like the distributions below 4dB loss in Fig. 9(a). The inherent RJ and PJ distributions of each transmitter will be physically unique due to process, supply voltage and temperature (PVT) variations. So at low loss location of observation, these will act as distinguishing metric where the channel does not provide significant separation.

B. DATA RECOVERY SCHEME

The ease of distinguishability with high loss comes with it a degradation of signal integrity. As the channel loss increases, the ISI increases and severely reduces the signal margin at

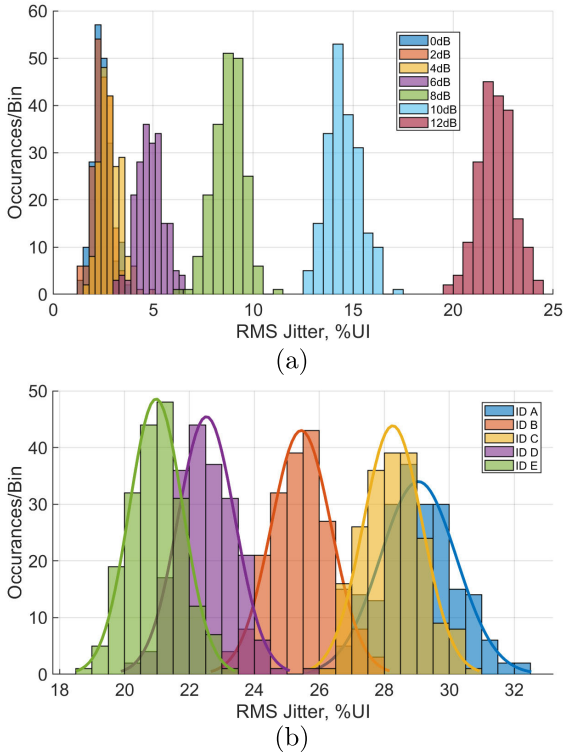

FIGURE 7. TJ distributions at the RX with 200 trials each, using (a) one message ID across different channel loss and (b) varying message IDs at 12dB channel.

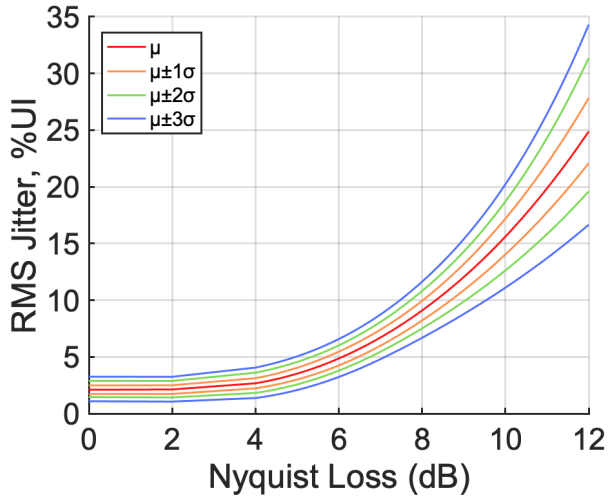

FIGURE 8. Total Jitter (TJ) amplification with loss, showing various detection bounds ($\pm\sigma$,$\pm 2\sigma$ and $\pm 3\sigma$).

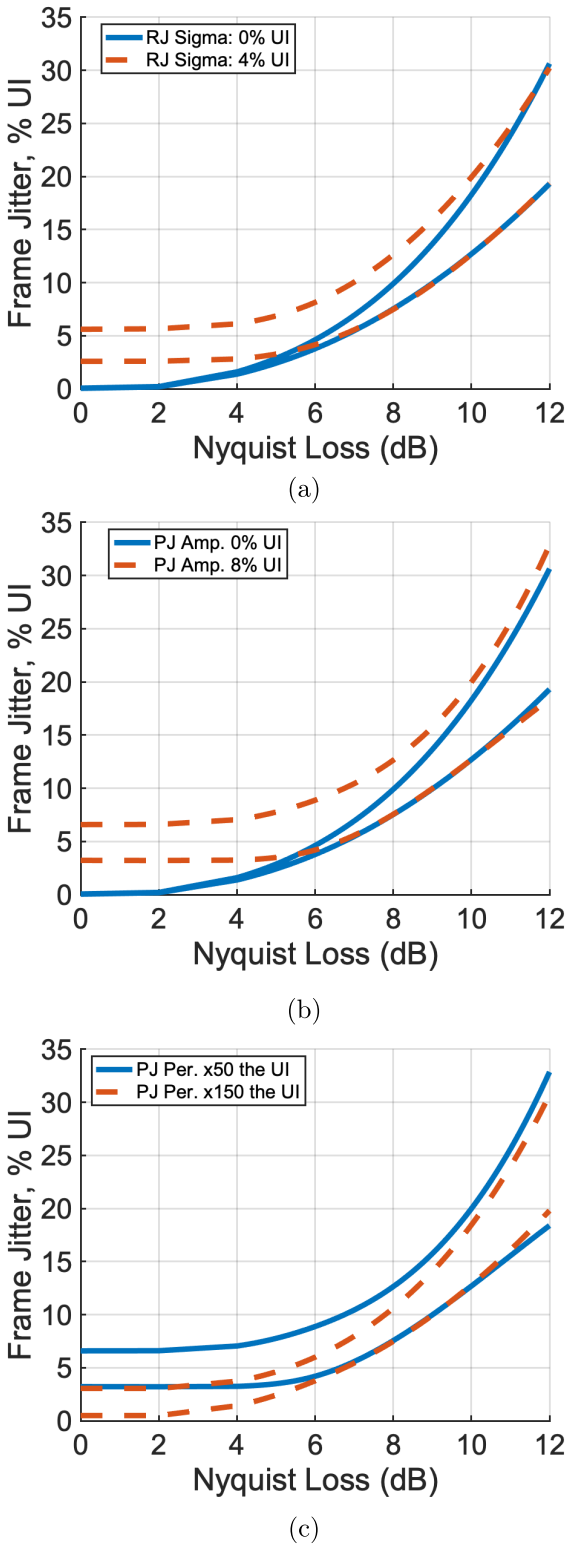

FIGURE 9. The change in the $\pm 2\sigma$ bound on the mean frame jitter (TJ) observed various channel loss due to increase of (a) RJ from 0% to 4% of UI (b) PJ amplitude from 0% to 8% of UI and (c) PJ period from 50UI to 150UI.

the receiver. The bathtub plots of the receiver eye width and height with increasing loss are shown in Fig. 10 for 10 Gbps binary non-return-to-zero (BNRZ) signaling. The maximum possible eye height (with zero ISI) is 2 V_{pp} and maximum eye width is 1 UI_{pp} (300 samples). For these simulations, 10 million data samples are run with varying RJ and PJ and channel loss from 8dB to 12dB. The receiver eye margin degrades significantly with channel loss and total jitter. The received eye is expected to be closed at 12 dB loss at a target BER of 1e-12, even at a TJ of 3% UIrms. As such

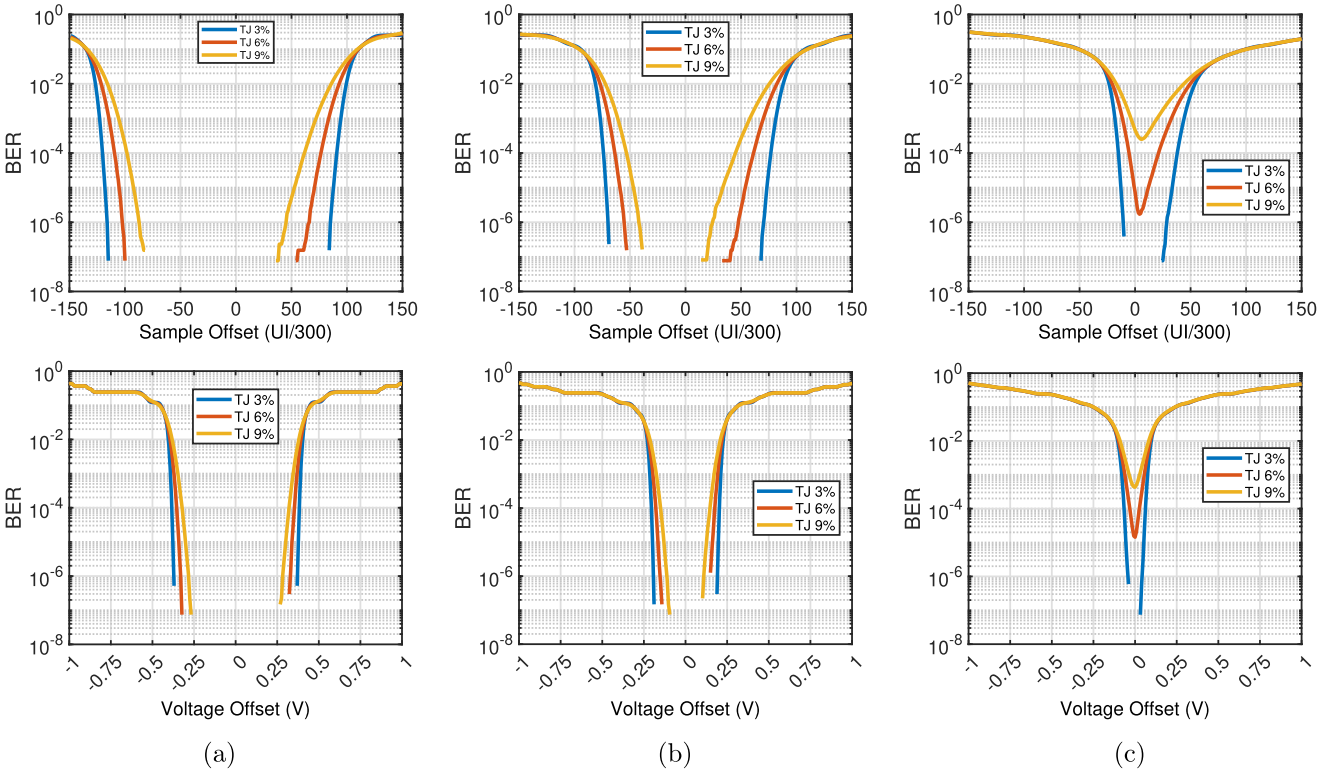

FIGURE 10. Bathtub plots showing the timing and voltage eye margins at the receiver for (a) 8 dB, (b) 10 dB and (c) 12 dB channel loss at 3%, 6% and 9% UIrms TJ.

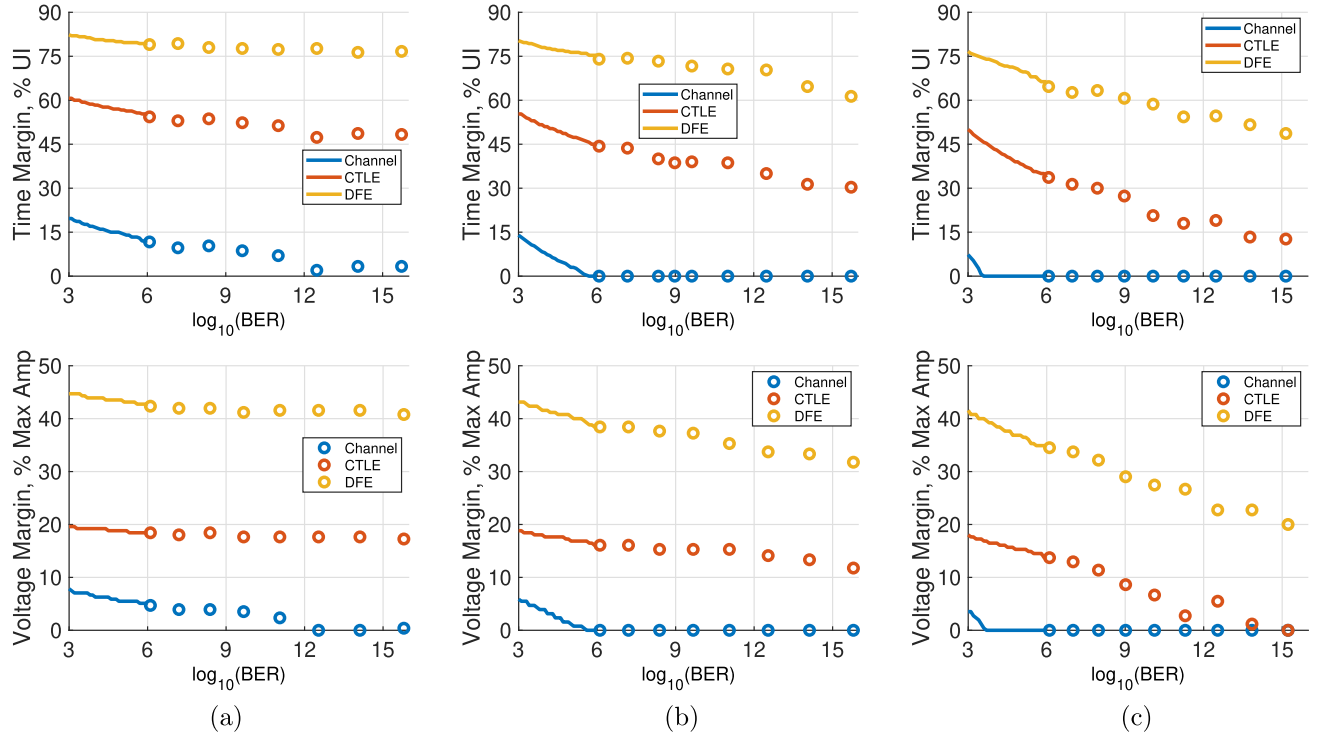

FIGURE 11. Recovered receiver eye margins at 12 dB channel loss after CTLE and DFE equalization showing the impact of (a) 3%, (b) 6% and (c) 9% UIrms TJ. The maximum available amplitude is 1 V for these simulations. Solid line is direct measurement from bathtub curve while markers indicate extrapolation using stressed eye.

to deploy the proposed authentication scheme with high authentication accuracy, equalization has to be assumed in the data path. However, the implementation of equalization in broadcast networks is not straightforward. Given the varied

channel lengths (and losses) from different transmitters on the broadcast network, the degree of equalization required will change based on the message source. The dynamic nature of the ECU transmitting on the network require a dynamic equalization approach.

The receiver of Fig. 5 gives a realization of the message-source driven equalization approach. Here, both the use of continuous-time linear equalizer (CTLE) and a decision-feedback equalizer (DFE) are explored. The mapping of the appropriate CTLE response from a family of curves [36] to a specific ECU is accomplished during training. The same approach is used to extract and store the DFE coefficients for each ECU. Given the proximity of several ECUs to each other, the size of the stored coefficient arrays does not need to match the number of ECUs on the broadcast network. For the simulations in this section, a set of four coefficient arrays were enough to cover a channel loss range of 12dB. To select the corresponding equalization to a particular ECU, a preamble detector extracts the message ID from the incoming data, and enables the desired equalizer state before the data payload. From Fig. 4, the frame structure allows enough cycles for the extraction to be completed and the selection to settle before the arrival of the data payload. If a wider range of channel losses in ECUs (more than the 12dB used in this demonstration) are needed, message ID extraction may be too error-laden to allow proper equalizer configuration. In such a case, weak equalization can be added before the preamble detection.

The implementation complexity of the proposed source-ID driven equalization is low, with reconfiguration settling times akin to that of the Rapid ON/OFF links [37] or burst-mode DFEs [38], [39], [40] and equalizer state caching similar to [41]. The eye margin of the receiver assuming no equalization, single-stage CTLE only equalization or 3-tap DFE only equalization is shown in Fig. 11. The margins are extracted from bathtub plots after 1 million UI simulations. This allows the direct margin extraction down to 1e-6 BER, and are shown with the solid lines. To derive eye margin at lower BER, the receiver eye is stressed with amplified receiver jitter and noise [42]. This allows the measurement of eye margin below 1e-12 BER, and are shown with broken markers. At the worst-case channel loss (12dB), a single-stage CTLE appears to provide adequate equalization, maintaining a timing margin above 15% of UI and a positive voltage margin up to a target BER of 1e-12. The eye margins are significantly better with the 3-tap DFE, showing ample time and voltage margins regardless of TJ values down to a projected BER of 1e-15. This confirms that regular equalization, expected at high data rate, is enough to ensure that the proposed authentication is compatible with data fidelity targets.

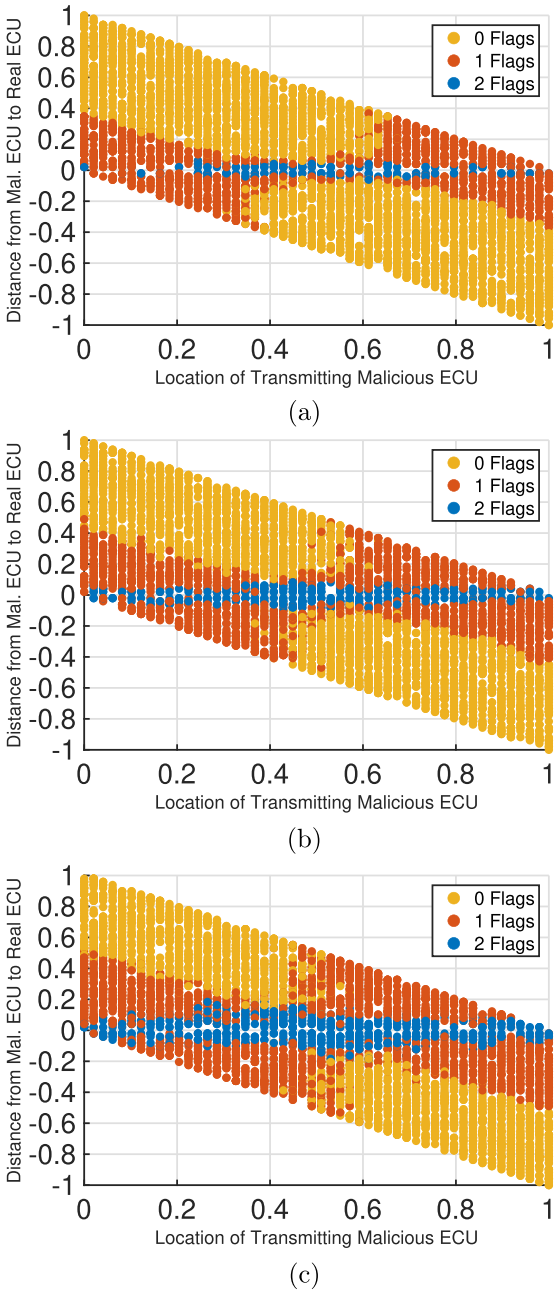

FIGURE 12. Failure rate of message source authentication with relative position of a malicious transmitter using varying number of detectors in the presence of (a) 3% UIrms total jitter, (b) 6% UIrms total jitter and (c) 9% UIrms total jitter at the transmitter. Max relative distance of ±1 translates to 12dB of loss.

IV. JITTER DETECTION AND ACCURACY

A. MULTI-POINT DETECTION AND PERFORMANCE

The jitter detection at the receiver consists of comparing the measured jitter of the incoming message ID and comparing it with the securely trained and stored mean reference distribution. For instance, the RMS jitter value of the incoming message is compared to the reference RMS jitter with a margin defined by predetermined detection bounds. Since the channel loss from the message source to the detection receiver is a linear function of distance of the former from the latter, the RMS jitter (sigma of the bitwise timing errors) is used as a stand-in for the distance. Unlike the channel loss dependent bounds of Fig. 8, the receiver's

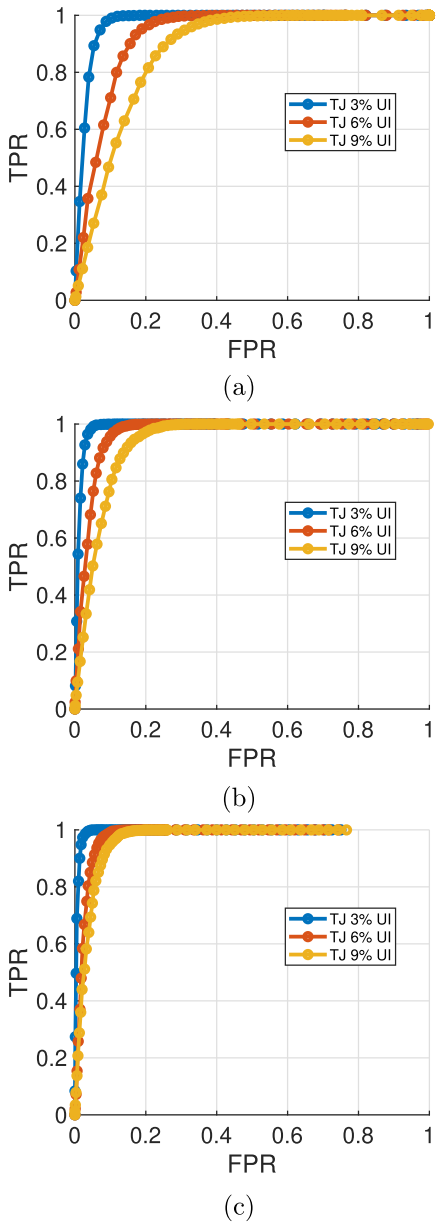

FIGURE 13. ROC using the proposed two-point detection with varying transmit side TJ values on 28bits using 50 ECUs with 100 training samples per ECU in the presence of (a) 8 dB, (b) 10 dB and (c) 12 dB channel loss.

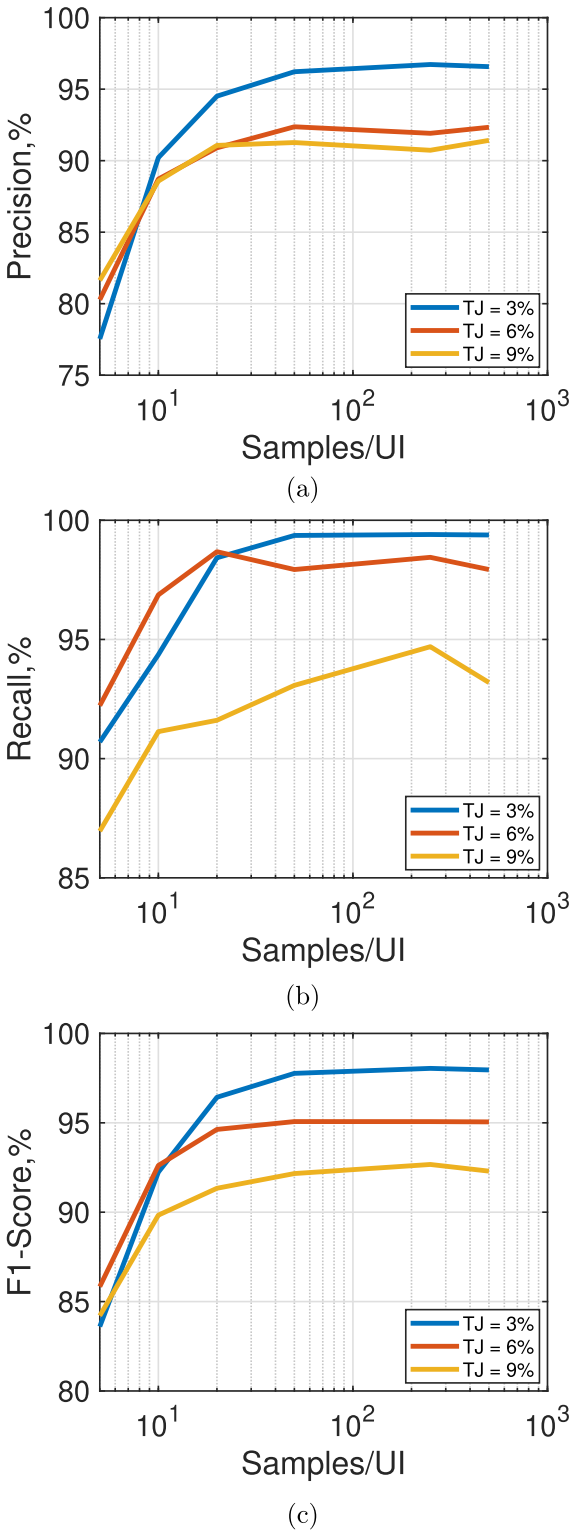

FIGURE 14. The sensitivity of authentication performance metrics to TDC resolution for (a) precision, (b) recall and (c) F1 Score at 3%, 6% and 9% UIrms TJ.

detection thresholds to validate the received jitter distribution is static value dependent on the degree of TJ in the network. The optimum detection threshold is found during training to maximize detection accuracy. Any incoming message ID with RMS jitter outside these thresholds is flagged to be malicious. As mentioned in Section III, there is a challenge distinguishing two ECUs that are close to each other due to low loss. However, the distinguishability between these same, close ECUs improves significantly if observed a far distance away, due to high TJ amplification slopes at high loss. For instance, two ECUs that are 2dB of loss from each other in Fig. 8 will have nearly indistinguishable distributions of jitter at 0dB/2dB with respect to the measurer but will be completely distinguishable at the $\pm 2\sigma$ bounds if they are at 8dB/10dB from the measurer. This is because their $\pm 2\sigma$ bounds overlap at 0dB/2dB but does not overlap at 8dB/10dB.

TABLE 1. Performance statistics.

	THR	Confusion Matrix				Model Performance Metrics			Threshold Performance Metrics			
Set (UIrms)	(UI)	TP	FN	TN	FP	TPR	FPR	AUC	Accuracy	Precision	Recall	F1 Score
TJ = 3%	1.0%	4989	31	4803	177	99.38%	3.53%	0.9932	97.92%	96.57%	99.38%	97.96%
TJ = 6%	1.8%	4975	105	4507	413	97.93%	8.13%	0.9736	94.82%	92.33%	97.93%	95.05%
TJ = 9%	2.0%	4709	344	4505	442	93.19%	8.75%	0.9626	92.14%	91.42%	93.19%	92.30%

Thus, a detector placed at a vantage point far away from any two transmitters close to each other will be able to distinguish between the two with high accuracy. Moreover, while a single detector may be susceptible to spoofing and replay attacks, it will be extremely difficult do so with multiple detectors placed away from each other. This is because an intruder could modulate its loss profile through equalization/filtering to match a targeted ECU but will not be able to do so with multiple detectors, as it will present an invalid channel profile to at least one detector [43].

Thus, a collaborative detection scheme is proposed to both address distinguishability concerns at low loss and to provide robustness against masquerade attacks. Two receivers at the opposite ends of the network will be configured to act as detectors. For a frame to be considered valid, it must be attributed a flag by both of these edge detectors. An alert that is immune to intruder override will be raised when a message source fails to match the statistics stored for its ID. A simulation of the failure rate to detect an intruder is shown in Fig. 12. The testbench includes 50 ECUs uniformly spaced between 0 dB and 12 dB loss locations. The TDC resolution is set to 500 steps per UI, to ensure no impact of the resolution on the authentication accuracy. Senstivity of the authentication accuracy to TDC resolution will be discussed later in this section. The maximum loss location is normalized to 1 for ease of illustration. Three detection instances with different transmitter jitter are shown in the figure. In Fig. 12(a), The transmit side TJ is 3% UIrms, with PJ period set at 50 UI. From the plot, while a masquerader can successfully raise a flag with one of the detectors depending on its relative physical location, it will have to be located very close to the target ECU it wants to imitate to pass both required flags in the proposed two-point detection. In Fig. 12(b) and Fig. 12(c), the transmitter noise values are increased to 6% and 9% UIrms, respectively. While the increased noise slightly loosens the location sensitivity, the proposed approach still significantly limits the range of locations an attacker could successfully launch an attack.

The receiver operating characteristics (ROC) using 50 ECUs and 10K trials per ECU are shown in Fig. 13. This provides a measure of the model validity independent of the thresholds. They show the improved performance of the proposed authentication approach with higher maximum loss. The diminishing impacts of increasing the transmit-side TJ with maximum loss are also shown for 3%, 6% and 9% UIrms, respectively. The definition of the true positive rate (TPR) and false positive rate (FPR) are

$$TPR = Pr\{\hat{y} = 1|y = 1\} = \frac{TP}{TP + FN} \tag{12}$$

$$FPR = Pr\{\hat{y} = 1|y = 0\} = \frac{FP}{TP + FN} \tag{13}$$

where TP, FP and FN are true positive, false positive and false negative, respectively. The TPR captures how often a frame if caught if it is malicious, while the FPR captures how often a legitimate frame is falsely labeled malicious. The performance parameters for all these metrics for the three TJ cases are included in Table 1. The area under the curve (AUC) defined in (14) is 0.9932, 0.9736 and 0.9626 for the 3%, 6% and 9% UIrms TJ, respectively for the 12 dB channel loss case.

$$AUC = \int_0^1 TPR\, dFPR \tag{14}$$

Using the same runs, four threshold metrics are also included in Table 1. They include Accuracy, Precision, Recall and F1 Score defined as

$$Accuracy = Pr\{\hat{y} = y\} = \frac{TP + TN}{TP + FN + TN + FP} \tag{15}$$

$$Precision = Pr\{y = 1|\hat{y} = 1\} = \frac{TP}{TP + FP} \tag{16}$$

$$Recall = Pr\{\hat{y} = 1|y = 1\} = \frac{TP}{TP + FN} \tag{17}$$

$$F1\ Score = \left[\frac{1}{2}\left(\frac{1}{Precision} + \frac{1}{Recall}\right)\right]^{-1} \tag{18}$$

The performance of the proposed authentication approach has some sensitivity to the resolution of the TDC used in the jitter extraction path. Prior simulations were run using 500 steps per UI (9.0 bits). The sensitivity of the precision, recall and F1 Score to the TDC resolution is shown in Fig. 14. While the minimum resolution needed changes with the prevailing TJ, 6 bit TDC resolution appears to be high enough to not impact the authentication performance.

In summary, the performance of the proposed authentication scheme is affected by the excess noise in the link. However, even with high transmitter jitter values, Table 1 shows very high detection accuracies are achieved. This indicates that the proposed approach will be an effective, low complexity approach to address the security concerns in automotive and other broadcast wireline networks like industrial and utility networks.

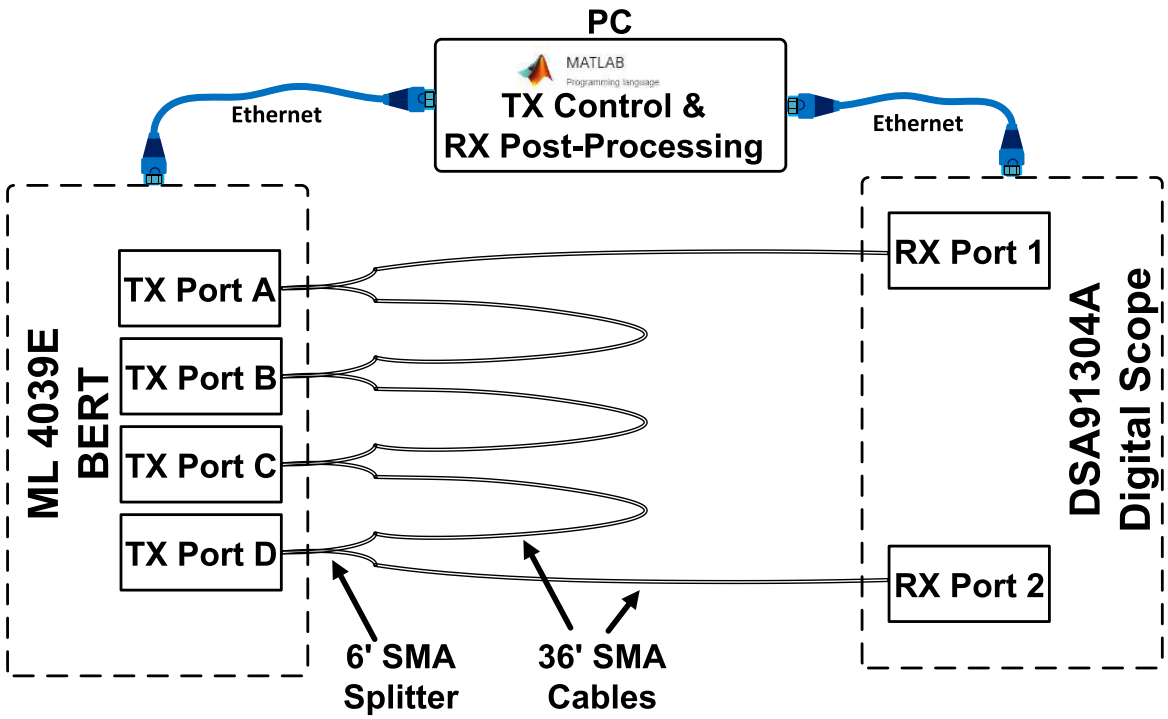

FIGURE 15. Table top measurment setup to evaluate the performance of proposed authentication scheme.

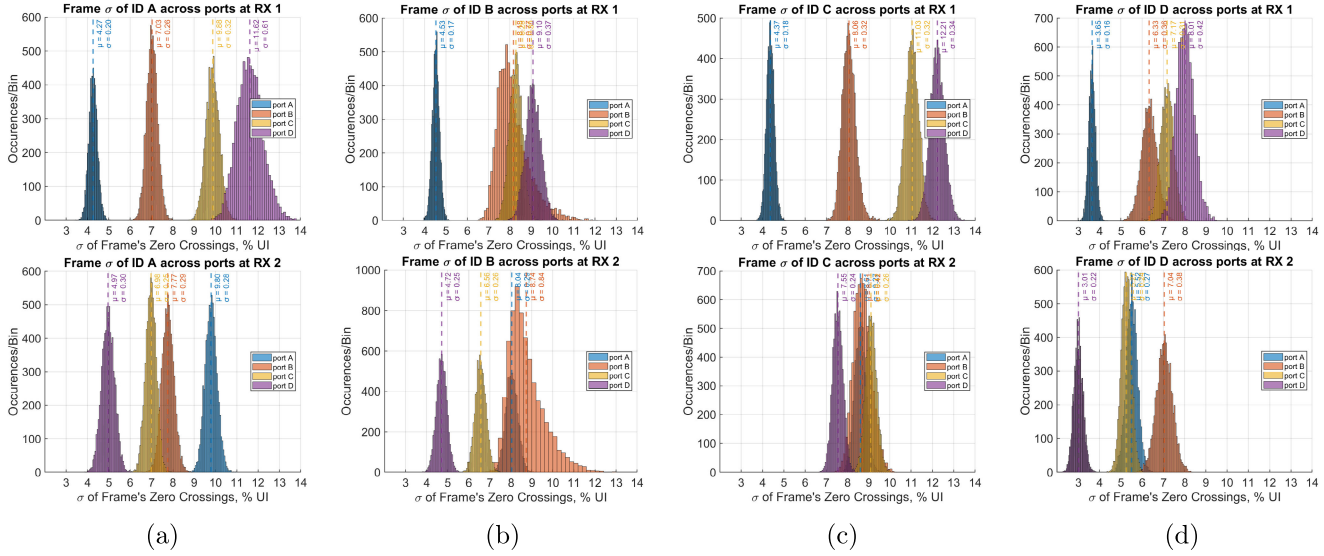

FIGURE 16. The distribution of jitter at the two RX observability ports using all four possible port IDs for (a) Port A, (b) port B, (c) Port C and (d) port D.

B. EVALUATION

To evaluate the performance of the proposed authentication scheme with real network infrastructure, the table-top experiment shown in Fig. 15 is designed. Four ECU transmitters are emulated as ports A-D using the separate channels of an ML 40139E bit error rate tester (BERT). The custom pattern definition capability of the BERT allowed the programming of each port to transmit a unique 32bit sequence representing the ID at 11.5 Gbps. These four ports are networked together using 36 in SMA cables and 6 in SMA splitters to allow a broadcast network. The two receivers ports performing the proposed two-point detection or CRA are attached to the opposite ends of the network. The data acquisition of the two receiver ports are performed by a 13 GHz Agilent DSA91304A digital oscilloscope. The jitter extraction is performed in MATLAB using 100 samples per UI, indicating less than 7bits of resolution needed in the TDC. The control of the ID at each port and receiver data

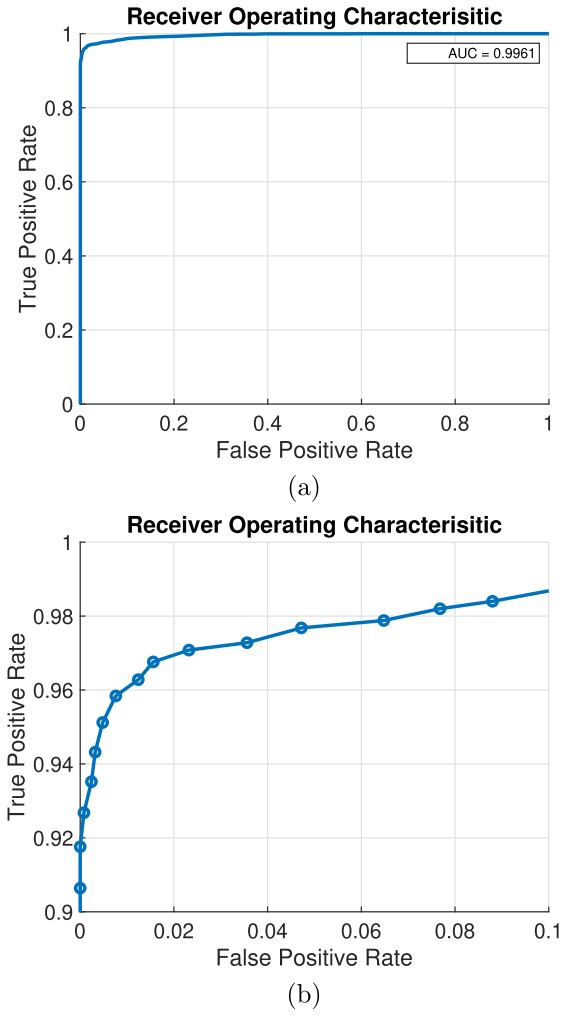

FIGURE 17. (a)ROC using the measurement results of the proposed CRA detection with four ECUs and 5000 trials and (b) a zoomed in look.

TABLE 2. Confusion matrix for CRA detection using single frame detection.

	ID A	ID B	ID C	ID D
Port A	100.0%	0.0%	0.0%	0.0%
Port B	0.0%	87.0%	0.0%	0.0%
Port C	0.0%	0.0%	100.0%	0.0%
Port D	0.0%	0.0%	18.7%	99.8%

post-processing to perform authentication is also conducted in MATLAB through a local network connection to the BERT and DSA. Since all four of the transmit ports are clocked from the same internal reference in the ML 4039E BERT, there were no frequency errors in the observed data. Simple static de-skewing are used at the receiver to ensure same frames are compared at each port. Once these skew parameters are extracted in training, they are kept static during validation.

With this setup, the jitter distribution of the four randomly generated 32-bit frame IDs are transmitted and measured. The generated Frame IDs in Hex are 835C774A, 423B1B63, F48ADEC9 and 30B4B5D2 for Ports A, B, C and D, respectively. The results included in Fig. 16 show that the jitter distribution is both a strong function of the frame ID and the location of the port. Moreover, the distribution observed at the two receiver ports are unique even for the same frame ID and present an extremely difficult challenge to break for an attacker. For instance, focusing on Fig. 16(a), an attacker attempting to masquerade as ECU A, which is located at TX Port A, through lets say compromised TX Port D, will still have to use ECU A's ID, ID A, for the system to register it as ECU A. However, the expected jitter distribution at RX Port 1 for TX Port A has significantly lower jitter RMS than that of TX Port D (0.20 %UI for A compared to 0.61 %UI for D). If the attacker were to adjust their channel (through equalization in this case) to narrow the jitter distribution presented at RX Port 1 to match the distribution expected from the true TX Port A, the frame will fail to meet the jitter expectation at the opposing RX port, RX Port 2, making intrusion detection robust.

The ROC using 5000 trials (50% valid and 50% malicious) is included in Fig. 17. The zoomed in version of the figure shows less than 8% FPR at 98% TPR. The calculated Accuracy, Precision, Recall and F1-Score from this data yields 97.60%, 98.41%, 96.76% and 97.58%, respectively at a threshold of 1.5 %UI. The confusion matrix shown in Table 2 indicate very high recognition rates for Ports/IDs. All the mis-classifications are from difficulty separating ID C sent by neighboring ports C or D. Looking at jitter distributions of Fig. 16(c), it is evident that the randomly generated frame ID for C leads to similar jitter distribution at RX Port 1 (0.32%UIrms for Port C vs 0.34%UIrms for Port D) and RX Port 2 (0.26%UIrms for Port C vs 0.24%UIrms for Port D). This mis-classification can be addressed through appropriate frame ID selection.

A comparison of the proposed approach to previously presented schemes is shown in Table 3. The proposed approach achieves similar accuracy to prior approaches while using single frame detection. This combined with the unprecedented data rate of 11.5 Gbps indicates one of the lowest authentication latencies.

The results shown in this section assume a forwarded receiver clock source. In practical implementations, a CDR will be used to recover the receiver clock from data [27], [36], [44]. The CDR will have its own jitter that will appear as additional noise to the detectors. However, the CDR will also track jitter within its bandwidth, thus improving immunity of the proposed authentication scheme to low frequency errant jitter. The jitter of interest embedded in the message ID will be outside the CDR bandwidth and will not be shaped by the CDR. Thus, the jitter signature used as feature for the proposed authentication scheme will not be affected by the specified CDR bandwidth. Moreover, equalization in the jitter extraction path was not considered in the presented analysis but could provide an additional degree of freedom and possibly confidentiality in the RMS value of the jitter used for authentication. This is because equalization could be used to modulate the dependence of jitter amplification on ECU distance from the detectors. The degree of equalization

TABLE 3. Performance comparison.

	Zhou [17]		Choi [21]		Hafeez [25]	This Work
Setup	Arduino,STM32	Arduino,STM32	Arduino	Car	Arduino	Benchtop
Data Rate	33 kbps	500 kbps	500 kbps	500 kbps	1 Mbps[1]	11.5 Gbps
Data Acquisition	500 MS/s	500 MS/s	2.5 GS/s	2.5 GS/s	2.0 GS/s	Continuous
Feature Quantization	8-bit ADC	8-bit ADC	8-bit ADC	8-bit ADC	8-bit ADC	6-7bit TDC
Feature Type	Clock Skew	Clock Skew	Voltage	Voltage	Voltage	Jitter
Frames/Detection	5	200	20	20	≈30[2]	1
Number of Features	1	8	8	8	7	1
Number of ECUs	6	6	12	28-45	7	4
F1 Score	99.98%	90.06%	98.45%	93.54%	99.81%	97.58%

[1] MPC2551 high speed CAN transceivers used supports 1 Mbps operation.
[2] Extracted from number of valid samples distributed across 7 ECUs.

deployed in the jitter extraction path does not need to be disclosed because it has no signal integrity implications.

V. CONCLUSION

A new message source authentication scheme for broadcast wireline networks has been presented. The automotive wireline network was chosen as the vehicle to study the effectiveness of the proposed scheme in achieving high authentication accuracy with no data bandwidth overhead and minimal latency and hardware cost. The use of jitter enabled an innovative mixing of message ID pattern and channel loss to generate a highly distinguishable feature for authentication. The sensitivity of the detection bounds used in the proposed scheme to random and periodic transmitter jitter is characterized. To further improve the robustness of the proposed scheme to spoofing and replay attacks, a two-point detection scheme has been proposed. Simulation results of proposed scheme in Simulink show high detection accuracies, even in the presence of significant transmitter jitter. Measurement results demonstrate extremely high authentication performance, and point to the possibility of further enhancement of the authentication robustness through Frame ID design. Thus, the proposed approach provides a feasible approach to secure the automotive and other broadcast networks even as data rates rise to 10s of Gb/s on these networks.

ACKNOWLEDGMENT

The authors would like to thank Shabbir Ahmed of Intel Labs for insightful discussions.

REFERENCES

[1] A. Lasry and E. Chen, "A-PHY: The cornerstone of MIPI automotive system solutions," MIPI Alliance Inc., Piscataway, NJ, USA. Accessed: Dec. 5, 2023. [Online]. Available: https://www.mipi.org/knowledge-library/webinars/events/mipi-webinar-a-phy-cornerstone-automotive-system-solution

[2] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 11, pp. 2898–2915, Nov. 2017.

[3] A. Greenberg, "Hackers remotely kill a jeep on the highway—With me in it," Wired. Accessed: Dec. 5, 2023. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

[4] S. Nie, Y. Du, and L. Liu, "Free-fall: Hacking Tesla from wireless to can bus," *Briefing, Black Hat USA*, vol. 25, pp. 1–16, Jul. 2017.

[5] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *Proc. Int. Conf. Detection Intrusions Malware, Vulnerability Assessment*, 2017, pp. 185–206.

[6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[7] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures," *Rel. Eng. Syst. Safety*, vol. 96, no. 1, pp. 11–25, 2011.

[8] J. Lastinec and L. Hudec, "A study of securing in-vehicle communication using IPSEC protocol," *J. Electr. Eng.*, vol. 72, no. 2, pp. 89–98, Apr. 2021.

[9] E. Ali, T. El-fouly, and A. Badr, "MESP: A modified IPSec for secure multicast communication," in *Proc. 6th Int. Conf. ITS Telecommun.*, Jun. 2006, pp. 812–816.

[10] D. Xu, P. Ren, J. A. Ritcey, and Y. Wang, "Code-frequency block group coding for anti-spoofing pilot authentication in multi-antenna OFDM systems," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1778–1793, Jul. 2018.

[11] P. Ramabadran, P. Afanasyev, D. Malone, M. Leeser, D. McCarthy, B. O'Brien, R. Farrell, and J. Dooley, "A novel physical layer authentication with PAPR reduction based on channel and hardware frequency responses," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 2, pp. 526–539, Feb. 2020.

[12] N. Gulati, R. Greenstadt, K. R. Dandekar, and J. M. Walsh, "GMM based semi-supervised learning for channel-based authentication scheme," in *Proc. IEEE 78th Veh. Technol. Conf. (VTC Fall)*, Sep. 2013, pp. 1–6.

[13] L. Senigagliesi, M. Baldi, and E. Gambi, "Comparison of statistical and machine learning techniques for physical layer authentication," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1506–1521, 2021.

[14] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[15] Y. Zhao, Y. Xun, and J. Liu, "ClockIDS: A real-time vehicle intrusion detection system based on clock skew," *IEEE Internet Things J.*, vol. 9, no. 17, pp. 15593–15606, Sep. 2022.

[16] L. Popa, B. Groza, C. Jichici, and P.-S. Murvay, "ECUPrint—Physical fingerprinting electronic control units on CAN buses inside cars and SAE J1939 compliant vehicles," *IEEE Trans. Inf. Forensics Security*, vol. 17, pp. 1185–1200, 2022.

[17] 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.

[18] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "SAIDuCANT: Specification-based automotive intrusion detection using controller area network (CAN) timing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1484–1494, Feb. 2020.

[19] S. Lee, W. Choi, H. J. Jo, and D. H. Lee, "ErrIDS: An enhanced cumulative timing error-based automotive intrusion detection system," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 11, pp. 12406–12421, Nov. 2023.

[20] Z. Huang, G. Li, A. Hu, J. Yu, and S. Wu, "Recognizing automotive Ethernet device by extracting fingerprint from power spectrum," in *Proc. IEEE 22nd Int. Conf. Commun. Technol. (ICCT)*, Nov. 2022, pp. 1442–1446.

[21] W. Choi, K. Joo, H. J. Jo, M. C. Park, and D. H. Lee, "VoltageIDS: Low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2114–2129, Aug. 2018.

[22] Z. Deng, J. Liu, Y. Xun, and J. Qin, "IdentifierIDS: A practical voltage-based intrusion detection system for real in-vehicle networks," *IEEE Trans. Inf. Forensics Security*, vol. 19, pp. 661–676, 2024.

[23] J. Li, M. Zhang, and Y. Lai, "A light-weighted machine learning based ECU identification for automotive CAN security," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Aug. 2023, pp. 545–550.

[24] A. Hafeez, K. Topolovec, and S. Awad, "ECU fingerprinting through parametric signal modeling and artificial neural networks for in-vehicle security against spoofing attacks," in *Proc. 15th Int. Comput. Eng. Conf. (ICENCO)*, 2019, pp. 29–38.

[25] A. Hafeez, J. Mohan, M. Girdhar, and S. S. Awad, "Machine learning based ECU detection for automotive security," in *Proc. 17th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2021, pp. 73–81.

[26] P.-S. Murvay and B. Groza, "Source identification using signal characteristics in controller area networks," *IEEE Signal Process. Lett.*, vol. 21, no. 4, pp. 395–399, Apr. 2014.

[27] T. Musah and A. Namachivayam, "Robust timing error detection for multilevel baud-rate CDR," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 10, pp. 3927–3939, Oct. 2022.

[28] J. Liang, M. S. Jalali, A. Sheikholeslami, M. Kibune, and H. Tamura, "On-chip measurement of clock and data jitter with sub-picosecond accuracy for 10 Gb/s multilane CDRs," *IEEE J. Solid-State Circuits*, vol. 50, no. 4, pp. 845–855, Apr. 2015.

[29] M. Takamiya, H. Inohara, and M. Mizuno, "On-chip jitter-spectrum-analyzer for high-speed digital designs," in *Proc. IEEE Int. Solid-State Circuits Conf.*, Feb. 2004, pp. 350–532.

[30] B. Casper and F. O'Mahony, "Clocking analysis, implementation and measurement techniques for high-speed data links—A tutorial," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 56, no. 1, pp. 17–39, Jan. 2009.

[31] J. Buckwalter, B. Analui, and A. Hajimiri, "Predicting data-dependent jitter," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 51, no. 9, pp. 453–457, Sep. 2004.

[32] G. Balamurugan, B. Casper, J. E. Jaussi, M. Mansuri, F. O'Mahony, and J. Kennedy, "Modeling and analysis of high-speed I/O links," *IEEE Trans. Adv. Packag.*, vol. 32, no. 2, pp. 237–247, May 2009.

[33] V. Stojanovic and M. Horowitz, "Modeling and analysis of high-speed links," in *Proc. IEEE Custom Integr. Circuits Conf.*, Sep. 2003, pp. 589–594.

[34] G. W. D. Besten, "30.1 single-pair automotive PHY solutions from 10 Mb/s to 10 Gb/s and beyond," in *Proc. IEEE Int. Solid- State Circuits Conf.*, Feb. 2019, pp. 474–476.

[35] W. Lee, M. Shim, Y. Lee, H. Yang, S. Shin, W.-S. Choi, and D.-K. Jeong, "Area and power efficient 10B6Q PAM-4 DC balance coder for automotive camera link," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 4, pp. 2056–2060, Apr. 2022.

[36] T. Musah, J. E. Jaussi, G. Balamurugan, S. Hyvonen, T.-C. Hsueh, G. Keskin, S. Shekhar, J. Kennedy, S. Sen, R. Inti, M. Mansuri, M. Leddige, B. Horine, C. Roberts, R. Mooney, and B. Casper, "A 4–32 Gb/s bidirectional link with 3-tap FFE/6-tap DFE and collaborative CDR in 22 nm CMOS," *IEEE J. Solid-State Circuits*, vol. 49, no. 12, pp. 3079–3090, Dec. 2014.

[37] D. Kim, M. G. Ahmed, W.-S. Choi, A. Elkholy, and P. K. Hanumolu, "A 12-Gb/s 10-ns turn-on time rapid ON/OFF baud-rate DFE receiver in 65-nm CMOS," *IEEE J. Solid-State Circuits*, vol. 55, no. 8, pp. 2196–2205, Aug. 2020, doi: 10.1109/JSSC.2020.2978138.

[38] P. Ossieur, C. Melange, T. De Ridder, J. Bauwelinck, B. Baekelandt, X.-Z. Qiu, and J. Vandewege, "Burst-mode electronic equalization for 10-Gb/s passive optical networks," *IEEE Photon. Technol. Lett.*, vol. 20, no. 20, pp. 1706–1708, Oct. 2008.

[39] K.-C. Chen and A. Emami, "A 25 Gb/s APD-based burst-mode optical receiver with 2.24ns reconfiguration time in 28nm CMOS," in *Proc. IEEE Custom Integr. Circuits Conf. (CICC)*, Apr. 2018, pp. 1–4.

[40] G. Coudyzer, P. Ossieur, J. Bauwelinck, and X. Yin, "A 25G baud PAM-4 linear burst-mode receiver with analog gain- and offset control in 0.25 μm SiGe:C BiCMOS," *IEEE J. Solid-State Circuits*, vol. 55, no. 8, pp. 2206–2218, Aug. 2020.

[41] Z. Hu, Z. Zhou, C. C. Chan, and Z. Liu, "Equalizer state caching for fast data recovery in optically-switched data center networks," *J. Lightw. Technol.*, vol. 39, no. 17, pp. 5362–5370, Sep. 2021.

[42] K. Ichiyama, T. Kusaka, and M. Ishida, "A stressed eye testing module for production test of 30-Gbps NRZ signal interfaces," in *Proc. IEEE Int. Test Conf. (ITC)*, Oct. 2018, pp. 1–10.

[43] S. Ahmed, M. Juliato, C. Gutierrez, and M. Sastry, "Two-point voltage fingerprinting: Increasing detectability of ECU masquerading attacks," 2021, *arXiv:2102.10128*.

[44] A. Abdelaziz, M. Ahmed, and T. Musah, "Hybrid timing error detector for baud rate multilevel clock and data recovery," *IEEE Open J. Circuits Syst.*, vol. 4, pp. 324–335, 2023.

SYDNEY LANG (Graduate Student Member, IEEE) received the B.S. degree in electrical and computer engineering from The Ohio State University, Columbus, OH, USA, in 2021, where she is currently pursuing the Ph.D. degree in electrical and computer engineering.

She is a Claire Booth Luce Fellow and is with the Mixed-Signal Integrated Circuits and Systems Laboratory. She has interned at various companies, including working in mixed-signal IC design with SenseICs, and in high-power filter design with Pole/Zero. Her research interests include high speed wireline transceiver design, time-domain signal process, and machine learning hardware design.

TAWFIQ MUSAH (Senior Member, IEEE) received the B.S. degree in electrical engineering from Columbia University, New York, NY, USA, in 2005, and the Ph.D. degree in electrical and computer engineering from Oregon State University, Corvallis, OR, USA, in 2010.

He was with Intel Laboratories, involved in micro-power ADC design, from 2006 to 2007, and interned with Texas Instruments (TI), designing a hardware sensor, in 2010. From 2010 to 2018, he was with the Signaling Research Laboratory, Intel Corporation, Hillsboro, OR, involved on circuits and systems to enable Intel's next generation chip-to-chip electrical and optical links. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH, USA. His research interests include low-power equalization techniques for next-generation electrical and optical I/O links, multi-GS/s ADCs, and high-level circuit modeling and verification.

Dr. Musah was a recipient of the Intel Labs Divisional Recognition Award in 2014 and 2017 and the Intel Laboratories Academy Award for Excellence in bringing new experiences or technical innovation to market in 2015.