HAL
open science

Benchmark for Fault Diagnosis of Water Distribution Network

Anna Sztyber, Elodie Chanthery, Louise Travé-Massuyès

To cite this version:

Anna Sztyber, Elodie Chanthery, Louise Travé-Massuyès. Benchmark for Fault Diagnosis of Water Distribution Network. The 34th International Workshop on Principles of Diagnosis (DX'23), PARC and the Silicon Austria Labs (SAL)., Sep 2023, Loma Mar, United States. hal-04327789

HAL Id: hal-04327789

https://hal.science/hal-04327789v1

Submitted on 6 Dec 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Benchmark for Fault Diagnosis of Water Distribution Network

Anna Sztyber-Betley[1] and **Elodie Chanthery**[2] and **Louise Travé-Massuyès**[2]
[1] Warsaw University of Technology, Warsaw, Poland
e-mail: anna.sztyber@pw.edu.pl
[2] LAAS-CNRS, ANITI, Université de Toulouse, CNRS, INSA, Toulouse, France
e-mails: echanthe@laas.fr, louise@laas.fr

Abstract

The DX community actively seeks meaningful benchmarks to compare diagnosis algorithms performance. This project aims to extend an existing benchmark providing structural models with simulated measurement data and various fault and cyber-attack scenarios. By utilizing existing benchmarks for leak detection in water networks, this project aims to create a tool for testing and comparing diagnosis algorithms.

1 Introduction

The DX community is often actively researching for interesting benchmarks for comparing the performance of diagnosis algorithms [1, 2, 3, 4].

The paper [5] proposed a set of water distribution network benchmarks for structural methods in fault diagnosis. However, it only provided structural models and no realistic data were provided. This project aims to extend the benchmark with simulated measurement data and to provide scenarios including different types of faults and cyber-attacks.

The water network community is actively developing benchmarks, mainly for leakage detection. These problems can be of interest to the fault diagnosis community.

Our idea is to develop a benchmark for fault diagnosis based on one benchmark of the water network community. The project aims to provide a tool for simulation and scenarios to test and compare diagnosis algorithms. The goals are as follows:

- to provide a tool that can be accessed using open-source software;
- to allow to simulate leakages, other faults, and cyber-attacks in a unified framework;
- to provide a structural model of the network used for simulation;
- to generate a set of exemplary scenarios for diagnosis.

The article is organized as follows. Section 2 provides background for structural analysis, Section 3 presents existing benchmarks from the water network research community. Section 4 describes our project for benchmarking. Then, Section 5 concludes the article and gives some future works.

2 Background

Consider a system described by a set of equations $\Sigma(z, x, \mathtt{f})$ for which z is the vector of known (or measured) variables of a set Z, x is the vector of unknown, i.e., unmeasured variables of a set X and $\mathtt{f}$ is the vector of faults of a set F. Z, X, and F are respectively of cardinal n_z, n_x, and n_f. Each equation is associated to a component of the system. The model generally represents nominal behavior, hence the violation of one equation indicates that the system is faulty and points at the responsible component.

The *structural model* of a system $\Sigma(z, x, \mathtt{f})$ can be obtained by abstracting the functional equations of $\Sigma(z, x, \mathtt{f})$ by structural equations. A structural equation e_i^S abstracts the links between the functional equation e_i and its variables.

When used for fault diagnosis, structural analysis may determine subsets of equations that will generate diagnostic tests. The degree of redundancy of a system is defined as the difference between the number of equations and the number of unknown variables included in them. The Structurally Overdetermined (SO) subsets of equations (i.e., with more equations than unknown variables) are useful for diagnosis because they show redundancy.

The MTES (Minimal Test Equations Support) is a very important concept defined in [6]. Very roughly speaking, MTES sets correspond to sets of equations that can be used to generate diagnosis residuals and they determine the degree of diagnosability.

3 Existing benchmarks

Water network companies often use simulation software to detect and localize the leakages in the network. Therefore, the water network research community can benefit from the existence of simulators. In recent years several benchmarks were proposed, with different goals, including leakage detection [7], leakage detection and isolation [8], cyber-attack detection [9], and sensor placement [10]. The benchmarks are described in the following subsections.

3.1 Battle of the Leakage Detection and Isolation Methods (BattLeDIM)

The Battle of the Leakage Detection and Isolation Methods (BattLeDIM) [7] competition was organized in 2020 as a part of the CCWI/WDSA 2020 conference. Eighteen teams submitted their solutions to the competition. The goal of the competition was to detect and localize the leakages. The

solutions were scored based on economic cost, including the value of water lost and the cost of the repair crew.

The competition was based on an L-Town network - an artificial network generated based on a real city in Cyprus. The organizers provided the participants with simulated SCADA datasets - one containing historical data with annotations for detected leaks and another for leak detection and localization. Additionally, the participants could use `.inp` file for the nominal model of the L-Town network. The nominal model was distorted compared to the "real" model used for dataset generation.

The 'real' model contains three demand patterns: residential, commercial, and industrial. Each node demand has unique values due to added randomness. The 'nominal' model was disturbed in the following ways:

- Only residential and commercial demand patterns are available.
- Each node demand is randomized.
- Pipe parameters (roughness, length, and diameter) are disturbed.
- Two additional pipes are added to the network structure.

The authors provided the following additional resources:

- Dataset generation and scoring algorithm: `https://github.com/KIOS-Research/BattLeDIM`
- SCADA Dataset: `https://zenodo.org/record/4017659`
- Reproducible code: `https://codeocean.com/capsule/2366240/tree/v1`

3.2 LeakDB: A benchmark dataset for leakage diagnosis in water distribution networks

This paper provides a benchmark for leakage detection algorithms called Leakage Diagnosis Benchmark (LeakDB) [8]. The benchmark consists of different networks with varying characteristics in terms of size, topology and type of elements they contain. The models of the networks used in the dataset are provided in the form of `.inp` files. The dataset comprises simulated scenarios accompanied by label files, indicating faults in binary notation.

A scoring algorithm is provided to evaluate the results of the different algorithms using various metrics based on the confusion matrix, such as accuracy, precision, recall, F1-score, and detection delay.

The dataset is available at `https://github.com/KIOS-Research/LeakDB`.

3.3 Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks

This Section describes the competition BATtle of the Attack Detection ALgorithms (BATADAL) [9]. The competition results were presented at the Water Distribution Systems Analysis Symposium (World Environmental and Water Resources Congress) in Sacramento, California, in 2017.

The competition was based on the C-Town network, a real-world, medium-sized water distribution system operated through programmable logic controllers and a SCADA system. The C-Town network consists of 429 pipes, 388 junctions, 7 storage tanks, 11 pumps, 5 valves, a reservoir, and 9 PLCs.

The goal of the competition was to detect cyber-attacks. The solutions were evaluated in terms of time-to-detection and classification accuracy.

The data sets were generated with epanetCPA, a MATLAB toolbox. The dataset (`https://www.batadal.net/data.html`) contains replay or deception attacks manipulating the information sent or received by sensors, PLCs and the SCADA system.

3.4 The Battle of the Water Sensor Networks (BWSN): A Design Challenge for Engineers and Algorithms

Paper [10] presents a set of examples provided for sensor placement competition with the task of detecting water contamination attacks. The competition was called Battle of the Water Sensor Networks BWSN and was undertaken as part of the 8th Annual Water Distribution Systems Analysis Symposium, Cincinnati, Ohio, in 2006. Fifteen research groups participated in the competition.

The goal of the algorithms was to minimize four objectives: expected time of detection, expected population affected before detection, expected consumption of contaminated water before detection, and detection likelihood.

The competition included two networks: Network 1 with 126 nodes, 1 source, 2 tanks, 168 pipes, 2 pumps, 8 valves and 5 sensors to place, and Network 2 with 12,523 nodes, 2 sources, 2 tanks, 14,822 pipes, 4 pumps, 5 valves and 20 sensors to place.

4 Project description

The benchmark proposed in [7] was selected for further development because it provides the following features:

- a realistically configured town description,
- Two `.inp` files: `L-TOWN_Real.inp` for a real town network that should be used for scenario simulation; and `L-TOWN.inp` for the nominal model that represents simplified and disturbed behaviour. The `L-TOWN.inp` file was given to the competition participants. It reflects the realistic situation where a water provider company has a simulator of the process but it is imperfect.
- a Python script to run the simulation with leakages,
- a configuration file to describe the simulated scenario.

4.1 L-Town

The L-Town network was proposed in [7] and is based on a real city in Cyprus. The L-Town network is shown in Fig. 1. It consists of 785 nodes and 905 pipes. Pressure in the network is maintained with one pump filling the tank. Figure 2 shows the network structure with labeled selected nodes and pipes. These points of interest will be used in the examples within the paper.

4.2 Structural model of L-Town

The structural model of L-Town was generated using the method described in [5]. The method was only based on equations describing flow in a pipe depending on pressures, flow balance equations, and flow and pressure measurements. Therefore, the method needs a few extensions to the base model to describe the L-Town network fully:

Figure 1: L-Town network. Nodes containing pressure sensors and pipes containing flow sensors were indicated in red.

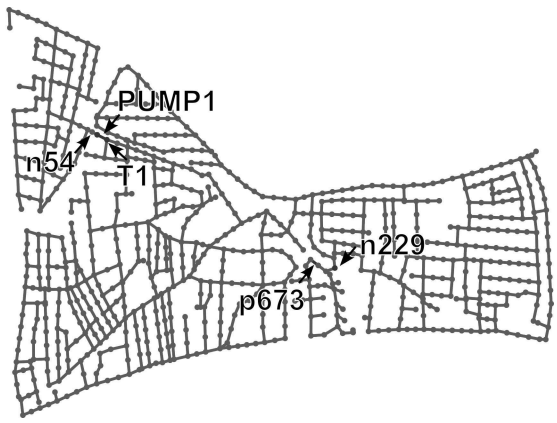

Figure 2: L-Town network with points of interest marked in red. $PUMP1$ - pump, $T1$ - tank, $n54$ - node nearest to $T1$, $p673$ - pipe with leak, $n229$ - node closest to the pipe with leak ($p673$).

1. AMRs (Wireless water meters) for measuring demands were added to the model, with the possibility to include sensor faults.
   In the base model, each network junction (v) represents a pressure variable p_j and a flow balance equation:
   $$\Sigma_{q_i \in Q_v} q_i = d_v, \tag{1}$$
   where Q_v is a set of flows incoming and outgoing the vertex v and d_v is the demand in node v.
   To represent demand measurement, the following equation is added:
   $$e^S_{d_v} = \{d_v, m_{d_v}, f_{m_{d_v}}\} \tag{2}$$
   where d_v is a demand variable, m_{d_v} is a known measurement variable for d_v and $f_{m_{d_v}}$ is the fault on the sensor.
2. An additional type of equation is added to the model for a pump.
   In the base model, each graph edge ϵ represents a flow variable q_ϵ and the corresponding flow equation:
   $$q_\epsilon = sgn(p_i - p_j).c(|p_i - p_j|)^\gamma \tag{3}$$
   where q_ϵ is the flow in the pipe corresponding to edge ϵ, p_i and p_j are the pressures of the vertices adjacent to edge $\epsilon = (v_i, v_j)$, and c and γ are parameters modelling physical properties of the pipe.
   When a pipe contains a pump, the flow is dependent on the pipe control, thus the flow equation is modified to:
   $$q_\epsilon = f(u_\epsilon), \tag{4}$$
   where u_ϵ is the known pipe control.
3. An additional type of equation is added to the model for representing a tank.
   In the base model, each node is associated to a flow balance equation of type (1). A tank adds storage capability to a node, so the equation associated to a tank node i becomes:
   $$L_i = \frac{1}{A} \int \Sigma_{q_i \in Q_v} q_i dt, \tag{5}$$
   where L_i is the level of water in the tank in the node i (we assume that the demands in tank nodes are equal to 0), and A is the tank's cross-sectional area.

The structural model of the L-Town network is generated by the code and in the configuration shown in Fig. 3. Sensors are selected according to the configuration in [7]. Leaks in each node and sensor faults are included in the model. The generated structural model contains 1694 unknown variables, 119 known variables, 904 fault variables, and 1813 equations. The degree of redundancy is 119.

It could be noted that the L-Town network (Fig. 1) contains many nodes, even where the pipe is not branching. It is motivated by the scheme of leakage localization in BattLeDIM [7] but introduces a lot of unnecessary complexity in the network structure.

To simplify the network, the algorithm from `wntr.morph.skel.skeletonize` is used. Network simplification is also known as skeletonization. The skeletonized network is shown in Fig. 4. It consists of 295 nodes and 419 pipes.

Additionally, with the skeletonized network, we generate a mapping from the nodes of the original L-Town network to the nodes of the skeletonized network. The node map is shown below. For example, nodes n4, n9, and n6 of the original network are all mapped to node n4 of the skeletonized network.

```
{"n1": "n1",
 "n4": "n4", "n9": "n4", "n6": "n4",
 "n7": "n7", "n351": "n7",
 "n350": "n7", "n349": "n7"
 ...
 }
```

The structural model of the skeletonized network is generated with the same sensor set as the original network. It is important to note that some nodes containing sensors were merged, so the resulting total number of sensors is smaller. The structural model was generated without sensor faults, and with 15 leaks placed randomly. The structural model contains 714 unknown variables, 72 known variables, 15 fault variables, and 786 equations. The degree of redundancy is 72. 15 MTES sets can be generated for this model providing full fault isolability with respect to the 15 leaks. All MTES have a degree of redundancy 1. The minimal size of MTES is 706 equations.

```
input_file_name = 'networks/L-TOWN.inp'

pressure_sensors = ['n1', 'n4', 'n31', 'n54', 'n105', 'n114', 'n163', 'n188',
                    'n215', 'n229', 'n288', 'n296', 'n332', 'n342', 'n410',
                    'n415', 'n429', 'n458', 'n469', 'n495', 'n506', 'n516',
                    'n519', 'n549', 'n613', 'n636', 'n644', 'n679', 'n722',
                    'n726', 'n740', 'n752', 'n769', 'T1']
flow_sensors = ['PUMP_1', 'p227', 'p235']
demands = ['n1', 'n2', 'n3', 'n4', 'n6', 'n7', 'n8', 'n9', 'n10', 'n11', 'n13',
           'n16', 'n17', 'n18', 'n19', 'n20', 'n21', 'n22', 'n23', 'n24',
           'n25', 'n26', 'n27', 'n28', 'n29', 'n30', 'n31', 'n32', 'n33',
           'n34', 'n35', 'n36', 'n39', 'n40', 'n41', 'n42', 'n43', 'n44',
           'n45', 'n343', 'n344', 'n345', 'n346', 'n347', 'n349', 'n350',
           'n351', 'n352', 'n353', 'n354', 'n355', 'n356', 'n357', 'n358',
           'n360', 'n361', 'n362', 'n364', 'n365', 'n366', 'n367', 'n368',
           'n369', 'n370', 'n371', 'n372', 'n373', 'n374', 'n375', 'n376',
           'n377', 'n378', 'n379', 'n381', 'n382', 'n383', 'n384', 'n385',
           'n386', 'n387', 'n388', 'n389']
epn_conv = EpanetConverter(input_file_name, pressure_sensors=pressure_sensors,
                           flow_sensors=flow_sensors, leaks=None,
                           sensor_faults=True, pumps=['PUMP_1'], tanks=['T1'],
                           demands=demands, pressure_prefix='', flow_prefix='')
epn_conv.structural_from_epanet()
```

Figure 3: Example usage

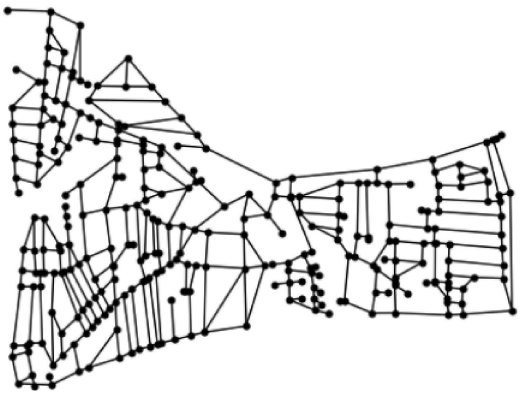

Figure 4: L-Town network skeletonized

4.3 Faults and attacks

We consider the following types of faults and cyber-attacks:

- leaks,
- outages,
- pump degradation,
- change of pump control high limit,
- change of pump control low limit,
- masking of measurements by replay of historical values.

Leaks are simulated using the method from [7] without modifications. There are two types of leaks: abrupt and incipient. The exemplary leak configuration is formulated as follows:

```
leakages:
- # linkID, startTime,
    endTime, leakDiameter (m),
    leakType, peakTime
- p257, 2018-01-08 13:30,
  2018-12-31 23:55, 0.011843,
  incipient, 2018-01-25 08:30
- p673, 2018-03-05 15:45,
  2018-03-23 10:25, 0.022916,
  abrupt, 2018-03-05 15:45
```

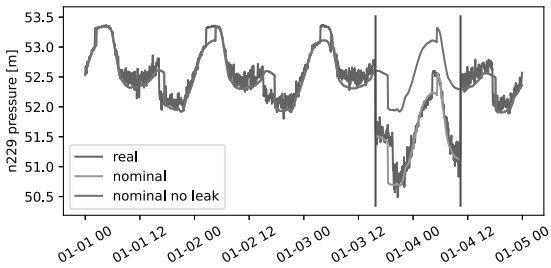

Figure 5: Pressure measurements during the leak in pipe $p673$

The exemplary measurements during the leak are shown in Fig. 5. Red lines indicate the start and the end of the leak. The blue plot shows pressure values in a node near the leaking pipe. Clear pressure drop can be observed (however, small leaks are nearly invisible). The orange line shows the same pressure with the same leak simulated using the nominal network model, and the green line shows the results from the nominal model without the leak. It proves that the nominal model can be helpful in fault detection.

Fig. 6 shows selected measurements during regular network operation. The pump is placed in a pipe connected to tank $T1$. Node $n54$ is the nearest node with a pressure sensor. We can observe that the tank level grows when there is flow through the pump.

The pump is controlled by a simple set of rules:

```
LINK PUMP_1 CLOSED IF NODE T1 ABOVE 3.9000
LINK PUMP_1 OPEN IF NODE T1 BELOW 2.4000
```

The first kind of fault is an outage (Fig. 7), which is a

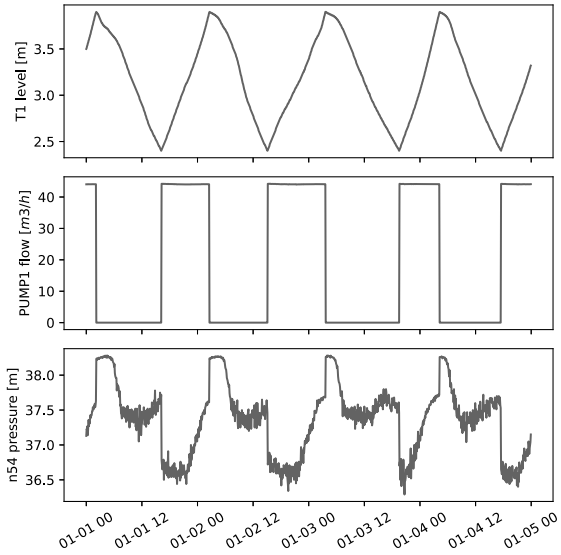

Figure 6: Regular case: measurement

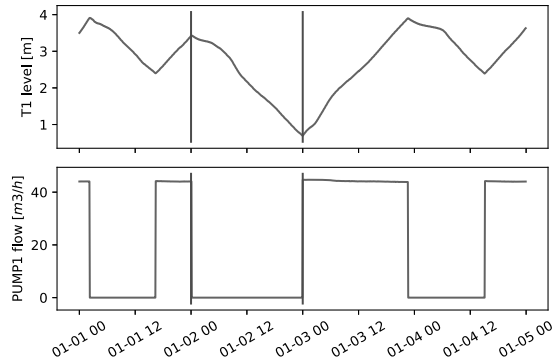

Figure 7: Outage: measurement

lack of power causing the pump to stop. The outages can be configured as follows:

```
outages:
 - StartTime: 2019-01-02 00:00
   EndTime: 2019-01-02 23:55
```

The second kind of fault is designed to model pump degradation (Fig. 8). Pump degradation can be configured as follows:

```
pump_curves:
 - StartTime: 2019-01-02 00:00
   EndTime: 2019-01-02 23:55
   curve: [[0.0, 70], [0.0076, 40],
           [0.0138, 0.0]]
```

Pump degradation is configured by a change in the characteristic pump curve. The curve describes dependency of the flowrate and pressure head. In Fig. 8, we can observe that the pump is working but with reduced flowrate.

Next, we consider cyber-attacks. The first type of attack is a change of pump control algorithms. There are two options. The first is to modify the low control limit:

```
pump_control_low:
  StartTime: 2019-01-02 00:00
  EndTime: 2019-01-02 23:55
```

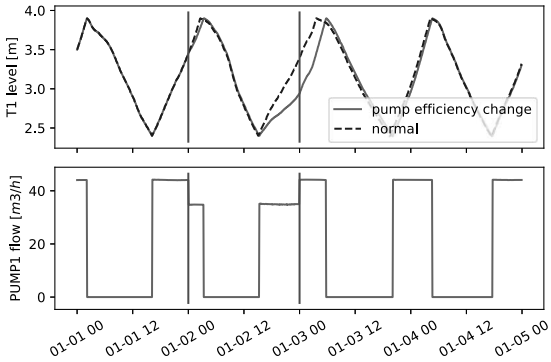

Figure 8: Pump degradation: measurement

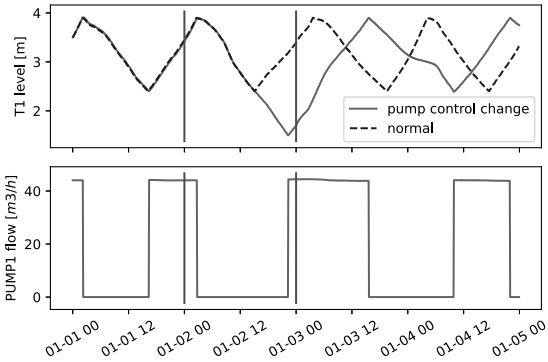

Figure 9: Measurement: pump low control limit change

```
  value: 1.5,
```

and the second to modify the high control limit:

```
pump_control_high:
  StartTime: 2019-01-02 00:00
  EndTime: 2019-01-02 23:55
  value: 3
```

Lowering the limits can cause a pressure drop in the network and changing the high limit to a higher value can cause tank overflow. Measurements corresponding respectively to the changes in low and high control limits are shown in Fig .9 and Fig. 10.

The second kind of attack is masking measurement values with a replay of historical values. The attack consisting

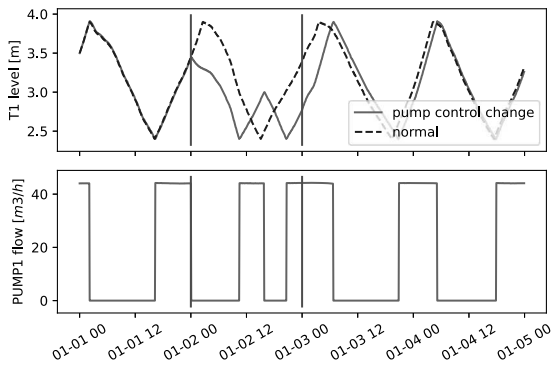

Figure 10: Measurement: pump low control limit change

of modifying the high pump control limit and masking the value of level in tank $T1$ was shown in Fig. 11. We can observe that the value of the $T1$ level is substituted with values from the normal range, but the pressure in node $n54$ shows the discrepancy from normal operation. Masking can be configured as follows:

```
masking_pressure:
  - StartTime: 2019-01-02 00:00
    EndTime: 2019-01-02 23:55
    node: T1
```

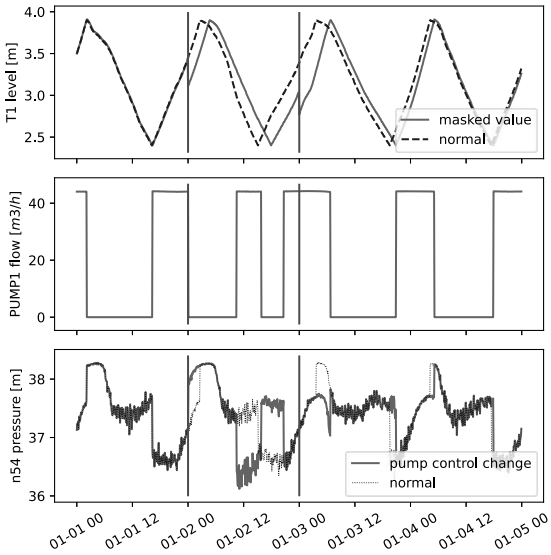

Figure 11: Measurement: masking

4.4 Scenarios

Two scenarios with simulated measurement data are prepared. Details of scenario 1 are shown in Fig. 12. It contains three leakages, an outage, pump degradation and an attack changing the control law of the pump. Scenario 2 is similar but it additionally contains masking of a value of the measurement of level in tank $T1$ during the attack.

4.5 Resources

Generated resources are published in a publicly available repositories:

- `https://github.com/asztyber/wdn-sa-benchmark` - contains `.inp` files for the original and simplified L-Town network, structural models for both networks and simulated measurements for both scenarios. Additionally, the repository contains modified code for structural model generation including demand, pump and tank equations.
- `https://github.com/asztyber/wdn-simulation` - contains code for simulation of leaks, faults and cyber-attacks in a desired configuration.

5 Conclusion

This article proposes a new benchmark for fault diagnosis. The benchmark illustrates water distribution networks. It is based on the L-Town network, based on a city of Cyprus. Our benchmark provides a structural model of the network, can generate a set of exemplary scenarios for diagnosis and allows simulating the values of leakages, other faults and also cyber-attacks. Thus, it can be used for structural analysis based diagnosis or data-based diagnosis. We hope that the DX community will use it in the future for comparing their different approaches and algorithms' performances.

Acknowledgments

This project was partially funded by a research grant no 504/04871/1141/43.022303 from the Scientific Council of the Discipline of Automation, Electronics, Electrical Engineering and Space Technologies of Warsaw University of Technology. This project is supported by ANITI through the French "Investing for the Future – PIA3" program under the Grant agreement noANR-19-PI3A-0004.

References

[1] Tolga Kurtoglu, Sriram Narasimhan, Scott Poll, David Garcia, Lukas Kuhn, Johan de Kleer, Arjan van Gemund, and Alexander Feldman. First international diagnosis competition-dxc'09. *Proc. DX*, 9:383–396, 2009.

[2] Scott Poll, Johan de Kleer, Alexander Feldman, David Garcia, Tolga Kurtoglu, and Sriram Narasimhan. Second international diagnostic competition œ dxc '10. 2010.

[3] Scott Poll, Johan de Kleer, R Abreau, Matthew Daigle, Alexander Feldman, David Garcia, and A Sweet. Third international diagnostics competition–dxc'11. In *Proc. of the 22nd international workshop on principles of diagnosis*, pages 267–278, 2011.

[4] Adam Sweet, Alexander Feldman, Sriram Narasimhan, Matthew Daigle, and Scott Poll. Fourth international diagnostic competition–dxc'13. In *Proc. of the 24th international workshop on principles of diagnosis*, pages 224–229, 2013.

[5] Anna Sztyber, Elodie Chanthery, Louise Travé-Massuyès, and Carlos Gustavo Pérez-Zuñiga. Water network benchmarks for structural analysis algorithms in fault diagnosis. In *33rd International Workshop on Principle of Diagnosis – DX 2022*, Toulouse, France, September 2022. LAAS-CNRS-ANITI.

[6] Mattias Krysander, Jan Åslund, and Erik Frisk. A structural algorithm for finding testable sub-models and multiple fault isolability analysis. In *21st International Workshop on Principles of Diagnosis (DX-10), Portland, Oregon, USA*, pages 17–18, 2010.

[7] Stelios G. Vrachimis, Demetrios G. Eliades, Riccardo Taormina, Zoran Kapelan, Avi Ostfeld, Shuming Liu, Marios Kyriakou, Pavlos Pavlou, Mengning Qiu, and Marios M. Polycarpou. Battle of the Leakage Detection and Isolation Methods. *Journal of Water Resources Planning and Management*, 148(12):04022068, December 2022.

[8] Stelios G Vrachimis, Marios S Kyriakou, et al. Leakdb: a benchmark dataset for leakage diagnosis in water distribution networks. In *WDSA/CCWI Joint Conference Proceedings*, volume 1, 2018.

[9] Riccardo Taormina, Stefano Galelli, Nils Ole Tippenhauer, Elad Salomons, Avi Ostfeld, Demetrios G.

```
Comments:
  - Scenario 1

Network:
  filename: L-TOWN_Real.inp

results_path: Scenario1//

times:
  StartTime: 2019-01-01 00:00
  EndTime: 2019-02-28 23:55

leakages:
- # linkID, startTime, endTime, leakDiameter (m), leakType, peakTime
- p101, 2019-01-03 20:05, 2019-02-28 23:55, 0.011906, incipient, 2019-02-28 22:10
- p413, 2019-02-10 13:25, 2019-02-28 23:55, 0.015008, abrupt, 2019-02-10 13:25
- p805, 2019-02-10 11:55, 2019-02-20 23:55, 0.013195, incipient, 2019-02-20 23:55

outages:
- StartTime: 2019-01-02 00:00
  EndTime: 2019-01-02 23:55

pump_curves:
- StartTime: 2019-02-22 00:00
  EndTime: 2019-02-28 23:55
  curve: [[0.0, 70], [0.007607111111111111, 40], [0.013888611111111112, 0.0]]

pump_control_low:
  StartTime: 2019-01-15 00:00
  EndTime: 2019-01-22 23:55
  value: 1.5
```

Figure 12: Scenario 1

Eliades, Mohsen Aghashahi, Raanju Sundararajan, Mohsen Pourahmadi, M. Katherine Banks, B. M. Brentan, Enrique Campbell, G. Lima, D. Manzi, D. Ayala-Cabrera, M. Herrera, I. Montalvo, J. Izquierdo, E. Luvizotto, Sarin E. Chandy, Amin Rasekh, Zachary A. Barker, Bruce Campbell, M. Ehsan Shafiee, Marcio Giacomoni, Nikolaos Gatsis, Ahmad Taha, Ahmed A. Abokifa, Kelsey Haddad, Cynthia S. Lo, Pratim Biswas, M. Fayzul K. Pasha, Bijay Kc, Saravanakumar Lakshmanan Somasundaram, Mashor Housh, and Ziv Ohar. Battle of the attack detection algorithms: Disclosing cyber attacks on water distribution networks. *Journal of Water Resources Planning and Management*, 144(8):04018048, 2018.

[10] Avi Ostfeld, James G. Uber, Elad Salomons, Jonathan W. Berry, William E. Hart, Cindy A. Phillips, Jean-Paul Watson, Gianluca Dorini, Philip Jonkergouw, Zoran Kapelan, Francesco di Pierro, Soon-Thiam Khu, Dragan Savic, Demetrios Eliades, Marios Polycarpou, Santosh R. Ghimire, Brian D. Barkdoll, Roberto Gueli, Jinhui J. Huang, Edward A. McBean, William James, Andreas Krause, Jure Leskovec, Shannon Isovitsch, Jianhua Xu, Carlos Guestrin, Jeanne VanBriesen, Mitchell Small, Paul Fischbeck, Ami Preis, Marco Propato, Olivier Piller, Gary B. Trachtman, Zheng Yi Wu, and Tom Walski. The battle of the water sensor networks (bwsn): A design challenge for engineers and algorithms. *Journal of Water Resources Planning and Management*, 134(6):556–568, 2008.