

WATER SUPPLY NETWORK PROTECTION FROM MALICIOUS ATTACKS BY SECTORIZATION

Armando DI NARDO¹, Michele DI NATALE¹, Mario GUIDA¹ & Dino MUSMARRA¹

- (1) Research Center of Environmental Engineering, Department of Civil Engineering, Second University of Naples, Annunziata Real Casa, Via Roma 29, 81031 Aversa (CE), Italy, e-mail: armando.dinardo@unina2.it

ABSTRACT

Water supply networks are sensitive to several malicious attacks that can potentially affect every single phase, from water adduction to distribution to end-users. One of the most dangerous threats is a backflow attack that occurs when a pump system, easily available on the market, is utilised to overcome the pressure gradient of network pipes. In this work, after modelling a simple backflow attack by introducing cyanide into the real-water system and defining the most dangerous introduction points for a contaminant incident, the network vulnerability has been analyzed by computing the lethal dose of cyanide ingested by users and the total contaminated length of the water system. Then the effects of network partitioning and district isolation for the security of water supply systems have been investigated. The results show how district closing, obtained according to water network sectorization techniques used to improve leakage search and reduction, can significantly decrease contaminant diffusion and protect part of the users from cyanide adsorption. Then network sectorization can also reduce the risk of simple malicious attacks because several introduction points are necessary in order to have a wide negative impact on the network. Simulation results have also shown that in some cases water network partitioning may worsen water network protection and further studies are necessary to design water districts for network security.

1 INTRODUCTION

Water supply networks are exposed to two types of risk: (i) mechanical, mainly due to the failure of one or more network elements (pipes, joints, water-lifting devices, etc.) under normal operating conditions (Mays, 2000) and (ii) contamination, from accidental or intentional introduction of toxic chemicals or bacterial agents into the water distribution system (NRC, 2007).

The contamination risk is mainly due to the natural, accidental or intentional introduction of chemical and/or biological contaminants in the water network and is less easily predictable than the mechanical risk.

Water contamination by malicious or terrorist attacks is a major risk for society and can have serious consequences such as poisoning and infectious diseases.

After September 11 2001, many countries adopted guidelines for water quality monitoring and emergency action plans (HSPDs, 2002; SRSI, 2002; US EPA, 2003,

2009 and 2010; CER, 2005).

A malicious act may consist in the introduction of chemical, biochemical or radioactive contaminants in the water supply network. The sabotage is most effective when the hazardous substance is injected as concentrated liquid or powder. The most hazardous substances are biotoxins (organic substances that can cause serious poisoning) and biological agents (viruses and/or bacteria).

Recently, the scientific literature has begun to look at contamination risk more systematically. Many technical safeguard/security problems of the water supply networks, are mainly due to the technical and managerial complexity of the water supply networks (Mays, 2002), the variability of the contaminant (Clark et al., 2006), the difficulty in estimating contaminant diffusion, the extreme contaminant speed of propagation, which requires fast and coordinated monitoring (Guidorzi et al., 2008).

Optimal measurement station localization and identification of point source contamination (Laird, 2005, Laird et al., 2006; Guan et al. 2006; Preis & Ostfeld, 2006; Ostfeld et al., 2008; Di Cristo & Leopardi, 2008) are widely described in the literature. These techniques are very helpful for early warning but they are not so effective in analysing the impact of the actions that have to be taken afterwards to guarantee health security.

In a water supply network contamination incident, two main actions can be carried out: a) you alert users not to use water and/or b) you close that sector of the network in order to limit dangerous to health.

For the first action to be successful warning is crucial while the effectiveness of the second one depends on both alert speed and the possibility of closing pipes to disconnect network sectors. The first action essentially relies on a good distribution of early warning network sensors and the second one exclusively relies on a previous design of network sectorization (or partitioning).

In the last years, Water Network Partitioning (WNP) has been proposed in order to simplify water balance and pressure management (Di Nardo and Di Natale, 2010a). Such technique consists in partitioning the water network in different permanent subsystems, called District Meter Areas (DMA), through boundary valves and flow meters. If WNP is carried out in the water supply network design phase, it is possible to plan different districts in order to improve system management, pressure regulation and water leakage detection without altering the network performance.

When water systems are already in operation it is more difficult to set the number and dimension of districts and, in many cases, WNP may even worsen considerably the hydraulic performance of water networks both in terms of water quality (creating more dead-end pipes and flow reversals) and of node heads (Wrc/ WSA/ WCA 1994).

Recently, the effects of network partitioning for the protection of water supply networks from a biological agent were studied in Grayman et al. (2009) and Murray et al. (2010) who, starting from WNPs compatible with hydraulic performance, observed significant improvements in security system just with DMAs design and without any security measures.

But the positive effects of network DMAs on the security of water supply systems depend on several aspects: dimension of water network, pollutant class, number of DMAs, features of the contaminant incident, exposure time, etc.; therefore simulation results may not be generalized (Grayman et al., 2009).

In this study, the security effects of network partitioning have been investigated for a

small water network with: different district layouts, a chemical agent and a simple malicious attack lasting only two hours. Then the effects of the isolation of one DMA after few hours from contaminant incident, have been analyzed.

2 METHODS

The analysis was carried out by modelling the malicious attack and contaminant transport in the water network, then evaluating the most dangerous insertion points based on the number of exposed users and finally comparing simulations with and without network sectorization.

All simulations were made by EPANET2 (Rossman, 2000) that allows the modelling of both contaminant transport and network sectorization.

2.1 Malicious attack modelling

The first step of methodology consists in the assessment of the characteristics of the contaminant incident: how many terrorists?, which pollutant?, how long an attack?, etc. In this case study a simple backflow attack in a network point has been investigated.

The backflow is carried out with a pump system – easy to find on the market – that by overcoming the pressure gradient of network pipes, may introduce a contaminant into the water system and disseminate it into the network affecting the areas surrounding the introduction point.

The malicious attack is carried out in a single point and, theoretically, by a single terrorist equipped with few simple devices (a small pump, a backpack to transport the pollutant, etc.) that allow him to go completely unnoticed and to do crime.

The contaminant chosen for the network malicious attack is potassium cyanide (Patnaik, 2007), an inorganic compound, highly soluble in water (716 g/l) and extremely toxic ($LD_{50} = 2.86 \text{ mg/kg}$).

The backflow attack can be achieved mixing cyanide with water in a room bath of a generic house of a generic town and pumping the cyanide solution inside the water network. The introduction point can be everywhere in the system but by network hydraulic simulation it is possible to choose the points where the contaminant diffusion can become more massive and dangerous. Then the second step consists in identifying the network critical introduction point for user exposure. Different assumptions have been made in order to evaluate the hazardous effects on user health:

- a fixed user number corresponds to each network node;
- the potassium cyanide amount (flow rate and concentration) is inserted in water network during only 2 hours (8.00 am and 10.00 am o'clock). A two-hour time interval is enough for room bath refilling and cyanide mixing;
- the lethal concentration for a single user of 70 kg is assumed as equal to 200 mg/l;
- the warning starts after two hours (at 10.00 am) or three hours (at 11.00 am) from the beginning of malicious attack and orders to close the network district.

Then n hydraulic simulations were carried out in order to identify which network node, both for the whole network and each DMA, is more effective for a malicious attack with a backflow technique.

Such analysis was achieved inserting a pump system with the same cyanide concentration in each network node defining risk scenarios.

2.2 Contaminant transport modelling

The cyanide transport modelling is simulated with EPANET2 quality module starting from water flow velocities u calculated with the hydraulic module. The values u are used as convective transport velocities in the quality module, which allows to describe transport of dissolved species through network pipes. In particular, the water quality module solves, along i -th network pipe, the following equations

$$\frac{\partial C_i}{\partial t} = -u \frac{\partial C_i}{\partial x} \quad (1)$$

In equation (1) C represents the concentration of the dissolved species (i.e.: contaminant concentration) and x is the position along the pipe. At network nodes, instantaneous and complete mixing is assumed, and the following equations are written:

$$C_{k,out} = \frac{Q_{k,ext} C_{k,ext} + \sum_{i \in I_k} Q_{i,in} C_{i,in}}{Q_{k,ext} + \sum_{i \in I_k} Q_{i,in}} \quad (2)$$

in which $C_{k,out}$ represents contaminant concentration leaving node k ; $Q_{k,ext}$ and $C_{k,ext}$ represent the external input contaminant flow and concentration, respectively; $Q_{i,in}$ and $C_{i,in}$ are flow and concentration in the i -th of the I_k pipes entering node k .

3 CASE STUDY

In order to explain the proposed methodology and to investigate the positive effects of WNP, a real Parete (Caserta-Italy) network, already studied by the authors (Di Nardo and Di Natale, 2010a), has been used. Parete, a little town with 10,800 inhabitants in a densely populated area of the South of Caserta (Italy), has a water supply network sketched in Figure 1. The main hydraulic characteristics of the EPANET model are reported in following Table 1. Specifically, the network is supplied from two different sources, illustrated in Figure 1, and then the kind of water consumption in Parete is exclusively residential with a prevalence of houses, built in 1970's and 1980's, with 3 to 4 floors.

Table 1. Parete network model characteristics

Model characteristics	Parete
junctions (n)	182
pipes (m)	282
pipe total length	32.67 km
pipe material	cast iron
reservoir head	two to 110 m
roughness	0.85 (Darcy-Weisbach)
total inflow (peak demand)	110.2 l/s

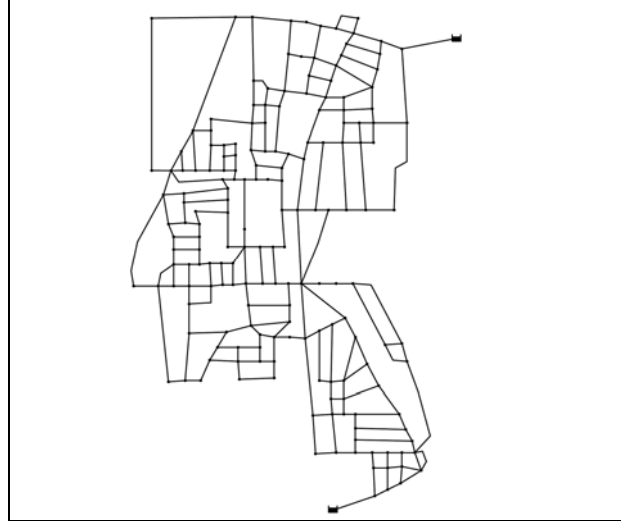
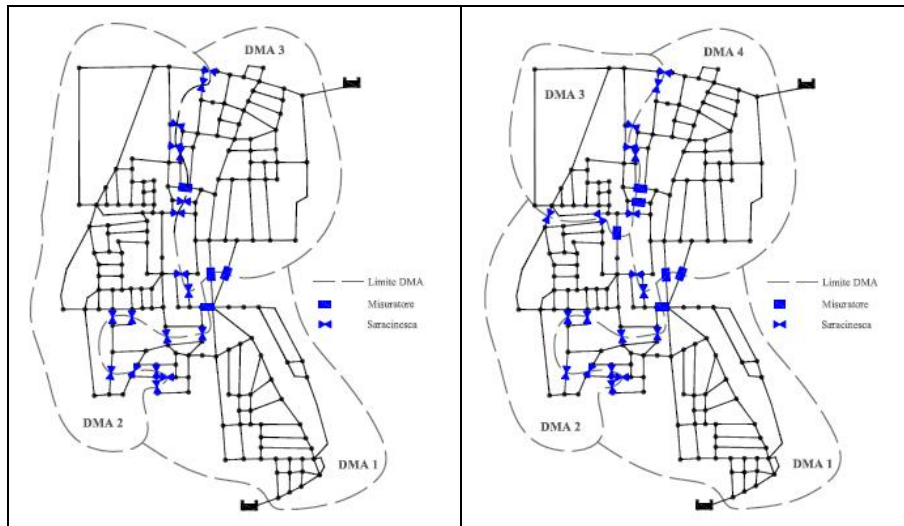


Figure 1. Parete network model

3.1 Network partitioning

The water network partitioning used in this work was developed in Di Nardo and Di Natale (2010a) in order to obtain other main objectives (i.e. water balance or pressure management) and not to limit the damage of a malicious attack. Specifically the WNP proposed in Figure 2 is compatible with the level of service for Parete as measured with specific performance indices developed in Di Nardo and Di Natale (2010b).



(a) WNP3 with 3 DMAs

(a) WNP4 with 4 DMAs

Figure 2. Different Partitioning (WNP) of Parete water network.

The two WNP's reported in Figure 2 refer to a different number of DMAs: 3 DMAs in Figure 2a and 4 DMAs in Figure 2b. These layouts were used to analyze the effects of different levels of water district partitioning on water network protection from malicious attacks.

4 RESULTS

The simulation results are reported in Table 2 and Table 3, for WNP3 and WNP4 respectively. Specifically the tables report, for each DMA and for the whole network (in the last two columns), the number of exposed users N_{eu} and the length of contaminated pipes L_{ep} . In particular in the 1st line of both tables, the results of the original network without WNP is reported, then in the 2nd line, the results of network with only WNP are reported and, finally, in all the others lines the results of a single DMA isolation are reported.

All simulations have been carried out inserting a pump system with potassium cyanide concentration in the insertion point of network that generates the most damage for users. The information about these points, the cyanide concentration and other specific simulation details are not reported in order to protect Parete water supply system.

In the first simulation – the case of water network without partitioning – the total number of exposed users is about 3,000 as reported both in Table 2 and 3.

The first results in Table 2 with 3 DMAs shows that the WNP (2th line) increases contamination risk with a higher value of N_{eu} (+14.38%) but reduces slightly L_{ep} (-3.00%). WNP changes the effects of contamination on the different DMAs with a significantly increment of N_{eu} in DMA3 and a small reduction of N_{eu} in DMA2. These results, obtained for WNP3 with 3 DMAs, are similar to WNP4 with 4 DMAs as reported in Table 3.

Table 2. Simulation results for WNP3 with 3 DMAs

WNP		DMA1		DMA2		DMA3		TOT	
		N_{eu}	L_{ep}	N_{eu}	L_{ep}	N_{eu}	L_{ep}	N_{eu}	L_{ep}
		-	[km]	-	[km]	-	[km]	-	[km]
NO		0	0	740	1.95	2367	2.95	3107	4.90
YES		0	0	670	1.02	2884	3.73	3554	4.75
10.00 am	DMA1 closed	100	0.45	1303	2.77	712	0.59	2115	3.81
	DMA2 closed	0	0	983	1.50	0	0.33	983	1.83
	DMA3 closed	0	0	0	0.60	2382	3.10	2382	3.70
11.00 am	DMA1 closed	100	0.52	2108	2.83	914	0.88	3122	4.23
	DMA2 closed	0	0	1708	2.34	0	0.35	1708	2.69
	DMA3 closed	0	0	440	0.60	2884	3.70	3324	4.30

Table 3. Simulation results for WNP4 with 4 DMAs

WNP		DMA1		DMA2		DMA3		DMA4		TOT	
		N _{eu}	L _{ep}	N _{eu}	L _{ep}	N _{eu}	L _{ep}	N _{eu}	L _{ep}	N _{eu}	L _{ep}
		-	[km]	-	[km]	-	[km]	-	[km]	-	[km]
NO		0	0	0	0	740	1.40	2367	3.50	3107	4.90
YES		100	0.52	808	1.70	1225	1.50	1202	1.10	3335	4.80
10.00 am	DMA1 closed	100	0.52	770	1.46	760	1.60	904	0.90	2534	4.48
	DMA2 closed	951	1.00	0	0	0	0	0	0	951	1.00
	DMA3 closed	0	0	0	0	1155	0.64	0	0	1155	0.64
	DMA4 closed	0	0	0	0	0	0.20	2824	3.50	2824	3.70
11.00 am	DMA1 closed	100	0.52	673	1.50	1305	1.70	1164	0.85	3242	4.57
	DMA2 closed	0	0	605	1.80	915	0.80	0	0	1520	2.60
	DMA3 closed	0	0	0	0	1240	0.70	0	0	1240	0.70
	DMA4 closed	0	0	0	0	525	1.40	2622	3.50	3147	4.90

In this last scenario the simulation shows a significant reduction of exposed users in DMA4 but a significant increment in DMA2 and DMA3 and a small increment in DMA1. Also in WNP4 with 4 DMAs a slight reduction (-2.00%) of the total contaminated pipes L_{ep} can be observed.

Both these scenarios were obtained without any security action and the different effects of the contaminant incident depend exclusively on the reduction of loop level of water system due to WNP.

Therefore different security scenarios, based on the complete isolation of a single DMA, where the insertion point was located, after two or three hours from the beginning of the malicious attack, were analyzed. These scenarios can be achieved if the water system has an affective warning system. Such protection action, limited to a single DMA, allows to activate security measures also if, in the first hours of the contaminant incident, the severity of the contamination is unknown, because the water supply is still partially guaranteed to a part of the users.

In the security scenarios with DMA isolation, the network protection is stronger than in the case without closure of the district and, in some simulations, corresponding to a DMA isolation achieved after two hours (at 10 am), the water security is evident for all DMAs both for WNP3 and WNP4 case study. While, if the alarm for the district isolation is given after three hours (at 11 am), the protection is effective only with the isolation of DMA2 (-45% of N_{eu}) for WNP3, and only with the isolation of DMA2 (-51% of N_{eu}) and DMA3 (-60% of N_{eu}) for WNP4.

However, in some cases, the simulation results showed that the DMA isolation may even slightly worsen user exposure: as in the DMA1 and DMA3 isolation of WNP3 at 11 am and in DMA1 and DMA4 of WNP4.

The simulation results for contaminated pipes L_{ep} show a non homogeneous effects of water partitioning network for the system protection too. These results show that, conversely to what stated by Grayman et al. (2009) and Murray et al. (2010), water

network partitioning without security measures does not improve the security of the water system while the DMA isolation can be more effective.

5 CONCLUSIONS

Different scenarios were analyzed to compute the number of users potentially exposed to a contamination attack of water supply networks by cyanide pollutant.

The simulation results showed that a significant protection can be achieved with DMA isolation, that is activated by an early warning system. Moreover simulation results showed how an early closure of a DMA may significantly decrease contaminant diffusion and protect part of the users from cyanide ingestion but, in other cases, may even slightly increase the effect of a contamination incident.

These heterogeneous results depend certainly on the peculiarity of water supply system and confirm that simulation results may not be easily generalized and that further studies have to be done also with different hypothesis on the contaminant incidents.

Some considerations on water network security can be obtained from these preliminary studies: a) WNP is probably more effective for medium or large network protection; b) DMA isolation is more effective than water network partitioning only; c) WNP with many DMAs may protect better the users; d) WNP may reduce the risk because several introduction points are necessary to have a wide negative impact on the network; e) WNP allows to activate easier protection measures because it is possible to disconnect only a small part of the network.

Some of these preliminary considerations suggest that water network partitioning has to be designed also taking into account the objective of water protection in addition to other objectives of water supply network management. Then the proposed methodology for water network protection can be developed together with the other improvement techniques of water network management (leakage reduction, pressure management, etc.) thus becoming cheaper.

REFERENCES

- CER (Centre for European Reform). (2005). The EU and counter-terrorism, Centre for European Reform, London.
- Clark R.M., Chandrasekaran, L. and Buchberger, S.B. (2006) Modeling the propagation of waterborne disease in water distribution systems: results from a case study, 8th WSDA Symposium, Cincinnati.
- Di Cristo C. and Leopardi A. (2008). Pollution source identification of accidental contamination in water distribution networks, *Journal of Water Resources, Plng. And Mgmt.*, ASCE, 134 (2); pp. 197-202.
- Di Nardo, A. and Di Natale, M. (2010a). A heuristic Design Support Methodology based on graph theory for district metering of water supply networks, *Engineering Optimization*, Taylor & Francis, 2010a, DOI: 10.1080/03052151003789858.
- Di Nardo, A. and Di Natale, M., (2010b). A design support methodology for district metering of water supply networks, in *Proceedings of Water Distribution Systems Analysis (WDSA)*, 12-15 September 2010, Tucson, AZ (USA).
- Grayman, W.M., Murray, R., Savic, D.A.(2009). Effects of redesign of water systems for security and water quality actors. In: Starrett, S. (Ed.), *Proceedings of the World Environmental and*

- Water Resources Congress. 49 Kansas City, MO.
- Guan, J., Aral, M.M., Maslia, M.L. and Grayman, W.M. (2006). Identification of Contaminant Sources in Water Distribution Systems using Symulation-Optimization Method: Case study. *J. Water Resour. Plng and Mgmt.*, ASCE, 132 (4); pp. 252-262.
- Guidorzi, M., Franchini M. and Alvisi S. (2008). A multi-objective approach for detecting and responding to accidental and intentional contamination events in water distribution systems. *Urban Water Journal*, 6 (2); pp. 115-135.
- HSPDs. (2002). Public Health Security and Bioterrorism Preparedness and Response, *Act of 2002 (Bioterrorism Act)*.
- Laird, C.D., Biegler, L.T. and van BloemenWaanderse B.G., (2006). Mixed-Integer approach for obtaining unique solutions in source inversion of water networks. *J. Water. Resour. Plng. and Mgmt.*, ASCE, 132 (4); pp. 242-251.
- Laird, C.D., Biegler, L.T., van Bloemen Waanderse, B.G. and Barlett, R.A. (2005). Contamination source determination for water networks. *J. Water Resour. Plng. and Mgmt.*, ASCE, 131 (2); pp. 125-134.
- Mays, L.W. (2002). *Urban Water Supply Handbook*. McGraw Hill, New York Mays.
- Murray, R., Grayman, W.M., Savic, D.A.(2010). Effects of DMA redesign on water distribution system performance. In: Boxall, J. & Maksimovic, C. (Eds.), *Proceedings of the Tenth International Conference on Computing and Control in the Water Industry 2009*. London, CRC Press.
- National Research Council (NRC). (2007). Improving the nation's water security: opportunities for research. Washington DC: The National Academies Press.
- Ostfeld, A. (2008). The Battle of water Sensor Networks (BWSN): A Design Challenge for Engineers and Algorithms. *J. Water Resour. Plng and Mgmt.*, ASCE, 134 (6); pp.556-568.
- Patnaik, P. (2007). A comprehensive guide to the hazardous properties of chemical substances. Third Edition, J. Wiley & Sons, New Jersey.DOI: 10.1002/9780470134955.ch16.
- Preis, A. and Ostfeld, A. (2006). Contamination Source Identification in water Systems: A Hybrid model Trees-linear Programming scheme. *J. Water Resour. Plng. and Mgmt.*, ASCE, 132 (4); pp. 263-273.
- Rossman, L.A. (2000). *EPANET 2 User's Manual*, EPA Publication.
- SRSI. (2002). Situating the concepts of security and risk, *SRSI paper*.
- US EPA. (2001). Distribution system research and information collection partnership factsheet, office of water (4607M) EPA-815-F-10-001. Available from: www.epa.gov/safewater and http://www.epa.gov/ogwdw000/disinfection/tcr/regulation_revisions_tcrdsac.html.
- US EPA. (2003). Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents, online version. Available from: http://www.epa.gov/safewater/watersecurity/pubs/guide_response_overview.pdf
- US EPA. (2009). National primary drinking water regulations. US. Environmental protection agency. Washington DC, USA, EPA 816-F-09-004.
- Wrc/WSA/WCA Engineering and Operations Committee. (1994). Managing leakage: UK water industry managing leakage. Report A-J. London: Wrc/WSA/WCA.