Network Tomography-based Anomaly Detection and Localisation in Centralised In-Vehicle Network

Amani Ibraheem  
School of Engineering and Informatics  
University of Sussex  
Brighton, UK  
A.Ibraheem@sussex.ac.uk

Zhenguo Sheng  
School of Engineering and Informatics  
University of Sussex  
Brighton, UK  
Z.Sheng@sussex.ac.uk

George Parisi  
School of Engineering and Informatics  
University of Sussex  
Brighton, UK  
G.Parisis@sussex.ac.uk

Daxin Tian  
School of Transportation Science and Engineering  
Beihang University  
Beijing, China  
Dtian@buaa.edu.cn

Abstract—The new automotive Electrical/Electronic (E/E) architecture is shifting towards a new design of in-vehicle network that is based on a centralised, cross-domain architecture. Such architecture implies communication between different domains of the vehicle network. From security standpoint, such cross-traffic can easily be exploited by adversaries to gain access to different system domains, including the safety-critical ones, and perform attacks that may result in serious consequences. Accurate detection and localisation of these anomalies is important in such critical systems where false alarms cannot be tolerated. To this end, in this work, we propose an anomaly detection and localisation approach using network tomography-based monitoring solution. Compared to existing solutions, network tomography approaches require only limited number of probes and do not necessitate direct access to the vehicle's networking devices. In this work, we evaluate three types of network tomography (binary tomography, delay tomography, and deep learning-based tomography) to detect and locate anomalies in in-vehicle networks. The results show that binary tomography can accurately detect and locate Denial-of-Service (DoS) attacks in centralised in-vehicle networks.

Keywords—in-vehicle network monitoring, network tomography, binary network tomography, deep neural network, anomaly detection and localisation, denial-of-service attack

I. INTRODUCTION

Controller Area Network (CAN) [1] is the most dominant communication protocol used in automotive industry which is naturally distributed. However, modern in-vehicle networks follow the new E/E architecture that is shifting from domain-specific decentralised architecture to a cross-domain centralised architecture with few powerful computers instead of large number of control units [2]. With the cross-domain E/E architecture, the anomalies’ impacts will not only affect the domain in which the anomaly originated from, but it can be extended to other domains for which it can result in serious consequences. Therefore, monitoring the in-vehicle network is crucial to ensure the security of the network and safety of the passengers. For this, different monitoring approaches can be used. One of the most effective and needed solutions is Network Intrusion Detection System (NIDS) [3] which can be broadly categorised into signature-based NIDS and anomaly-based NIDS. One limitation with signature-based NIDS is that it cannot detect zero-day attacks due to its stringent matching rules, while anomaly-based solutions are robust against zero-day attacks [4]. To this end, we focus in this work on detecting and locating anomalies in centralised in-vehicle network architecture that is composed of multiple subsystems (i.e., domains) with cross-traffic between them. In particular, we investigate the use network tomography monitoring approach in detecting and locating anomalies within the vehicle network.

The main concept of network tomography is to monitor a small subset of the network along selected paths where the remaining subset can be inferred using the available measurements. Hence, network tomography does not require contribution from internal elements of the network [5]. There are two main benefits of using network tomography to monitor the in-vehicle network. First, due to difficulty in accessing the networking elements of the in-vehicle network, monitoring the internal network performance becomes more challenging, while network tomography, with its ability to infer the overall network performance without contribution from internal elements, can provide a suitable monitoring approach where only nodes at the edge, e.g., Electronic Control Units (ECUs), can monitor the network [6]. Second, with network tomography, only subset of the network can be monitored while the remaining can be inferred using the available measurements. This leads to reduced monitoring overhead; a feature that is highly desirable in critical systems such as in-vehicle networks.

In this work, we propose to use two types of network tomography to detect and locate anomalies in in-vehicle network. First is Delay Network Tomography (DNT) which infers the link-level status from a set of end-to-end (path-level) delay measurements. Second is Binary Network Tomography (BNT) which infers the link-level status from the end-to-end binary
measurements. For the latter type, delay metric is used to determine the end-to-end binary status. Although in this study we focus on detecting Denial of Service (DoS) attacks by monitoring the delay metric, our approach can be extended to detect other attacks that result in violations of normal network behaviour where other metrics can be used, such as loss/success rate, bandwidth consumption, etc.

This paper is organised as follows: Section II discusses the existing anomaly detection approaches and network tomography related work. System model and problem formulation are described in Section III. Our proposed anomaly detection and localisation approach is presented in Section IV. Section V describes the simulation and evaluates the obtained results. Finally, the paper is concluded in Section VI along with a discussion of limitations and future works.

II. RELATED WORK

A. Anomaly detection

A number of state-of-the-art anomaly detection solutions were proposed for the in-vehicle network. For example, to detect DoS attacks, authors in [7] proposed an intrusion detection system (IDS) that relies on measuring the time intervals of CAN messages. This approach requires a new hardware that monitor all CAN messages on the bus. To detect DoS attack, they used a single threshold for the time intervals as 0.2 milliseconds for all CAN messages. Because there are normal messages with time intervals less than 0.2 milliseconds, they used a scoring threshold to minimise false positive rate. Their approach achieved 100% accuracy when the scoring threshold is at least 4. Meaning that the IDS classify the message as DoS attack if there are 4 (or more) consecutive instances of this message with time interval less than 0.2 ms. Same authors then proposed to utilise remote frames to detect DoS attack by measuring the offset ratio (number of messages between remote frame request and its reply) and time interval of remote frame responses [8]. This method requires that remote frames for all CAN IDs to be periodically broadcast which add more overload to the network. Another approach [9] shows better results in terms of detection latency where authors used transmitter ECU’s clock offset to fingerprint ECUs. The obtained fingerprint is then used to learn the ECU’s normal behaviour. Any anomaly is then detected based on clock offset deviation; if the change in clock offset exceeds a positive or negative value, the system report this behaviour as an anomaly.

On the other hand, with the contemporary advances in artificial intelligence and machine learning (ML), more researchers are focusing on applying ML-based solutions to detect anomalies in in-vehicle network. For example authors in [10] proposed to use Generative Adversarial Network (GAN) where they converted and represented CAN data as images. Same authors used different machine learning algorithm that is based on deep convolutional neural network [11]. Their approach could only detect attacks that the model was trained on. To tackle this, they later proposed a self-supervised detection solution [12]. These methods require collecting and storing large volume of data to train the models. In addition, they cannot completely avoid false negative/positive [13] which cannot be tolerated in critical systems such as in-vehicle networks.

Unlike current monitoring approaches that either require monitoring every part of the network or rely on training large volume of data obtained from all traffic in the network, our approach only monitors subset of the network without the need to access the internal networking elements or obtain large volume datasets. In addition, it can accurately detect and locate anomalies with no false positive or false negative.

B. Network tomography

Employing network tomography in in-vehicle networks is still at its infancy with very limited number of studies. For instance, authors in [14], proposed to use network tomography as a monitoring approach for the in-vehicle network delay performance. They studied the applicability of network tomography on three E/E architectures and found that network tomography can be applied on these architectures as long as they satisfy the identifiability conditions. If the identifiability conditions are violated, [15] proposed to use a partial tomography with deep learning-based approach. Later they evaluated the proposed network tomography-based approach to infer the internal network performance and found that algebraic tomography outperforms deep learning tomography [16].

Typically, to handle anomalies in in-vehicle network, there are four main steps that need to be taken: monitoring, detection, localisation, and mitigation. The above studies have considered network tomography for the first step; which is the monitoring stage, and they did not investigate the ability of network tomography for the other steps. On the contrary, in this work we study network tomography’s ability in detecting and locating anomalies in in-vehicle network. In addition, we explore another type of tomography, i.e., binary tomography (sometimes also called boolean tomography); a branch of network tomography that is used to infer links’ states from path-level states [17].

III. SYSTEM MODEL AND PROBLEM FORMULATION

A. System Model

Table I shows the notations we used throughout this paper and their descriptions. We assume that the in-vehicle network topology is known, and we follow graph theory conventions defined in [18] to represent the network and its characteristics. We map the in-vehicle network topology into graph \( G = (V,E) \) containing a set of vertices (or nodes) \( V(G) \) interconnected through a set of edges (or links) \( E(G) \). Let \( \mathcal{E} \subset V(G) \) and \( \mathcal{R} \subset V(G) \) be two sets for edge nodes and intermediate nodes, respectively, where \( \mathcal{E} \cup \mathcal{R} = V(G) \) and \( \mathcal{E} \cap \mathcal{R} = \emptyset \).

Definition 1: Given an in-vehicle network \( G \), sets of edge nodes \( \mathcal{E} \in V(G) \) and intermediate nodes \( \mathcal{R} \in V(G) \) are defined as

- \( \mathcal{E} = \{ v \in V(G) \mid d(v) = 1 \} \); and
- \( \mathcal{R} = \{ v \in V(G) \mid d(v) \geq 2 \} \)

where \( d(v) \) is the degree of node \( v \in V(G) \).
Table I: Used notations and their descriptions.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{E} \subseteq V(G)$</td>
<td>set of edge nodes (see Definition 1) in $G$</td>
</tr>
<tr>
<td>$\mathcal{R} \subseteq V(G)$</td>
<td>set of intermediate nodes (see Definition 1) in $G$</td>
</tr>
<tr>
<td>$\mathcal{P}$</td>
<td>set of all paths between any two edge nodes in $\mathcal{E}$</td>
</tr>
<tr>
<td>$\mathcal{P}^m \subseteq \mathcal{P}$</td>
<td>set of measured paths</td>
</tr>
<tr>
<td>$\mathcal{M}$</td>
<td>set of all messages being transmitted between edge nodes in $G$</td>
</tr>
<tr>
<td>$c_m \in \mathbb{Z}^+$</td>
<td>priority level of message $m \in \mathcal{M}$</td>
</tr>
<tr>
<td>$r(A)$</td>
<td>rank of matrix $A$</td>
</tr>
<tr>
<td>$\gamma :=</td>
<td>E(G)</td>
</tr>
<tr>
<td>$\eta :=</td>
<td>\mathcal{P}^m</td>
</tr>
<tr>
<td>$v_{m} \in \mathcal{E}$</td>
<td>source node of message $m \in \mathcal{M}$</td>
</tr>
<tr>
<td>$v_{m} \in \mathcal{E}$</td>
<td>destination node of message $m \in \mathcal{M}$</td>
</tr>
<tr>
<td>$d(v)$</td>
<td>degree of node $v \in V$</td>
</tr>
<tr>
<td>$S(\cdot) \in {0, 1}$</td>
<td>status of $\cdot$ as bad ($S(\cdot) = 1$) or good ($S(\cdot) = 0$)</td>
</tr>
<tr>
<td>$y_i^p \in {0, 1}$</td>
<td>status measurement of path $p_i \in \mathcal{P}$</td>
</tr>
<tr>
<td>$y_i^p \in \mathbb{R}^+$</td>
<td>delay measurement of path $p_i \in \mathcal{P}$</td>
</tr>
</tbody>
</table>

While the status of each path can be determined by measuring the status of each link it passes through

$$S(p_i) = \begin{cases} 0, & \text{if } S(e_j) = 0 \forall e_j \in p_i \\ 1, & \text{if } S(e_j) = 1 \exists e_j \in p_i \end{cases},$$

where $i \in \{1, \ldots, |\mathcal{P}|\}$, $j \in \{1, \ldots, \gamma\}$, and $\alpha_{e_j}$ and $\beta_{e_j}$ are threshold values for the minimum and maximum link-level delay of link $e_j \in E(G)$ in the normal network behaviour, and $x_j$ is the measured link-level delay of link $e_j \in E(G)$.

C. Objectives

Our main objectives are as follows
1) First, determine the status of $G$ as either $S(G) = 0$ or $S(G) = 1$ (detection phase);
2) if $S(G) = 1$, then the second objective is to locate the anomalous link $e_j \in E(G)$ with $S(e_j) = 1$ (localisation phase).

D. Assumptions

Throughout this paper we adopt the following assumptions
1) Nodes’ clocks are synchronised. This is valid assumption for in-vehicle wired networks.
2) All messages transmitted in the network are CAN (periodic) messages.
3) We assume that there is single source of DoS attack at a time.
4) There is one single path between any two edge nodes in $\mathcal{E}$.
5) Only edge nodes in $\mathcal{E}$ can monitor the end-to-end performance.

IV. PROPOSED SOLUTION

A. Network Tomography

Formally, network tomography is expressed as the following linear system

$$y = A \otimes x$$

where $y = [y_1, y_2, \ldots, y_{\eta}]^T$ is a vector of known path-level measurements, $A$ is a $\eta \times \gamma$ measurement matrix ($\eta := |\mathcal{P}^m|$ and $\gamma := |E(G)|$) and $x = [x_1, x_2, \ldots, x_{\gamma}]^T$ is a vector of unknown link-level metrics. Note that the routing in in-vehicle network is deterministic and there is only one single path in use between any two edge nodes $v_i, v_j \in \mathcal{E}$, where $i, j \in \{1, \ldots, |\mathcal{E}|\}$ and $i \neq j$. Thus, the measurement matrix $A$ is a binary matrix with entries $a_{ij} \in \{0, 1\}$, $i \in \{1, \ldots, \eta\}$, $j \in \{1, \ldots, \gamma\}$. If path $i$ traverses link $j$, we say $a_{ij} = 1$, otherwise $a_{ij} = 0$. The operation $\otimes$ depends on the problem type. If the problem is additive (e.g., delay or packet success/loss rate tomography) then $\otimes$ is matrix multiplication operation. For boolean problems, $\otimes$ is the boolean matrix multiplication, i.e., $y_i = \bigvee_j (a_{ij} \land x_j)$. 

In Fig. 1, the gateway is an intermediate node, while ECUs are edge nodes. Let $p_i = \{e_j \mid e_j \in E(G)\}$ be an end-to-end path (or simply a path) between two nodes in $\mathcal{E}$ and it is represented as a set of links that are traversed by $p_i$. Let $\mathcal{P}$ be the set of all possible paths in $G$. Further, let $\mathcal{M}$ represents a set of messages transmitted by nodes in $\mathcal{E}$. Each message $m \in \mathcal{M}$ is associated with priority level $c_m$ called message identifier (ID). In CAN, the message ID is used to indicate the priority of the message. The lower the value of $c_m$ the higher the priority level of message $m$.

B. Problem Statement

To detect the status of $G$, we need to examine its traffic. We say that $S(G) = 1$ if there is at least one anomalous path $p_i$, $i \in \{1, \ldots, |\mathcal{P}|\}$, with $S(p_i) = 1$ and $S(G) = 0$ if status of all paths in $\mathcal{P}$ is normal. Formally,

$$S(G) = \begin{cases} 0, & \text{if } S(p_i) = 0 \forall p_i \in \mathcal{P} \\ 1, & \text{if } S(p_i) = 1 \exists p_i \in \mathcal{P} \end{cases}$$

While the status of each path can be determined by measuring the status of each link it passes through

$$S(p_i) = \begin{cases} 0, & \text{if } S(e_j) = 0 \forall e_j \in p_i \\ 1, & \text{if } S(e_j) = 1 \exists e_j \in p_i \end{cases},$$

where $i \in \{1, \ldots, |\mathcal{P}|\}$, $j \in \{1, \ldots, \gamma\}$, and $\alpha_{e_j}$ and $\beta_{e_j}$ are threshold values for the minimum and maximum link-level delay of link $e_j \in E(G)$ in the normal network behaviour, and $x_j$ is the measured link-level delay of link $e_j \in E(G)$.

C. Objectives

Our main objectives are as follows
1) First, determine the status of $G$ as either $S(G) = 0$ or $S(G) = 1$ (detection phase);
2) if $S(G) = 1$, then the second objective is to locate the anomalous link $e_j \in E(G)$ with $S(e_j) = 1$ (localisation phase).

D. Assumptions

Throughout this paper we adopt the following assumptions
1) Nodes’ clocks are synchronised. This is valid assumption for in-vehicle wired networks.
2) All messages transmitted in the network are CAN (periodic) messages.
3) We assume that there is single source of DoS attack at a time.
4) There is one single path between any two edge nodes in $\mathcal{E}$.
5) Only edge nodes in $\mathcal{E}$ can monitor the end-to-end performance.

IV. PROPOSED SOLUTION

A. Network Tomography

Formally, network tomography is expressed as the following linear system

$$y = A \otimes x$$

where $y = [y_1, y_2, \ldots, y_{\eta}]^T$ is a vector of known path-level measurements, $A$ is a $\eta \times \gamma$ measurement matrix ($\eta := |\mathcal{P}^m|$ and $\gamma := |E(G)|$) and $x = [x_1, x_2, \ldots, x_{\gamma}]^T$ is a vector of unknown link-level metrics. Note that the routing in in-vehicle network is deterministic and there is only one single path in use between any two edge nodes $v_i, v_j \in \mathcal{E}$, where $i, j \in \{1, \ldots, |\mathcal{E}|\}$ and $i \neq j$. Thus, the measurement matrix $A$ is a binary matrix with entries $a_{ij} \in \{0, 1\}$, $i \in \{1, \ldots, \eta\}$, $j \in \{1, \ldots, \gamma\}$. If path $i$ traverses link $j$, we say $a_{ij} = 1$, otherwise $a_{ij} = 0$. The operation $\otimes$ depends on the problem type. If the problem is additive (e.g., delay or packet success/loss rate tomography) then $\otimes$ is matrix multiplication operation. For boolean problems, $\otimes$ is the boolean matrix multiplication, i.e., $y_i = \bigvee_j (a_{ij} \land x_j)$.

Fig. 1: Centralised in-vehicle network topology with four domains. The circles represent ECUs.
Solving (4) requires that the rank of $A$, $r(A) = \gamma$. In other words, the measurement matrix $A$ should be a full-rank matrix.

Remark 1: The measurement matrix $A$ is a full-rank matrix with $r(A) = \gamma$ if the following conditions are met:

1. Measured paths in $P^m$ are linearly independent.
2. Degree of all intermediate nodes in $R$ is at least 3 (i.e., $d(v_i) \geq 3 \forall v_i \in R$) [14], assuming that only edge nodes are able to perform the monitoring.

B. Delay Network Tomography (DNT)

This type of tomography uses delay metric to monitor the network. The end-to-end delay can be measured using timestamps [19], [20] as

$$t_i^D = t_{\text{recv}} - t_{\text{trans}}$$

where $t_{\text{recv}}$ is the time when a monitoring message is received and $t_{\text{trans}}$ is the transmission time of the same message. Then, where $\otimes$ is the matrix multiplication operation, solving (4) for vector $x$ (assuming $r(A) = \gamma$), the status of the network can be determined. In particular, by comparing the inferred delay value $x_j$ of link $e_j$ with the normal behaviour value using (3).

The main steps of this approach are as follows

1. Using (5), collect path-level delay measurements $y_p^D, \forall p_i \in P^m$.
2. Solve (4) to infer the set of link-level delays $x$.
3. Using (3) for the inferred value $x_j \in x$, if $S(e_j) = 1 \exists e_j \in E(G)$, then $S(G) = 1$ and link $e_j$ is anomalous.

C. Binary Network Tomography (BNT)

This approach uses metric of binary states (0 or 1) where $\otimes$ is the boolean matrix multiplication. BNT only requires knowing the normal delay behaviour of paths in $P^m$ which then will be used to compare against the obtained measurements using

$$y_i^B = \begin{cases} 0, & \text{if } \alpha_{p_i} \leq y_i^D \leq \beta_{p_i} \\ 1, & \text{if } y_i^D < \alpha_{p_i} \text{ or } y_i^D > \beta_{p_i} \end{cases}$$

where $\alpha_{p_i}$ and $\beta_{p_i}$ are threshold values for the minimum and maximum path-level delays of path $p_i \in P^m$ in the normal network behaviour, and $y_i^D$ is the measured path-level delay of $p_i \in P^m$ obtained by computing (5). Then, the status of each link $x_i \in x$ can be determined following below steps

1. Using (5), collect path-level delay measurements $y_p^D, \forall p_i \in P^m$.
2. Determine the path-level status $y_i^S, \forall p_i \in P^m$ using (6).
3. If $y_i^S = 1 \exists p_i \in P^m$, then $S(G) = 1$.
4. If $S(G) = 1$, then solve (4) for $x$ to obtain the status $x_j \forall e_j \in E(G)$.
5. The anomalous link $e_j$ is the one with $x_j = 1$.

For both DNT and BNT we assume that $r(A) = \gamma$, however this is not guaranteed to be satisfied. To tackle this, we adopt a deep-learning based approach using deep neural network. In particular, we use the approach proposed in [15] where it takes, as input, the set of available end-to-end measurements of paths in $P^m = \{p_1, \ldots, p_n\}$ and outputs the estimated (delay or binary) performance for paths in $P \setminus P^m = \{p_j, \ldots, p_r\}$, where $j = \eta + 1$.

D. Discussion

In DNT, both detection phase and localisation phase are performed in the same step (i.e., step 3), while in BNT, they take place in two different steps where the detection occurs before the localisation. In other words, in BNT, only if an anomaly is detected, $S(G) = 1$, then the localisation phase would take place. For in-vehicle network with its limited resources, periodically solving (4) adds unnecessary computational overhead. Thus, BNT is favored over DNT for this matter.

V. SIMULATION AND RESULTS

In this section, we evaluate both delay tomography (DNT) and binary tomography (BNT) in detecting and locating anomalies in in-vehicle network. Furthermore, when $r(A) < \gamma$, we evaluate the DNN-based tomography [15] solution for both approaches (DNN-DNT and DNN-BNT). Additionally, we compare with a baseline (BL) solution that uses threshold values such as in (3).

A. Experiment Setup

We used framework provided by CoRE project [21] based on OMNeT++ simulator [22] to simulate the in-vehicle network shown in Fig. 1. Nodes in each subsystem are connected using CAN bus while all the subsystems are connected through central gateway. $v_1$, $v_5 \in \mathcal{E}$ are edge nodes in chassis domain, $v_2$, $v_6 \in \mathcal{E}$ in telematics domain, $v_3$, $v_7 \in \mathcal{E}$ in body domain and $v_4$, $v_8 \in \mathcal{E}$ in powertrain domain. Table II shows the traffic details used for the normal behaviour.

Table II: Normal traffic details used for network shown in Fig. 1. $t_0$ is the start time, $\text{freq.}$ is the can message frequency and $\text{pyl}$. is the payload size in Bytes.

<table>
<thead>
<tr>
<th>$v_m$</th>
<th>$v_{\text{dst}}$</th>
<th>$c_m$</th>
<th>$t_0$ (s)</th>
<th>$\text{freq.}$ (s)</th>
<th>$\text{pyl}$ (B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$v_1$</td>
<td>$v_2$, $v_3$, $v_4$, $v_5$</td>
<td>2</td>
<td>0.500</td>
<td>0.600</td>
<td>8</td>
</tr>
<tr>
<td>$v_2$</td>
<td>$v_4$, $v_6$</td>
<td>3</td>
<td>0.900</td>
<td>0.05</td>
<td>5</td>
</tr>
<tr>
<td>$v_3$</td>
<td>$v_7$</td>
<td>4</td>
<td>0.005</td>
<td>0.060</td>
<td>3</td>
</tr>
<tr>
<td>$v_4$</td>
<td>$v_5$</td>
<td>5</td>
<td>0.005</td>
<td>0.080</td>
<td>8</td>
</tr>
</tbody>
</table>

The measured paths in case of DNT and BNT are $P^m = \{p_1, p_2, p_3, p_4\}$, where $p_1 = e_1$, $p_2 = e_1$, $p_3 = e_1$, $p_4 = e_4$ and $p_4 = e_3$, $e_4$ (corresponds to the CAN bus in the chassis domain, $e_2$ in the telematics domain, $e_3$ in the body domain and $e_4$ in the powertrain domain). Table III shows the characteristics of the monitoring traffic used to monitor paths in $P^m$. The monitoring traffic has no payload, its header size is 47 bits, and it is sent periodically every 1 second.

We first simulated the normal behaviour with no anomalies. Then, for the anomalous behaviour, we simulated four DoS attacks, each originated from one of the four domains. The frequency of the attack is every 0.5 milliseconds with payload size of 8 bytes. The priority of DoS attack is 1, i.e., the highest priority. The attack in this scenario targets single CAN bus at a time. Each simulation lasts for 120 seconds.
B. DNN Setup

For DNN-based tomography, we used similar parameters as in [15]. The neural network structure has two hidden layers in addition to the input and output layer. Each hidden layer consists of $2n - 1$ neurons. The set of measured paths here is $\mathcal{P}^m = \{p_1, p_3\}$, while the DNN estimates the performance for $\mathcal{P} \setminus \mathcal{P}^m = \{p_2, p_4\}$.

C. Results

We note that all approaches could accurately detect the anomalies. Hence, in the following we show the results for the localisation step.

The following metrics are used for the evaluation:

- **Precision**: it measures the ability of correctly classifying anomalous links out of all positive predictions

  \[
  \text{Precision} = \frac{TP}{TP + FP}
  \]

- **Recall**: it measures the ability of correctly classifying anomalous links out of all actual anomalous links

  \[
  \text{Recall} = \frac{TP}{TP + FN}
  \]

- **F1-measure**: it measures the harmonic mean between precision and recall

  \[
  \text{F1-measure} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}
  \]

- **Accuracy**: it measures the ability of correctly classifying normal and anomalous links

  \[
  \text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}
  \]

  where $TP$ is true positive, $TN$ is true negative, $FP$ is false positive, and $FN$ is false negative.

All the results are shown in Tables IV-VII. It is worth noting that BNT achieves the best performance for all metrics. It correctly locates all the anomalous links with no false positives or false negatives. On the other hand, DNT achieves 100% recall for correctly detecting all anomalous links. However, it sometimes misclassifies normal links as anomalous. This means that it cannot uniquely locate the anomalous link. Compared with the baseline solution, BNT yields better results while DNT performs worse.

On the other hand, when DNN-based tomography approach is used, DNN-BNT performs worse than DNN-DNT. Especially, it cannot detect when link $e_2$ is anomalous. However, we observe that it sometimes can correctly classify $e_2$ when it is normal. This is reflected in the accuracy score. Moreover, it correctly detects anomalies when links other than $e_2$ are anomalous, but it cannot uniquely locate the anomalous link. On the contrary, DNT can detect all anomalous links but cannot uniquely determine the anomalous one. As compared with the baseline solution, both DNN-based approaches perform worse.

D. Discussion

The above results show that binary network tomography can be used to accurately detect and locate anomalies within the in-vehicle network. Delay tomography, however, cannot uniquely locate the anomalous links. This is due to the fact that message priority in CAN affect the performance of DNT. Particularly, if for example, two messages $m_i$ and $m_j$ with priorities $c_{m_i} = 53$ and $c_{m_j} = 52$, are transmitted simultaneously, then message $m_j$ will win the arbitration and access the bus before
Thus, the delay of $m_i$ is larger than $m_j$. As mentioned in [14], this can result in having asymmetric behaviour which can perturb the actual delay measurements. On the other hand, BNT does not rely on the delay measurements to locate the anomalies. Instead, it uses the path-level binary performance which, due to the deterministic behaviour of in-vehicle network, can accurately classify paths’ states. Hence, uniquely locates the anomalous links. The results of DNN-based tomography solutions show that they are not very reliable, especially in locating the anomalies. Hence, it is better to use more reliable solution such as BNT which, due to its algebraic nature, requires satisfying the topological conditions.

VI. CONCLUSION AND FUTURE WORK

In this work, we proposed to use network tomography monitoring approach to detect and locate anomalies in in-vehicle network with centralised architecture. In addition, if the measurement matrix does not meet the rank requirements, we used a deep neural network-based approach to compensate for the rank-deficiency. Two types of network tomography have been evaluated: binary tomography and delay tomography. The evaluation results show that, by monitoring only subset of the network, binary network tomography achieved the best performance in correctly detecting the anomaly and locating the anomalous link in the network, while delay tomography and deep neural network-based tomography approaches did not perform as well in locating all the anomalous links. These results indicate that to accurately detect and locate anomalies, binary network tomography can be used. However, the rank requirement of the measurement matrix should be satisfied to obtain accurate results. Hence, it is important to ensure that the topology is identifiable (satisfies topological conditions). As our future work, we intend to propose a new in-vehicle network topology that supports this property.

One aspect of our approach that can be seen as a limitation is that it cannot detect attacks that result in behaviour that is conformed with the normal performance of the network as it highly depends on measuring how the network performance deviates from the normal behaviour. However, we argue that most anomalies should yield some deviations from the normal behaviour, otherwise the network operation would not be affected. In addition, the proposed approach requires that the threshold values for the normal behaviour are accurately determined, otherwise, the classification results might not be precise. Another limitation of network tomography is that the collection of end-to-end measurements and computation of link-level metrics require a powerful and central unit to perform these tasks. The central architecture of in-vehicle network facilitates this. For instance, the central gateway can be part of a Software-Defined Networking (SDN) controller that is responsible for inferring the results and taking actions to mitigate the anomalies effect. This is also one of the future directions to be investigated.

REFERENCES