IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 9 June 2023, accepted 22 July 2023, date of publication 11 August 2023, date of current version 8 September 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3304331

RESEARCH ARTICLE

A Novel Hybrid Quantum-Classical Framework for an In-Vehicle Controller Area Network Intrusion Detection

M SABBIR SALEK[1], (Graduate Student Member, IEEE), PRONAB KUMAR BISWAS[2], JACQUAN POLLARD[3], JORDYN HALES[4], ZECHENG SHEN[4], VIVEK DIXIT[4], MASHRUR CHOWDHURY[1], (Senior Member, IEEE), SAKIB MAHMUD KHAN[1], (Senior Member, IEEE), AND YAO WANG[4]

[1]Glenn Department of Civil Engineering, Clemson University, Clemson, SC 29631, USA
[2]HDR, Phoenix, AZ 85012, USA
[3]Kiewit Engineering Inc., Lenexa, KS 66219, USA
[4]Department of Physics and Astronomy, Clemson University, Clemson, SC 29631, USA

Corresponding author: M Sabbir Salek (msalek@g.clemson.edu)

This work was supported in part by the Center for Connected Multimodal Mobility (C^2M^2) (a U.S. Department of Transportation Tier 1 University Transportation Center) headquartered at Clemson University, Clemson, SC, USA. The work of Vivek Dixit and Yao Wang was supported by the National Science Foundation (NSF) under Award DMR-2038011.

ABSTRACT In-vehicle controller area network (CAN) is susceptible to various cyberattacks due to its broadcast-based communication nature. An attacker can inject false messages to a vehicle's CAN via wireless communication, the infotainment system, or the onboard diagnostic port. Thus, an effective intrusion detection system is essential to distinguish authentic CAN messages from false ones. In this study, we developed a hybrid quantum-classical CAN intrusion detection framework using a classical neural network (NN) and a quantum restricted Boltzmann machine (RBM). The classical NN is dedicated to feature extraction from CAN images generated from a vehicle's CAN bus data. In contrast, the quantum RBM is dedicated to CAN image reconstruction for classification-based intrusion detection. The novelty of the study lies in utilizing the generative ability of an RBM to reconstruct the pixels in a CAN image, a portion of which is dedicated to labeling. Then, that portion of the reconstructed image is used to classify the image as an attack image or a normal image. To evaluate the performance of the hybrid quantum-classical CAN intrusion detection framework, we used a real-world CAN fuzzy attack dataset to create three separate attack datasets, where each dataset represents a unique set of features related to the vehicle. We compared the performance of our hybrid framework to a similar but classical-only framework. Our analyses showed that the hybrid framework performs better in CAN intrusion detection compared to the classical-only framework. For the three datasets considered in this study, the best models in the hybrid framework achieved 97.5%, 97%, and 98.3% intrusion detection accuracies and 94.7%, 93.9%, and 97.2% recalls, respectively. In contrast, the best models in the classical-only framework achieved 92.5%, 95%, and 93.3% intrusion detection accuracies and 84.2%, 89.8%, and 88.9% recalls, respectively.

INDEX TERMS Controller area network, cyberattack detection, intrusion detection, quantum artificial intelligence, restricted Boltzmann machine, generative artificial intelligence.

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

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION

Controller area network (CAN) is a de facto standard for the broadcast-based in-vehicle message communication system to provide a dedicated, reliable, and efficient communication channel for all in-vehicle connected electronic control units or ECUs, sensors, and systems. Although CAN is widely popular among in-vehicle networks, it lacks common security features, such as authentication. Attackers can easily inject false messages to a vehicle's CAN via the onboard diagnostic (OBD-II) port, the infotainment system, or wireless communication. Thus, different CAN intrusion detection systems (IDSs) have been widely studied in recent years due to the inherent vulnerabilities of CAN communication to cyberattacks [1], [2], [3]. Researchers presented various IDSs based on different machine learning (ML) and deep learning (DL) techniques [4], [5], [6], [7], [8]. In addition to the variation in ML or DL techniques, different features and their combinations have been attempted by researchers to improve CAN intrusion detection accuracy. Some common features used in the existing studies include message timing (e.g., message frequency/rate and interval) [9], signatures (e.g., ID, time interval, and correlation) [10], and anomaly [4].

Beyond the classical computer-based CAN IDSs, quantum computing can be used for CAN intrusion detection to detect the increasing number of cyberattacks. Dong et al. [11] presented a quantum beetle swarm optimization-based extreme learning machine or ELM (i.e., a neural network where randomly selected input weights and hidden layer biases are utilized for faster learning) for network intrusion detection. The ELM in [11] provided higher detection accuracy and faster convergence than several other classical IDSs, such as backpropagation, support vector machine, improved rough ELM, particle swarm optimization, and genetic algorithm optimization-based ELM models. Chen et al. [12] applied quantum computing for k-means clustering combined with a quantum-inspired ant lion optimization algorithm for intrusion detection. Their approach [12] improved the convergence of k-means clustering to the global optimal solution. Caivano et al. [13] presented a quantum annealing or QA-based IDS for CAN that achieved a similar detection accuracy for denial of service and fuzzy attacks as a classical classification technique with significantly shorter training and prediction time.

This study presents a hybrid quantum-classical CAN intrusion detection framework that utilizes a classical computer for data preprocessing to generate CAN images with embedded labels and a quantum computer for restricted Boltzmann machine or RBM-based CAN image reconstruction and classification technique to detect CAN intrusions. RBM is a widely used energy-based generative stochastic neural network (NN) model. The training process of an RBM can be done using algorithms such as contrastive divergence (CD) [14] and quantum annealing (QA) [15]. QA provides more accurate gradient estimates for training RBM models compared to CD-based training for problems with high energy gaps between modes, as shown by Korenkevych et al. [16]. Dixit et al. [17] trained an RBM model using the D-Wave 2000Q QA machine with 64 visible and 64 hidden units, a task difficult to achieve using a gate-based approach. Such QA-based training can also be utilized for training RBM models to detect intrusions in an in-vehicle CAN, which is the motivation for this study.

B. CONTRIBUTION

In a transportation cyber-physical systems environment, classical and quantum computers can be used together in a hybrid fashion for CAN intrusion detection. For example, Islam et al. [18] presented a hybrid quantum-classical NN-based framework for CAN intrusion detection that outperformed both the classical-only and quantum-only approaches by overcoming the limitations of each of them. However, to the best of our knowledge, a hybrid approach of a classical NN and a quantum RBM has not been undertaken for CAN intrusion detection yet. In addition, existing studies on NN-based CAN IDSs, including generative NN-based CAN IDSs, do not consider embedding labels directly into the corresponding CAN images to leverage the image generation capability of generative NNs for an image classification-based CAN IDS. Utilizing QA-based training of an RBM, which enables sampling from the original probability distribution of the model, our CAN image (embedded with dedicated labeling pixels) reconstruction-based CAN intrusion detection framework offers more efficient learning (i.e., faster convergence with a high detection accuracy) compared to the existing generative NN-based CAN IDSs. Thus, this study contributes to the current body of CAN IDS literature by presenting a hybrid quantum-classical framework for CAN intrusion detection that leverages the image generation capability of generative NNs. We utilize the image generation capability by reconstructing the embedded labels in CAN images, which is then used for image classification-based CAN intrusion detection.

The rest of the paper is organized as follows: Section II provides preliminary information regarding CAN protocol and CAN frame structure; Section III presents a review of the existing studies related to generative NN-based CAN intrusion detection; Section IV presents the details of the hybrid quantum-classical CAN intrusion detection framework developed in this study, including classical computer-based CAN data preprocessing for CAN image generation and quantum RBM-based CAN image reconstruction and binary classification; Section V presents the evaluation method, including the details of the CAN datasets used for evaluation, the CAN intrusion detection process, and the evaluation metrics; Section VI presents the evaluation results; and Section VII presents the conclusions.

II. CAN PROTOCOL AND STRUCTURE

CAN is a broadcast-based messaging system in which messages are broadcast to the CAN bus nodes. Vehicle CAN utilizes the Carrier-Sense Multiple Access protocol with Collision Detection and Arbitration on Message Priority (CSMA/CD+AMP) that enables transmitting nodes detect collisions. This collision occurs due to simultaneous transmission of multiple messages. A filter at each node selects the CAN messages to be broadcast based on the CAN arbitration identifiers (IDs). The arbitration ID gives the broadcasting priority of a CAN message.

Fig. 1 shows the standard structure of a CAN frame, which includes seven fields, i.e., Start of Frame (SOF), arbitration, control, data, Cyclic Redundancy Code (CRC), acknowledgment (ACK), and End of Frame (EOF) fields. The SOF field includes a single dominant bit representing the start of transmission of a CAN frame. The arbitration field contains 11 bits dedicated to the arbitration ID and a single bit dedicated to Remote Transmission Request (RTR). The arbitration ID is used to determine the broadcasting priority of the frame, whereas the RTR varies based on the type of the frame. Six bits are dedicated to the control field among which the first two bits are reserved for future use and the remaining four bits indicate the Data Length Code (DLC), i.e., the length of the data field. From zero to a maximum of 64 bits are dedicated to the data field representing the actual data or payload. The CRC field (containing 16 bits) helps check the integrity of the message, and the ACK (containing two bits) is reserved for acknowledgment of a message received earlier. Finally, the EOF field denotes the termination of the frame and consists of seven bits.

III. RELATED WORK

CAN intrusion detection is widely studied by researchers in the recent years because of the inherent vulnerabilities of CAN communication due to its broadcast-based nature. As a result, the existing body of literature is quite vast and there are also several surveys on CAN IDSs [2], [3], [19], [20], [21], [22]. Since we developed a hybrid quantum-classical framework that utilizes a generative NN, we explicitly focus on reviewing studies that used generative NN models for CAN intrusion detection in this section. The studies reviewed here are presented in chronological order.

Seo et al. [23] developed a generative adversarial network (GAN)-based IDS for in-vehicle networks that can detect unknown attacks while using only normal data (i.e., non-attack data) for training. The generator in their GAN-based IDS [23] generates fake CAN images to train the discriminator to distinguish between normal and fake CAN images. The authors in [23] evaluated their GAN-based IDS for denial of service (DoS), fuzzy, RPM, and gear attack datasets and obtained 97.9%, 98%, 98%, and 96.2% accuracies, respectively.

Xie et al. [24] developed a GAN-based CAN IDS utilizing an enhanced GAN model to overcome the limitation of generating rough CAN message blocks utilized in other GAN-based IDSs. The authors in [24] tested their CAN IDS against DoS, injection, masquerade, and data tampering attacks and achieved approximately 99% precision, recall, and F1 score for the tested attack types.

Nam et al. [25] developed a generative pretrained transformer (GPT)-based CAN IDS that can learn normal CAN ID sequences to detect any small changes in the sequence due to an attack. The authors used two GPT NNs arranged bi-directionally to learn both historical and future CAN ID sequences. The authors in [25] evaluated their CAN IDS for flooding, spoofing, replay, and fuzzing attacks, which showed a minimum 95% attack detection F-measure.

Zhang et al. [26] developed a CAN fuzz testing method to filter fuzzy messages using a GAN to generate fuzzy messages and an Adaptive Boosting or AdaBoost-based detection system to detect anomalies in CAN communication due to the fuzzy message injection. The Adaptive Boosting-based anomaly monitor in [26] was shown to be able to detect even slight anomalies in CAN communication.

Zhao et al. [27] developed a CAN IDS based on Auxiliary Classifier GAN (ACGAN) and out-of-distribution detection. Their proposed IDS consists of two stages of classifiers. In the first stage, an ACGAN-based multi-class classifier is responsible for classifying normal and known attacks and filtering out-of-distribution samples. In the second stage, a binary classifier is responsible for detecting unknown attacks from the out-of-distribution samples found in the first-stage classifier. The authors in [27] achieved an average of 99% recall, 99% precision, and 99% F1 score for DoS, fuzzy, gear spoofing, and RPM spoofing attack detections.

Zhao et al. [28] developed a novel CAN intrusion attack method called the same origin method execution (SOME) attack and a GAN-based CAN IDS. Their proposed CAN IDS utilizes one-hot encoding with an adopted GAN known as GANomaly [29]. The authors in [28] tested their CAN IDS against spoofing, bus-off, masquerade, and SOME attacks and achieved a minimum of 91% and 93% detection accuracy

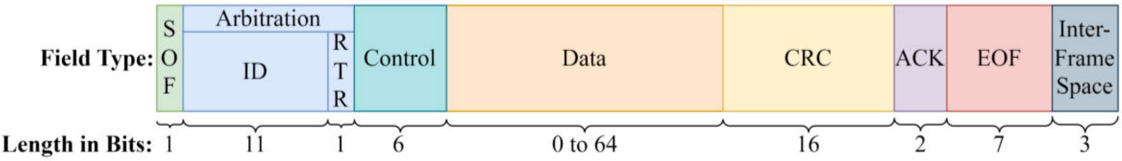


FIGURE 1. Structure of a CAN frame.

for two test vehicles under all four types of attacks mentioned above.

Although the studies listed in this section utilize one or more generative NN models for either training their IDSs or detecting in-vehicle CAN intrusions, or doing both, none of the studies has considered embedding the label as a set of pixels directly into the corresponding CAN image, and then reconstructing the CAN image using a quantum RBM for CAN intrusion detection. This study developed a hybrid quantum-classical CAN intrusion detection framework leveraging RBM's generative ability to reconstruct the embedded labeling pixels in a CAN image and then utilize the reconstructed CAN image for CAN intrusion detection.

IV. HYBRID QUANTUM-CLASSICAL FRAMEWORK FOR CAN INTRUSION DETECTION

In this section, we present the hybrid quantum-classical framework for CAN intrusion detection that utilizes a classical computer for data preprocessing and a quantum computer for image reconstruction and classification. The steps involved in our hybrid quantum-classical framework for CAN intrusion detection are presented in Fig. 2.

A. CLASSICAL COMPUTER-BASED DATA PREPROCESSING

As mentioned in Section II, CAN messages can include different data fields, such as timestamp, CAN arbitration ID (i.e., an ID allocated to an in-vehicle system based on its CAN message broadcasting priority), DLC (i.e., a code that represents the length of the data contained in a CAN message), data (i.e., a string that contains various information in an encoded format related to the system that is broadcasting the CAN message), CRC sequence (i.e., an error-detecting code), and acknowledgment. In our hybrid quantum-classical CAN intrusion detection framework, we convert a set of CAN messages into a CAN image that not only contains the information included in the CAN messages but also contains a label representing whether the CAN messages are normal messages or attack messages (i.e., injected false messages by an attacker). The steps to convert the CAN messages into label-embedded CAN images are as follows, 1) primary CAN image construction, 2) feature extraction using a classical NN, and 3) binary encoding and label embedding. Fig. 3 presents the details of data preprocessing based on a classical computer, which we explain in this subsection.

1) PRIMARY CAN IMAGE CONSTRUCTION

The data contained in a CAN message is typically encoded (e.g., HEX-encoded). Thus, the first step for primary CAN image construction is to decode the encoded data using the corresponding database CAN (DBC); a DBC contains relevant information to decode CAN messages that may vary based on a vehicle's make, model, and year. Once decoded, a set of features containing data from different in-vehicle sensors is obtained. Then, we construct an N × N primary CAN image using a set of N consecutive CAN messages with the same CAN ID, where N is the number of decoded features present in a CAN message with that CAN ID. Thus, in a primary CAN image, a row represents a single CAN message, whereas a column represents a feature.

2) FEATURE EXTRACTION USING A CLASSICAL NN

We use a classical NN to extract features from an N × N primary CAN image to create an 8 × 8 secondary CAN image following the feature extraction procedure presented in [18]. In a later stage, when we utilize a QA-based RBM, we consider 64 neurons in each layer. Thus, our motivation for creating 8 × 8 CAN images from N × N primary CAN images is to be able to map each pixel of an image to a neuron of the visible layer of an RBM, which we will discuss in Section IV-B. The feature extraction using a classical NN can be described as follows,

$$L_{8\times8} = L_{p-1} \bigcirc L_{p-2} \bigcirc L_{p-3} \bigcirc \ldots.. \bigcirc L_1 \bigcirc L_0 \tag{1}$$

$$L_n : x_{n-1} \longrightarrow x_n = \phi(W_n x_{n-1} + v_n) \tag{2}$$

Here, $L_{8\times8}$ denotes the output of a classical NN, p denotes the number of layers, L_n denotes the n^{th} layer of the classical NN, x_{n-1} denotes the input vector of L_n, x_n denotes the output vector of L_n, W_n denotes the weight, v_n denotes a bias vector, and ϕ denotes a non-linear function. The model parameters (W_n, p, v_n) are optimized while training the classical NN.

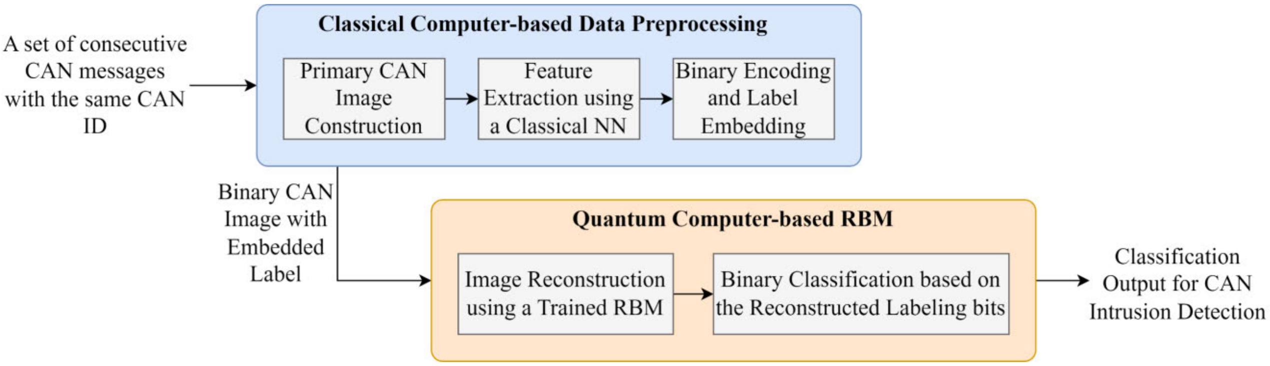

A set of consecutive CAN messages with the same CAN ID
Classical Computer-based Data Preprocessing
Primary CAN Image Construction
Feature Extraction using a Classical NN
Binary Encoding and Label Embedding
Binary CAN Image with Embedded Label
Quantum Computer-based RBM
Image Reconstruction using a Trained RBM
Binary Classification based on the Reconstructed Labeling bits
Classification Output for CAN Intrusion Detection

FIGURE 2. A hybrid quantum-classical CAN intrusion detection framework.

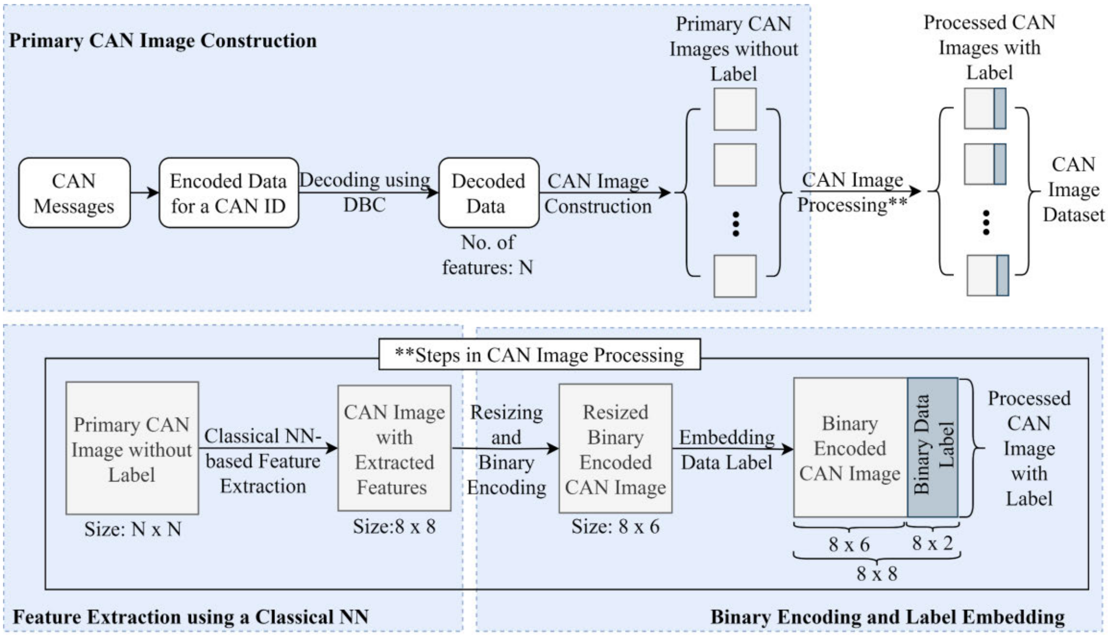

Primary CAN Image Construction
CAN Messages
Encoded Data for a CAN ID
Decoding using DBC
Decoded Data
No. of features: N
CAN Image Construction
Primary CAN Images without Label
CAN Image Processing**
Processed CAN Images with Label
CAN Image Dataset
**Steps in CAN Image Processing
Primary CAN Image without Label
Size: N x N
Classical NN-based Feature Extraction
CAN Image with Extracted Features
Size:8 x 8
Resizing and Binary Encoding
Resized Binary Encoded CAN Image
Size: 8 x 6
Embedding Data Label
Binary Encoded CAN Image
Binary Data Label
8 x 6
8 x 2
8 x 8
Processed CAN Image with Label
Feature Extraction using a Classical NN
Binary Encoding and Label Embedding

FIGURE 3. Steps in classical computer-based data preprocessing.

3) BINARY ENCODING AND LABEL EMBEDDING

We resize the 8 × 8 secondary CAN images into 8 × 6 reduced-size secondary CAN images to allocate two right-most columns, i.e., a total of 16 bits of each image, for embedding the corresponding label to indicate whether the image is a normal image or an attack image. Then, binary encoding is performed on each 8 × 6 image. In a binary CAN image, each row represents a six-bit binary string: $x_m = (b_1, b_2, \ldots, b_6)$, where $b_i \in \{0, 1\} \forall i = 1, 2, \ldots, 6$, and m represents the row number. Each bit is a binary representation of a pixel in a 8 × 6 reduced-size secondary CAN image, e.g., $b_1 = 1$ in x_m indicates the first feature is present in the m-th row, whereas $b_1 = 0$ indicates the first feature is absent in the m-th row. Binary image thresholding with a fixed threshold value of 0.5 is used to generate a binary CAN image x_m from an 8 × 6 reduced-size secondary CAN image [18]. After performing binary encoding, each binary CAN image of 8 × 6 size is embedded with the corresponding image label, i.e., whether the image represents an attack image or a normal image. This embedding is either an 8 × 2 matrix of ones when an image represents an attack image, or an 8 × 2 matrix of zeroes when an image represents a normal image. Then, this 8 × 2 matrix is concatenated horizontally with the corresponding 8 × 6 binary CAN image giving each final processed binary CAN image with the embedded label an overall size of 8 × 8.

B. QUANTUM RBM FOR IMAGE RECONSTRUCTION AND BINARY CLASSIFICATION

The final processed binary CAN images with embedded labels are reconstructed by a quantum RBM. The reconstructed CAN images are then used for binary classification based on the reconstructed bits in the images dedicated to labeling. In this framework, we consider an adiabatic quantum computer offered by D-Wave, which is based on superconducting electronics and allows QA-based sampling [30], for image reconstruction and classification. This subsection starts with the motivation for using quantum computers for training RBM models and then presents the details of training a quantum RBM for CAN image reconstruction.

Quantum computing utilizes quantum mechanics principles to process information. As opposed to classical computers that use classical bits (i.e., 0 and 1), quantum computers use quantum bits (qubits) represented by photons, atoms, ions, etc., to process information. In addition, due to quantum phenomena, such as superposition and entanglement, quantum computing has the potential to process information at a much higher rate compared to classical computers. Unlike a classical bit that can only take a value of 0 or 1, a qubit can be in a state of 0, 1, or any combination of 0 and 1, known as superposition. A classical system with four bits can be used to represent only one out of 16 combinations at once, whereas a quantum computer with four qubits can represent all 16 combinations simultaneously using superposition. On the other hand, the entanglement of two qubits refers to a quantum phenomenon that enables a quantum computer to instantaneously determine the state of an entangled qubit by only measuring the state of the other entangled qubit. Because of this uniqueness, quantum computing has shown tremendous potential in speeding up the process of solving complex problems, such as complex non-linear and non-convex optimization problems. This is particularly beneficial for training ML or DL models since the gradient descent-based model parameter

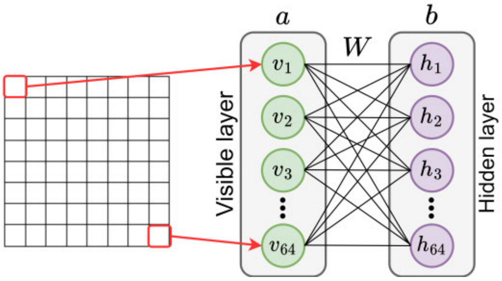


FIGURE 4. Schematic of an RBM architecture.

update rule is among the most fundamental algorithms for developing most ML and DL models. However, for a complex non-linear optimization problem, gradient descent-based ML or DL model training often suffers from non-convergence issues due to getting stuck at a local minimum. Thus, reaching the global minimum for such problems is sometimes challenging and computationally expensive for classical computers, which can be eased down by using a quantum approach.

In this study, the authors are particularly interested in developing RBM models using a quantum computer. RBM is an energy-based stochastic generative NN model, which can be represented by a bipartite graph (i.e., only nodes from alternate layers between the two layers of the bipartite graph can be connected) consisting of two layers of nodes known as visible layer and hidden layer nodes (as shown in Fig. 4). Each connection is associated with a weight while the corresponding nodes are associated with biases. The energy function of an RBM is given by,

$$E\left(v,h\right)=-\sum_{i}a_iv_i-\sum_{j}b_jh_j-\sum_{i,j}v_ih_jw_{ij} \tag{3}$$

where, v_i and h_j are two visible and hidden layer nodes, and a_i and b_j are their associated biases, respectively; and w_{ij} is the weight of the connection between v_i and h_j. Here, the probability of a given state (v, h) is given by,

$$p\left(v,h\right)=\frac{1}{Z}e^{-E(v,h)} \tag{4}$$

where, Z is a partition function used for normalization and is given by,

$$Z=\sum_{(v,h)}e^{-E(v,h)} \tag{5}$$

As it is difficult to compute all the possible combinations of v and h, computing Z is a computationally expensive process. In CD-based training, this problem is simplified by assuming that the variables are independent. The readers are referred to [14] for CD-based training.

Alternatively, an RBM model can be mapped to a binary quadratic model (BQM), in which the variables are essentially binary, and the model is a combination of linear and quadratic terms. The objective function of a BQM is given by the Ising model, which is shown in the following equation [31],

$$E_{ising}\left(\boldsymbol{s}\right)=\sum_{i=1}^{N}h_is_i+\sum_{i=1}^{N}\sum_{j=i+1}^{N}J_{i,j}s_is_j \tag{6}$$

where, $\boldsymbol{s}$ is a vector of binary variables representing the spins, i.e., $s_i \in \{-1,+1\}$, and h denotes the linear coefficients associated with the qubit biases, and J denotes the quadratic coefficients associated with the coupling strengths. A similar way to represent the BQM models in computer science is the quadratic unconstrained binary optimization (QUBO) model, where the objective function is given by the following equation [31],

$$f\left(\boldsymbol{x}\right)=\sum_{i}Q_{ii}x_i+\sum_{i<j}Q_{ij}x_ix_j \tag{7}$$

where, $\boldsymbol{x}$ is a vector of binary variables such that $x_i \in \{0, 1\}$, $\boldsymbol{Q}$ is an N × N upper triangular matrix consisting real weights, i.e., Q_{ij} represents the element of the i^{th} row and j^{th} column of $\boldsymbol{Q}$, and Q_{ii} represents the diagonal element of the i^{th} row of $\boldsymbol{Q}$; and x_i and x_j are the i^{th} and the j^{th} elements of $\boldsymbol{x}$, which is a vector of binary variables. Note that the conversion between the functions presented in (6) and (7) is trivial, as (7) simply performs a linear transformation to change the spins (s_i) to a binary variable x_i, i.e., $x_i = (1 + s_i)/2$. Thus, the energy function of an RBM in (3) can also be mapped to the objective function of a QUBO problem in (7).

A QUBO problem as in (7) can be expressed as a Hamiltonian given by the following equation,

$$H\left(\boldsymbol{x}\right)=-\sum_{i}Q_{ii}\sigma_i^z-\sum_{i<j}Q_{ij}\sigma_i^z\sigma_j^z \tag{8}$$

where, σ_i^z denotes a Pauli-Z gate applied on the i-th qubit. In [32], the authors presented how to solve such problems using QA by extending the Hamiltonian in (8) with a transverse field. QA is an optimization technique to find the global optimum of an objective function from a given set of candidates. The Hamiltonian with a transverse field can be written as follows,

$$H\left(\boldsymbol{x}\right)=-A\left(\boldsymbol{x}\right)\sum_{i}\sigma_i^x-B\left(\boldsymbol{x}\right)\left[\sum_{i}Q_{ii}\sigma_i^z+\sum_{i<j}Q_{ij}\sigma_i^z\sigma_j^z\right] \tag{9}$$

where, A and B are two weighting functions, and σ_i^x denotes a Pauli-X gate applied on the i-th qubit. In [32], the authors proved that using the Hamiltonian in (9), QA could lead to fast convergence (i.e., reaching the ground state with the lowest energy in (9)) with a much higher probability than its classical counterpart.

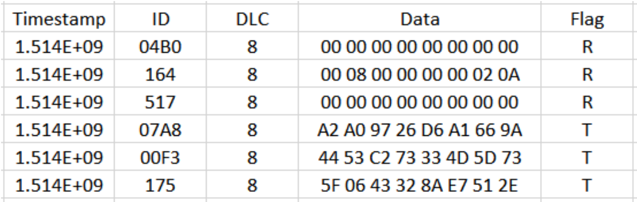
D-Wave is a commercially available QA system that can be utilized to solve such QUBO problems using the Hamiltonian given in (9) [31]. Thus, the authors chose to utilize a D-Wave QA system (i.e., D-Wave Advantage 4.1 system with over 5,000 qubits) for training the quantum RBM models in this study. In addition, using D-wave's quantum sampler, the authors can obtain accurate samples from the original probability distribution of the model given in (4) [33]. Obtaining accurate samples from the original probability distribution is a computationally expensive task for classical computers. However, unlike CD-based training, assuming that the variables are independent is unnecessary while using QA-based training. The authors refer the readers to [33] for the details of an RBM implementation using QUBO and QA-based training, which the authors adopted in this framework.

V. EVALUATION METHOD

This section presents the evaluation method for evaluating our hybrid quantum-classical CAN intrusion detection framework based on data collected from a real-world vehicle. To evaluate the efficacy of the framework, we compared the intrusion detection performance of our framework with a similar but classical-only framework, i.e., all steps of the classical-only framework are accomplished in a classical computer, including the RBM-based image reconstruction. In this section, first, we will discuss the datasets we used for this evaluation. Next, we will explain the details of CAN intrusion detection based on the framework presented in Section IV followed by a discussion on the evaluation metrics we used.

A. DATASET

For evaluation, we used a CAN intrusion dataset created by the Hacking and Countermeasure Research Lab (HCRL) [34]. The CAN intrusion datasets provided in [34] include fuzzy, malfunction, and replay attack datasets. For this study, we used a fuzzy attack dataset generated by injecting random CAN messages to the CAN bus of a KIA Soul vehicle. The dataset is already labeled and includes both the fuzzy CAN messages and the normal CAN messages. As shown in Fig. 5, the dataset contains the following fields: (i) timestamp, (ii) CAN ID (in Hex), (iii) data length code (DLC), (iv) data (encoded as a Hex string), and (v) flag or label ('R' represents a normal message, and 'T' represents an injected message). We divided the messages into different datasets based on the associated CAN IDs and selected three datasets based on randomly chosen CAN IDs, i.e., dataset 1 (with CAN ID: 0x220), dataset 2 (with CAN ID: 0x316), and dataset 3 (with CAN ID: 0x329), that contain both the normal and injected CAN messages. Each CAN ID is dedicated to broadcasting a particular set of information. Thus, the three datasets used here contain different sets of information encoded as Hex strings. Details of the datasets are presented in Table 1.



Timestamp	ID	DLC	Data	Flag
1.514E+09	04B0	8	00 00 00 00 00 00 00 00	R
1.514E+09	164	8	00 08 00 00 00 00 02 0A	R
1.514E+09	517	8	00 00 00 00 00 00 00 00	R
1.514E+09	07A8	8	A2 A0 97 26 D6 A1 66 9A	T
1.514E+09	00F3	8	44 53 C2 73 33 4D 5D 73	T
1.514E+09	175	8	5F 06 43 32 8A E7 51 2E	T

FIGURE 5. CAN fuzzy attack dataset.

B. CAN INTRUSION DETECTION

First, we decoded the encoded data fields in each dataset using a generic Database CAN (DBC) file for KIA vehicles from the OpenDBC repository [35]. After decoding, we obtained several features containing data from different in-vehicle sensors. Table 1 lists some example features for each dataset. Next, we constructed primary CAN images from the decoded CAN messages in each dataset. Each primary CAN image is obtained by vertically stacking N consecutive decoded CAN messages from a dataset, where N is the number of decoded features in that dataset. Then, we trained a classical NN to extract features from the primary CAN images to form 8 × 8 secondary CAN images, as explained in Section IV-A-II. The 8 × 8 secondary CAN images were resized to 8 × 6 to concatenate two columns that represent the labeling bits. After concatenating the labels with the 8 × 6 CAN images, we obtained the final processed 8 × 8 CAN images with embedded labels, as explained in Section IV-A-III. Fig. 6 provides some examples of the binary encoded CAN images with embedded labels.

The final processed CAN images in each dataset were divided into a training dataset (including randomly

TABLE 1. Details of the datasets.

Dataset	Size	No. of normal messages	No. of attack (injected) messages	No. of features[a]	Some example features[b]
1	2384	1192	1192	14	LAT_ACCEL, LONG_ACCEL, CYL_PRES, YAW_RATE, YAW_RATE_DIAG, and ESP12_Checksum
2	2648	1324	1324	13	SWI_IGK, F_N_ENG, ACK_TCS, PUC_STAT, TQ_COR_STAT, and TQFR
3	1800	900	900	19	MUL_CODE, TEMP_ENG, ACK_ES, TPS, ACC_ACT, ENG_CHR, and ENG_VOL

[a,b] These information are available when the data is decoded.

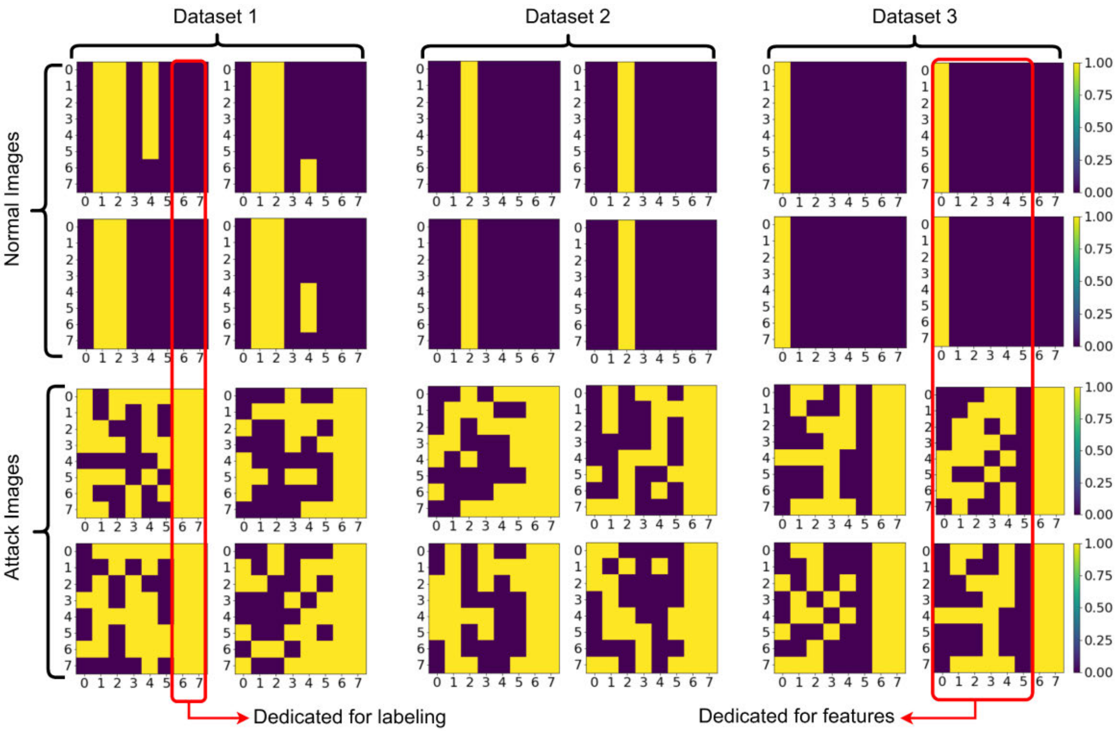


FIGURE 6. Examples of processed binary CAN images with embedded labels.

shuffled 80% of the CAN images) and a test dataset (including the remaining 20% of the CAN images). For each training dataset, we trained a classical RBM model using CD-based training and a quantum RBM model using QA-based training. The QA-based training of RBM models was performed using the D-Wave Advantage 4.1 System, whereas the CD-based training for the classical RBM models was performed in a classical computer. The hyperparameters (i.e., learning rate, number of epochs, weights, and biases) of each RBM model were optimized to yield the best CAN intrusion detection performance. Both classical and quantum RBM models included 64 visible layer nodes and 64 hidden layer nodes that resulted in 64 visible layer biases, 64 hidden layer biases, and 64 × 64 weights to be trained. The same training and test datasets were used for training both the classical and the quantum RBM models for comparison. The source code is provided in GitHub [36].

For evaluation, the labeling bits of each CAN image in a test dataset are first replaced by random binary bits. The trained RBM models are then used for reconstructing the CAN images in the test datasets. A reconstructed image is classified as a normal image if most of the bits among the 16 bits dedicated to labeling indicate a normal image, otherwise the reconstructed image is classified as an attack image.

C. EVALUATION METRICS

The CAN intrusion detection task in this study (i.e., fuzzy attack detection) falls under the category of binary classification (i.e., attack data or normal data). Therefore, classification accuracy (i.e., CAN intrusion detection accuracy) is considered as the primary evaluation metric in this study. Recall is considered as the secondary evaluation metric since it provides a measure of correctly detected attack data among all the attack data. Binary classification accuracy and recall are given by,

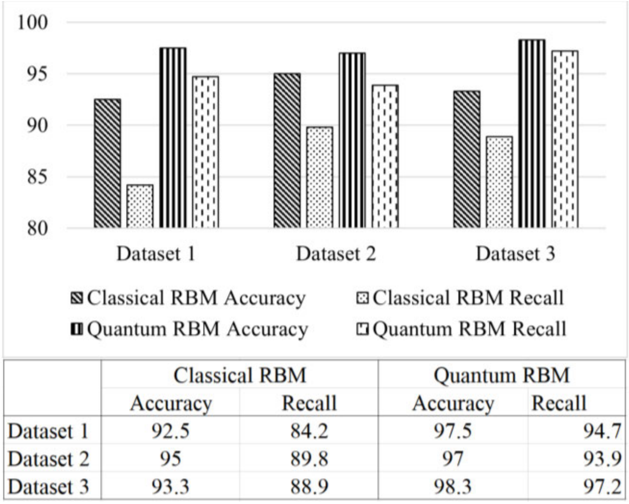
$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{10}$$

$$Recall = \frac{TP}{TP + FN} \tag{11}$$

where, TP denotes the total number of true positives, TN denotes the total number of true negatives, FP denotes the total number of false positives, and FN denotes the total number of false negatives. In addition, we utilize a confusion matrix to present a closer view at the classification performance of a model on the test dataset.

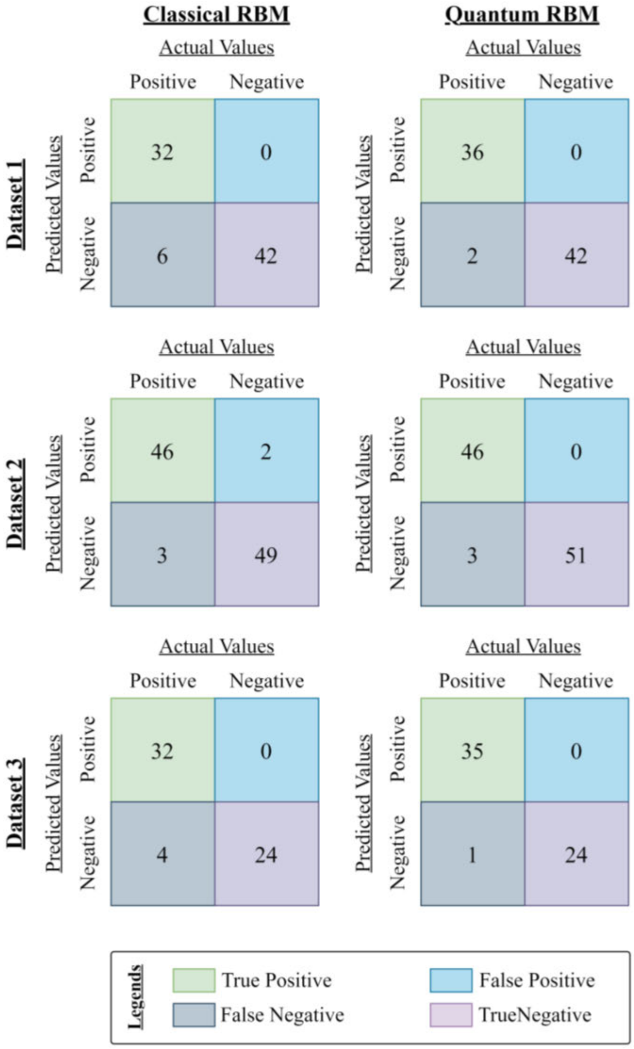
VI. EVALUATION RESULTS AND DISCUSSIONS

Fig. 7 presents the accuracies and recalls of the classical RBM and the quantum RBM approaches for each dataset. As observed from Fig. 7, the quantum RBM approach outperformed the classical RBM approach for all three datasets used in this study. Among the three datasets, the minimum and maximum CAN intrusion detection accuracies while using the quantum RBM approach were 97% and 98.3%, respectively, whereas the minimum and maximum CAN intrusion detection accuracies for the classical RBM approach were



	Classical RBM		Quantum RBM	
	Accuracy	Recall	Accuracy	Recall
Dataset 1	92.5	84.2	97.5	94.7
Dataset 2	95	89.8	97	93.9
Dataset 3	93.3	88.9	98.3	97.2

FIGURE 7. **Comparison of CAN intrusion detection performance.**



Classical RBM, Dataset 1

Predicted Values	Actual Values: Positive	Negative
Positive	32	0
Negative	6	42

Quantum RBM, Dataset 1

Predicted Values	Actual Values: Positive	Negative
Positive	36	0
Negative	2	42

Classical RBM, Dataset 2

Predicted Values	Actual Values: Positive	Negative
Positive	46	2
Negative	3	49

Quantum RBM, Dataset 2

Predicted Values	Actual Values: Positive	Negative
Positive	46	0
Negative	3	51

Classical RBM, Dataset 3

Predicted Values	Actual Values: Positive	Negative
Positive	32	0
Negative	4	24

Quantum RBM, Dataset 3

Predicted Values	Actual Values: Positive	Negative
Positive	35	0
Negative	1	24

FIGURE 8. **Confusion matrices.**

92.5% and 95%, respectively. On the other hand, the minimum and maximum recalls for the quantum RBM approach were 93.9% and 97.2%, respectively, whereas the minimum and maximum recalls for the classical RBM approach were 84.2% and 89.8%. Thus, the hybrid quantum-classical framework was able to improve both the accuracies and recalls for CAN intrusion detection on all three datasets used in this study compared to the classical-only framework. Fig. 8 shows a confusion matrix for each model's classification performance on each test dataset, which also shows that the quantum RBM models improved the classification performance on all three test datasets (contained in datasets 1, 2, and 3) compared to the classical RBM models.

The improvement in intrusion detection performance found in this study while using the quantum RBM can be attributed to several factors. Quantum DL models have been reported in the literature to achieve similar or better classification performance while being trained on a much smaller dataset compared to their classical counterparts. This implies that while being trained on the same dataset and using the same DL model architecture with the same number of model parameters, quantum DL models might achieve better classification performance compared to the classical DL models, which aligns with the observations of this study. Training ML or DL models heavily utilizes optimization-based approaches for updating the model parameters. However, a classical computing-based optimization process might get stuck at some local minima, which can be overcome by utilizing a quantum optimization approach as it leverages quantum tunneling to bypass the local minima and reach the global minimum quickly. Quantum tunneling enables atoms, electrons, or photons to pass through potential energy barriers, which helps in bypassing local minima to reach the global minimum. In addition, the hybrid framework utilized D-Wave's QA-based sampling for training the RBM models that enables accurate sampling from the original probability distribution of the models unlike the CD-based training of the RBM models used in the classical-only framework that samples from the conditional probability distribution, as discussed in Section IV-B. Also, unlike other generative NNs (e.g., generative adversarial network or GAN and generative pretrained transformer or GPT) that would require rigorous training to obtain a well-performing CAN IDS, the hybrid framework utilizes a simpler generative NN architecture of an RBM that can quickly learn to detect attacks by learning the patterns of normal and attack CAN images embedded with labeling pixels. All of the quantum RBM models in this study converged within a comparable number of epochs while yielding an overall higher attack detection accuracy and recall than the classical RBM, which proves the efficacy of the hybrid quantum-classical CAN intrusion detection framework.

VII. CONCLUSIONS

Quantum computing has the potential to build an ironclad defense against numerous cyberattacks in a transportation cyber-physical systems environment. However, given the current status of quantum computers, the best way to utilize them is to use hybrid quantum-classical approaches. In this study, we presented a hybrid quantum-classical CAN intrusion detection framework utilizing a classical NN and a quantum RBM. In this framework, data preprocessing is done in a classical computer to generate CAN images with embedded labeling pixels from CAN messages. A quantum RBM is used in the framework to reconstruct each CAN image along with its labeling pixels, which is then used for an image classification-based CAN intrusion detection. We evaluated our hybrid quantum-classical CAN intrusion detection framework on three different real-world fuzzy attack datasets and compared the CAN intrusion detection performance of the hybrid framework with a similar but classical-only framework. Based on the experiments conducted on the datasets, the minimum accuracy and recall for the hybrid framework were 97% and 93.9%, respectively, whereas for the similar but classical-only framework, the minimum CAN intrusion detection accuracy and recall were 92.5% and 84.2%, respectively. The uniqueness of this study lies in utilizing the generative ability of a generative NN (i.e., RBM) for reconstructing the labeling pixels embedded in a CAN image, which could contribute towards an accurate image classification-based CAN intrusion detection.

It should be noted that although the hybrid quantum-classical CAN intrusion detection framework utilizes a quantum computer to train the RBM models, once the RBM models are trained to yield a desired intrusion detection performance, the quantum computer is not used anymore. The trained models can then be transferred to an in-vehicle computing unit where the entire process of CAN intrusion detection will take place. This will help minimize the end-to-end latency in a CAN IDS, which then could support a real-time in-vehicle intrusion detection application.

This study used QA-based training to develop the RBM models for the hybrid quantum-classical CAN IDS. Future studies should focus on developing gate-based RBM models for CAN IDS and compare them with the QA-based RBM models.

ACKNOWLEDGMENT

Any opinions, findings, conclusions, and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of C^2M^2, and the U.S. Government assumes no liability for the contents or use thereof.

REFERENCES

[1] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 3, pp. 919–933, Mar. 2020, doi: 10.1109/TITS.2019.2908074.

[2] C. Young, J. Zambreno, H. Olufowobi, and G. Bloom, "Survey of automotive controller area network intrusion detection systems," *IEEE Design Test*, vol. 36, no. 6, pp. 48–55, Dec. 2019, doi: 10.1109/MDAT.2019.2899062.

[3] S.-F. Lokman, A. T. Othman, and M.-H. Abu-Bakar, "Intrusion detection system for automotive controller area network (CAN) bus system: A review," *EURASIP J. Wireless Commun. Netw.*, vol. 2019, no. 1, p. 184, Jul. 2019, doi: 10.1186/s13638-019-1484-3.

[4] W. Lo, H. Alqahtani, K. Thakur, A. Almadhor, S. Chander, and G. Kumar, "A hybrid deep learning based intrusion detection system using spatial–temporal representation of in-vehicle network traffic," *Veh. Commun.*, vol. 35, Jun. 2022, Art. no. 100471, doi: 10.1016/j.vehcom.2022.100471.

[5] T. Moulahi, S. Zidi, A. Alabdulatif, and M. Atiquzzaman, "Comparative performance evaluation of intrusion detection based on machine learning in in-vehicle controller area network bus," *IEEE Access*, vol. 9, pp. 99595–99605, 2021, doi: 10.1109/ACCESS.2021.3095962.

[6] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198, doi: 10.1016/j.vehcom.2019.100198.

[7] O. Minawi, J. Whelan, A. Almehmadi, and K. El-Khatib, "Machine learning-based intrusion detection system for controller area networks," in *Proc. 10th ACM Symp. Design Anal. Intell. Veh. Netw. Appl.* New York, NY, USA: Association for Computing Machinery, Nov. 2020, pp. 41–47, doi: 10.1145/3416014.3424581.

[8] M. D. Hossain, H. Inoue, H. Ochiai, D. Fall, and Y. Kadobayashi, "Long short-term memory-based intrusion detection system for in-vehicle controller area network bus," in *Proc. IEEE 44th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Jul. 2020, pp. 10–17, doi: 10.1109/COMPSAC48688.2020.00011.

[9] M. R. Moore, R. A. Bridges, F. L. Combs, M. S. Starr, and S. J. Prowell, "Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: A data-driven approach to in-vehicle intrusion detection," in *Proc. 12th Annu. Conf. Cyber Inf. Secur. Res.* New York, NY, USA: Association for Computing Machinery, Apr. 2017, pp. 1–4, doi: 10.1145/3064814.3064816.

[10] S. Jin, J.-G. Chung, and Y. Xu, "Signature-based intrusion detection system (IDS) for in-vehicle CAN bus network," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2021, pp. 1–5, doi: 10.1109/ISCAS51556.2021.9401087.

[11] Y. Dong, W. Hu, J. Zhang, M. Chen, W. Liao, and Z. Chen, "Quantum beetle swarm algorithm optimized extreme learning machine for intrusion detection," *Quantum Inf. Process.*, vol. 21, no. 1, p. 9, Jan. 2022, doi: 10.1007/s11128-021-03311-w.

[12] J. Chen, X. Qi, L. Chen, F. Chen, and G. Cheng, "Quantum-inspired ant lion optimized hybrid k-means for cluster analysis and intrusion detection," *Knowl.-Based Syst.*, vol. 203, Sep. 2020, Art. no. 106167, doi: 10.1016/j.knosys.2020.106167.

[13] D. Caivano, M. De Vincentiis, F. Nitti, and A. Pal, "Quantum optimization for fast CAN bus intrusion detection," in *Proc. 1st Int. Workshop Quantum Program. Softw. Eng.* New York, NY, USA: Association for Computing Machinery, Nov. 2022, pp. 15–18, doi: 10.1145/3549036.3562058.

[14] G. E. Hinton, "A practical guide to training restricted Boltzmann machines," in *Neural Networks: Tricks of the Trade*. Berlin, Germany: Springer, 2012, pp. 599–619.

[15] S. H. Adachi and M. P. Henderson, "Application of quantum annealing to training of deep neural networks," 2015, *arXiv:1510.06356*.

[16] D. Korenkevych, Y. Xue, Z. Bian, F. Chudak, W. G. Macready, J. Rolfe, and E. Andriyash, "Benchmarking quantum hardware for training of fully visible Boltzmann machines," 2016, *arXiv:1611.04528*.

[17] V. Dixit, R. Selvarajan, M. A. Alam, T. S. Humble, and S. Kais, "Training restricted Boltzmann machines with a D-wave quantum annealer," *Frontiers Phys.*, vol. 9, Jun. 2021, Art. no. 589626, doi: 10.3389/fphy.2021.589626.

[18] M. Islam, M. Chowdhury, Z. Khan, and S. M. Khan, "Hybrid quantum-classical neural network for cloud-supported in-vehicle cyberattack detection," *IEEE Sensors Lett.*, vol. 6, no. 4, pp. 1–4, Apr. 2022, doi: 10.1109/LSENS.2022.3153931.

[19] H. J. Jo and W. Choi, "A survey of attacks on controller area networks and corresponding countermeasures," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6123–6141, Jul. 2022, doi: 10.1109/TITS.2021.3078740.

[20] B. Lampe and W. Meng, "A survey of deep learning-based intrusion detection in automotive applications," *Expert Syst. Appl.*, vol. 221, Jul. 2023, Art. no. 119771, doi: 10.1016/j.eswa.2023.119771.

[21] A. Buscemi, I. Turcanu, G. Castignani, A. Panchenko, T. Engel, and K. G. Shin, "A survey on controller area network reverse engineering," *IEEE Commun. Surveys Tuts.*, early access, Apr. 5, 2023, doi: 10.1109/COMST.2023.3264928.

[22] S. Rajapaksha, H. Kalutarage, M. O. Al-Kadri, A. Petrovski, G. Madzudzo, and M. Cheah, "AI-based intrusion detection systems for in-vehicle networks: A survey," *ACM Comput. Surv.*, vol. 55, no. 11, pp. 237:1-237:40, Feb. 2023, doi: 10.1145/3570954.

[23] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in *Proc. 16th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2018, pp. 1–6, doi: 10.1109/PST.2018.8514157.

[24] G. Xie, L. T. Yang, Y. Yang, H. Luo, R. Li, and M. Alazab, "Threat analysis for automotive CAN networks: A GAN model-based intrusion detection technique," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4467–4477, Jul. 2021, doi: 10.1109/TITS.2021.3055351.

[25] M. Nam, S. Park, and D. S. Kim, "Intrusion detection method using bi-directional GPT for in-vehicle controller area networks," *IEEE Access*, vol. 9, pp. 124931–124944, 2021, doi: 10.1109/ACCESS.2021.3110524.

[26] H. Zhang, K. Huang, J. Wang, and Z. Liu, "CAN-FT: A fuzz testing method for automotive controller area network bus," in *Proc. Int. Conf. Comput. Inf. Sci. Artif. Intell. (CISAI)*, Sep. 2021, pp. 225–231, doi: 10.1109/CISAI54367.2021.00050.

[27] Q. Zhao, M. Chen, Z. Gu, S. Luan, H. Zeng, and S. Chakrabory, "CAN bus intrusion detection based on auxiliary classifier GAN and out-of-distribution detection," *ACM Trans. Embed. Comput. Syst.*, vol. 21, no. 4, pp. 45:1-45:30, Sep. 2022, doi: 10.1145/3540198.

[28] Y. Zhao, Y. Xun, J. Liu, and S. Ma, "GVIDS: A reliable vehicle intrusion detection system based on generative adversarial network," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2022, pp. 4310–4315, doi: 10.1109/GLOBECOM48099.2022.10001410.

[29] S. Akcay, A. Atapour-Abarghouei, and T. P. Breckon, "GANomaly: Semi-supervised anomaly detection via adversarial training," in *Computer Vision—ACCV 2018* (Lecture Notes in Computer Science), C. V. Jawahar, H. Li, G. Mori, and K. Schindler, Eds. Cham, Switzerland: Springer, 2019, pp. 622–637, doi: 10.1007/978-3-030-20893-6_39.

[30] *What is Quantum Annealing?—D-Wave System Documentation Documentation*. Accessed: Jun. 29, 2022. [Online]. Available: https://docs.dwavesys.com/docs/latest/c_gs_2.html

[31] D-Wave Systems. *Solving Problems With Quantum Samplers—D-Wave System Documentation*. Accessed: Dec. 28, 2022. [Online]. Available: https://docs.dwavesys.com/docs/latest/c_gs_3.html#qubo

[32] T. Kadowaki and H. Nishimori, "Quantum annealing in the transverse Ising model," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 58, no. 5, pp. 5355–5363, Nov. 1998, doi: 10.1103/PhysRevE.58.5355.

[33] K. Kurowski, M. Slysz, M. Subocz, and R. Różycki, "Applying a quantum annealing based restricted Boltzmann machine for MNIST handwritten digit classification," *Comput. Methods Sci. Technol.*, vol. 27, no. 3, pp. 99–107, 2021, doi: 10.12921/cmst.2021.0000011.

[34] M. L. Han, B. I. Kwak, and H. K. Kim, "Anomaly intrusion detection method for vehicular networks based on survival analysis," *Veh. Commun.*, vol. 14, pp. 52–63, Oct. 2018.

[35] *OpenDBC*. Accessed: Jun. 29, 2022. [Online]. Available: https://github.com/commaai/opendbc

[36] M. S. Salek. (Nov. 24, 2022). *A Novel Hybrid Quantum-Classical CAN IDS*. Accessed: Nov. 24, 2022. [Online]. Available: https://github.com/msabbirsalek/Restricted-Boltzmann-Machine-for-CAN-IDS

M SABBIR SALEK (Graduate Student Member, IEEE) received the B.S. degree in mechanical engineering from the Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, in 2016, and the M.S. degree in civil engineering from Clemson University, Clemson, SC, USA, in 2021, where he is currently pursuing the Ph.D. degree. The Ph.D. thesis is focused on cybersecurity and resiliency for connected and autonomous vehicles.

His current research interests include cloud computing, connected and automated vehicles, transportation cyber-physical systems (TCPS), and machine learning.

PRONAB KUMAR BISWAS received the B.Sc. degree in civil engineering from the Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh, in 2015, and the M.S. degree in civil engineering from Clemson University, in 2023.

He is currently a Traffic EIT with HDR, Phoenix, AZ, USA. His current research interests include quantum artificial intelligence and connected and automated vehicles.

JACQUAN POLLARD received the B.Sc. degree in electrical engineering from the Benedict College, Columbia, SC, USA, in 2019, and the M.S. degree in civil engineering from Clemson University, Clemson, SC, USA, in 2023. The M.S. thesis is focused on using artificial intelligence and machine learning to detect the presence of fugitive methane emissions for oil and natural gas facilities.

He is currently a Electrical Engineer I with Kiewit Engineering Inc., Lenexa, KS, USA. His current research interests include artificial intelligence and machine learning for environmental forecasting applications.

JORDYN HALES received the B.S. degree in physics (mathematics) from Utah Valley University, Orem, UT, USA, in 2021. They are currently pursuing the Ph.D. degree with Clemson University, Clemson, SC, USA.

Their current research interest includes researching quantum many-body systems.

ZECHENG SHEN received the B.Sc. degree in physics from Sun Yat-sen University (SYSU), Guangzhou, China, in 2020. He is currently pursuing the Ph.D. degree with the Department of Physics and Astronomy, Clemson University, SC, USA.

His current research interests include condense matter physics and corresponding simulation methods.

VIVEK DIXIT received the M.S. and Ph.D. degrees in physics and applied physics from Mississippi State University, Starkville, MS, USA, in 2011 and 2015, respectively.

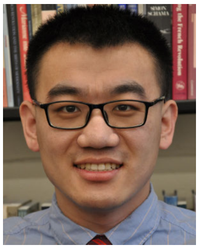
He is a former Postdoctoral Fellow with Clemson University, SC, USA, and Purdue University, Indiana, USA. During his postdoctoral period, he conducted research using quantum computers, such as D-Wave and IBM-Q, for various applications. His current research interests include applying quantum computing in machine learning and many-body physics.

MASHRUR (RONNIE) CHOWDHURY (Senior Member, IEEE) is currently the Eugene Douglas Mays Chair of transportation with Clemson University, Clemson, SC, USA. He is also the Founding Director of the National Center for Transportation Cybersecurity and Resiliency (TraCR), a USDOT National University Transportation Center (UTC) and the USDOT Tier 1 UTC Center for Connected Multimodal Mobility (C^2M^2), both headquartered with Clemson University. He is the Co-Director of the Complex Systems, Analytics and Visualization Institute (CSAVI), Clemson University. His current research interests include cyber-physical systems and cybersecurity for transportation systems and smart cities.

He served as an elected member of the IEEE ITS Society Board of Governors. He is a fellow of the American Society of Civil Engineers (ASCE) and an alumnus of the National Academy of Engineering (NAE) Frontiers of Engineering Program. He is a member of the Transportation Research Board (TRB) Committee on Intelligent Transportation Systems. He is a Registered Professional Engineer in Ohio.

SAKIB MAHMUD KHAN (Senior Member, IEEE) received the M.S. and Ph.D. degrees in civil engineering from Clemson University, Clemson, SC, USA, in 2015 and 2019, respectively.

He is a former Assistant Research Professor with the Glenn Department of Civil Engineering, Clemson University, and a former Assistant Director of the Center for Connected Multimodal Mobility (C^2M^2). His current research interests include transportation cyber-physical systems, digital infrastructure, and machine learning.



YAO WANG received the Ph.D. degree in applied physics (computational and mathematical engineering) from Stanford University, Stanford, CA, USA, in 2017.

After his graduation, he joined a MPHQ Postdoctoral Fellow with Harvard University, until 2020. He is currently an Assistant Professor with the Department of Physics and Astronomy, Clemson University. His current research interests include quantum many-body problems and corresponding quantum simulation methods.