HAL
open science

Intentional contamination of water distribution networks: developing indicators for sensitivity and vulnerability assessments

Amir Nafi, Eric Crastes, Rehan Sadiq, Denis Gilbert, Olivier Piller

To cite this version:

Amir Nafi, Eric Crastes, Rehan Sadiq, Denis Gilbert, Olivier Piller. Intentional contamination of water distribution networks: developing indicators for sensitivity and vulnerability assessments. Stochastic Environmental Research and Risk Assessment, 2018, 32 (2), pp.527-544. 10.1007/s00477-017-1415-y . hal-01730256

HAL Id: hal-01730256

https://hal.science/hal-01730256v1

Submitted on 13 Mar 2018

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.

Author-produced version of the article published in
Stochastic Environmental Research and Risk Assessment,
32 (2), 2018, p.527-544
The original publication is available at http://link.springer.com/article/10.1007/s00477-017-1415-y

Intentional contamination of water distribution networks: developing indicators for sensitivity and vulnerability assessments

Amir NAFI[1], Eric CRASTES[1], Rehan SADIQ[2], Denis GILBERT[3] and Olivier PILLER[3]

[1] Unité Mixte de Recherche Gestion territoriale de l'Eau et de l'Environnement (GESTE) IRSTEA-ENGEES, 1 quai Koch, 67070 Strasbourg Cedex, France. amir.nafi@engees.unistra.fr ; crastes.eric@gmail.com.

[2]School of Engineering, the University of British Columbia | Okanagan Campus, Kelowna, BC, Canada, V1V 1V7. Rehan.Sadiq@ubc.ca

[3]Irstea UR ETBX, Dept. of Water, Bordeaux Regional Centre, F-33612 Cestas, France. denis.gilbert@irstea.fr ; olivier.piller@irstea.fr

Abstract

Performing a comprehensive risk analysis is primordial to ensure a reliable and sustainable water supply. Though the general framework of risk analysis is well established, specific adaptation seems needed for systems such as water distribution networks (WDN). Understanding of vulnerabilities of WDN against deliberate contamination and consumers' sensitivity against contaminated water use is very vital to inform decision-maker. This paper presents an innovative step-by-step methodology for developing comprehensive indicators to perform sensitivity, vulnerability and criticality analyses in case of absence of early warning system (EWS), which may lead to reliable risk assessment. The assessment and the aggregation of these indicators with specific fuzzy operators allow identifying the most critical points in a WDN. Intentional intrusion of contaminants at these points can potentially harm both the consumers as well as water infrastructure. The implementation of the developed methodology has been demonstrated through a case study of a French WDN unequipped with sensors.

Keywords: Risk, vulnerability, sensitivity, backtracking, intentional contamination, fuzzy logic, aggregation, water distribution network, security.

1. Introduction

Water distribution networks (WDN) are considered as core public infrastructures because of their relevance to social and economic activities. Unfortunately, WDN are vulnerable against various sources of accidental and intentional contaminations (US EPA 2003). Accidental contamination can be generally due to compromise in water quality caused by external factors such as dysfunction of devices, human errors and aging infrastructure etc. Intentional contamination is due to malicious attacks through deliberated injection of contaminants into water supply system (Nilsson et al. 2005; Clark et al. 2008; Copeland 2010).

According to Di Nardo et al. (2014), a malicious act involves deliberately introducing chemical, biochemical or radioactive contaminants. Recently, Islam et al. (2015) conduct a comprehensive literature review on existing decision models addressing risk analysis in case of contamination intrusion. The awareness on the need of risk assessment methodology for potential malevolent attack for water systems has increased to counter potential bioterrorism acts.

Di Nardo et al. (2013) consider the intentional contamination of water network as a major risk for society. For authors contamination can occur by the introduction of biological or chemical contaminant in simple way as backflow attack for example. According to authors, contamination risk is not exclusively technical but is also due to managerial complexity, the characteristics of contaminant and the difficulty of describing the phenomenon of contaminant propagation. One of the key points is the ability of developing an Early Warning Systems (EWS) that ensures an early detection of the contamination by monitoring the water quality through some significant parameters such as pH, turbidity; 2 main actions can be carried out : i) alert the population and ii) to close contaminated area when it's possible to limit the propagation. Other approaches are based on the optimal location of measurement devices in order to identify source contamination. It seems that Water Network Partitioning (WNP) which consists in dividing the water network in permanent subnetworks called District Meter Area (DMA) are capable of protecting water network from attacks by isolating infected areas and stopping contaminant propagation without decreasing the performance of the entire network. Di Nardo et al. (2013) assess the impact of isolation of DMA few hours after a chemical contamination (potassium cyanide) of a water network unequipped with EWS.

Hart and Murray (2010) describe EWS and review several works around this topic. Authors realize a significant literature review concerning the problematic of optimal placement of sensors. It appears that sensors placement is one of the critical aspects of the design of EWS.

Hall et al. (2007) discuss recent initiatives of investigating how changes in some water quality parameters can potentially indicate contamination. Interrogations concern the set of parameters to consider and the appropriate sensors for on-line monitoring to detect potential contamination. Authors lists programs and set of parameters such as pH, free chlorine, oxidation reduction potential (ORP), dissolved oxygen, conductance, turbidity, total organic carbon (TOC), chloride, ammonia and nitrate. Sensors could be discriminated according to the type of monitored parameters, technology or manufacturer and their cost. Authors test several sensors by using a pilot scale distribution system simulator. They inject various types of contaminant and use several types of sensors in order to check the response of sensors to the injected contaminants and how quality parameters change. For authors the use of online monitors may increase water quality and constitutes a complimentary source of other monitoring data that could help to protect water network against contamination. Authors conclude that no single sensor responded to all contaminants but some of them respond to a large number of contaminants.

Murray et al. (2006) deals with spatiotemporal model for health risk distribution in case of contamination events of drinking water network. Authors develop a model that links flow and transport model to dynamic models for disease in order to estimate the spatial distribution of health risks due to ingestion of contaminated water. They discussed the effectiveness of an EWS on water quality sensors for reducing the risks of intentional contamination of water systems.

The effectiveness of sensors can also depend on its location and its capacity to be close to vulnerable area of the network. Ailmaki et al. (2003) describe a distribution and operation protocol for the location and the utilization of in situ sensors. Developed approach is based on the combination of a new algorithm for spatiotemporal data mining and a new modeling of water quality and security dynamics. Authors assume that effective early detection requires an extensive monitoring coupled with modelling of the link between varying distribution conditions, loading of pathogens and their persistence in the system. Responses issued from sensors require specific data evaluation for decision making.

The main focus of our work is to present decision aiding tools allowing a better preparedness against an intentional contamination of WDN that could be implemented independently or as part of an EWS. Proposed model is referred as **WARNING** (**W**ater **A**nalysis **R**isks for **N**etworks **I**ncidents and u**N**expected events **G**uidance). It has been adapted from the RAMCAP framework (Risk Analysis and Management for Critical Asset Protection) (ASME 2006), which has been used by the U.S. Department of Homeland Security to improve the risk analysis practice among various industrial sectors.

Proposed methodology employs multi-criteria decision analysis and fuzzy logic approaches by involving both theoretical and practical knowledge around two main elements of the WDN: i) consumers and ii) physical assets. Complexity of risk analysis framework depends on the level of knowledge of these components and how a contamination could possibly impact them. Proposed methodology intends to improve the understanding of the sensitivity of consumers and the intrinsic vulnerability of the physical assets against contamination events. This paper investigates the appropriate scale for analysis. It will identify potential risk locations that could correspond to a consumption place or a WDN asset based on the concept of "Criticality".

Proposed methodology uses a step-by-step approach, where each intermediate result enhances the knowledge of decision maker regarding risk of contamination in a WDN. To capture the details of the proposed methodology, two papers in series are presented.

Current paper predicts the WDN criticality and second paper combines the criticality analysis results with consequence analysis to perform risk assessment for intentional contamination.

In this paper, we build specific criteria to identify sensitive consumers and vulnerable assets in order to estimate the criticality of a WDN unequipped with sensors and where EWS does not exist. Following are the key points that will be addressed by the developed methodology:

- Intentional contamination: contaminated water in the WDN is the result of an intentional attack. The technical feasibility of the contaminant intrusion is also addressed which constitutes potential pathway.
- Intrusion of contaminant in the distribution network: contaminant is deliberately introduced into the WDN. A specific analysis of WDN components is required in

order to determine if they could constitute a potential intrusion point in accordance with the chosen pathways.

- Chemical or microbiological contaminants: analysis is restricted to only chemical or microbiological contaminants. The radioactive compounds or other derived substances are excluded from the analysis.
- Implementation of sensitivity analysis and vulnerability analysis in order to match most critical areas of WDN.

The paper is divided into 4 sections. A general description of the developed methodology is presented in the next section, which provides details on the sensitivity analysis, vulnerability analysis and related criteria. Section 3 illustrates an implementation of proposed methodology and discusses main results. Final section provides the conclusions and highlights improvements. and establishes the connection to the second paper.

2. Materials and Methods

Scope of this paper does not include production and storage systems as a potential source of the contamination event. Likewise, the vulnerability of the water resource(s) will not be considered in the risk analysis approach (i.e., the efficiency of the water treatment system will not be addressed).

The context of "intentional contamination" of a dynamic system delivering consumers implies adapting of the "first –order" risk definition[1] introduced by the RAMCAP framework. Hence, the Eq. (1) defines the risk caused by the intrusion of contaminant in the WDN as the combination of following three components:

$$\textit{Risk} = \textit{Consequences} \times \textit{Threat} \times \textit{Criticality} \quad (1)$$

The consequences of the water contamination will be evaluated for two main categories of impacts regarding to the water utility: i) impacts on the water utility and ii) impacts on third party that comprise impacts on human health and socio-economic activities.

The RAMCAP framework (ASME 2006) defines the *Threat* as "the likelihood of a specific attack scenario directed toward a specific asset". It seems hard to estimate the likelihood of particular scenarios. In general, risk is analyzed as a conditional risk with a maximal probability of occurrence (equal to 1). Thus, we assume that the occurrence of an attack is certain. This assumption leads to the simplification of the Equation (1).

[1] Risk = Consequences X Threat X Vulnerability

Estimating how vulnerable is the WDN in front of a contamination scenario requires the consideration of 2 sub-levels: i) the intrinsic vulnerability of WDN components -asset level- that could be considered as potential intrusion points (target); ii) the magnitude of the spread of contamination from the intrusion point to the water users, the network level. We define the Criticality of the WDN component (asset) as the combination of the intrinsic vulnerability of the component with the magnitude of the contaminant spread within the WDN.

$$\textit{Criticality} = \textit{Intrinsic Vulnerability} \times \textit{Contaminant Spread Magnitude} \quad (2)$$

The *Intrinsic Vulnerability* estimates the possibility of introducing contaminant into the WDN from a specific and predetermined point. To assess susceptibility of intrusion both technical characteristics and the environment of the intrusion point are analyzed. The *Magnitude of the contaminant Spread* from a determined intrusion point describes the water flow patterns within the WDN. This magnitude corresponds to the spatial dispatching of contaminant into the system. As the *Contaminant Spread* depends on hydraulics, a simulation model can be used to predict the propagation of the contaminant throughout the WDN as recommended by Nilsson et al. (2005).

Proposed risk analysis methodology enables to link three components of the risk equation, i.e., consequence, intrinsic vulnerability and contaminant spread magnitude. It appears that the risk assessment in case of intentional contamination of the WDN requires the pairing of intrusion and consumption points in terms of time and space scales. Developed methodology follows 4 main steps: 1) users' sensitivity analysis, 2) WDN vulnerability analysis, 3) consequences analysis and 4) risk assessment. The calculation of risk factors for risk assessment requires the aggregation of numerous sub-results derived from each step. Fig.1 proposes a conceptual framework for risk analysis. It consists of 3 levels of aggregation that successively enables estimating *contaminant spread magnitude, criticality* of the WDN components, and finally estimating the *risk* for the intentional intrusion of contaminant. Specific fuzzy membership functions and knowledge bases (KB) fitted according to the decision maker preferences are used for successive aggregation levels. The use of fuzzy logic approach concerns a wide range of problematics related to water systems. Panigrahi and Mujumdar (2000) develop a fuzzy rule based model for the operation of reservoir. Authors detail the use of fuzzy approach by explaining the construction of membership functions for the inflow, storage, demand and the release. They also define fuzzy operator and defuzzification method. Developed model had been applied to the Malaprabha irrigation reservoir in Karnataka, India. It appears that

fuzzy approach avoids complex optimization procedures and allows easy operation of system based on linguistic statements. Rehan et al. (2007) address risk of water quality failure in distribution network. Authors develop a methodology based on aggregative risk analysis approach where each risk assessment is expressed by triangular fuzzy number. chorzewska-Cieślak (2011) implements a failure risk approach based on fuzzy logic. Author defines 3 criteria as components of the risk and use specific membership functions to modelise each criterion. All steps of the implantation of fuzzy logic approach are detailed in pedagogic way and in order to assess the fuzzy risk of failure of water pipes based on specific inference rules. In our case, fuzzy logic is used to achieve the vulnerability analysis and to aggregate sub-results obtained from analysis shown by Fig.1.

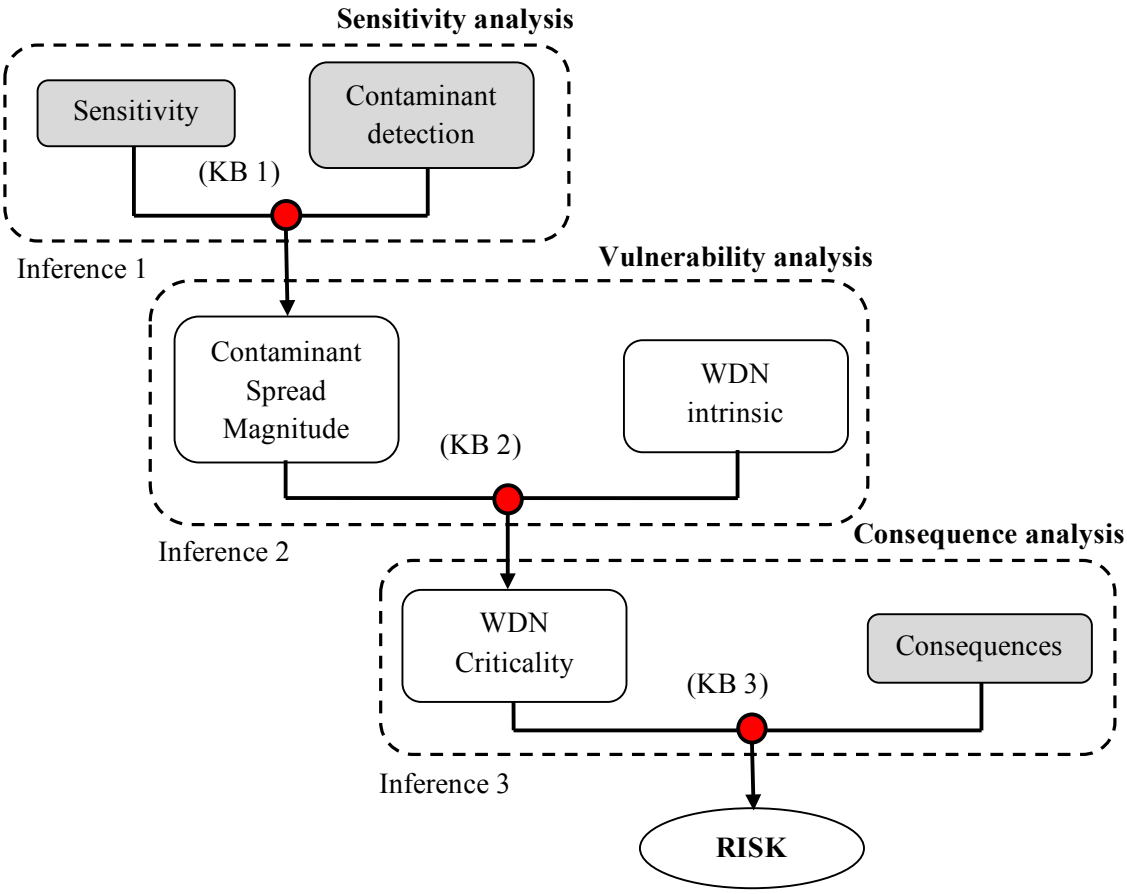


Fig.1. Proposed risk analysis framework

Factors in shaded boxes are the direct results of hydraulic simulations that are conducted as recommended by Nilsson et al. (2005). Simulations are performed during peak period by considering a specific mass loading of contaminant and according to demand characteristic. The combination of these parameters defines a contamination scenario as mentioned in Rasekh and Brumbelow (2013).

The first level of aggregation, “Inference 1”, evaluates the contaminant spread magnitude. In addition, the location of existing sensors in the WDN could help to better designate contamination location. We assume that the average time of detection corresponds to the elapsed time between the contaminant intrusion and its detection by sensors (if they exist) or by a positive concentration of the contaminant into nodes obtained by a hydraulic simulation in case of absence of sensors. This delay is taken into consideration to assess the contaminant spread magnitude in combination with the percentage of sensitive users exposed to the contaminant.

The second level, “Inference 2”, involves the assessment of the WDN components criticality based on *spread magnitude* and *WDN intrinsic vulnerability.* The third level of aggregation is done to perform risk assessment based on *criticality* and *consequences*. It can also be noted that several types of risks can be measured depending on the type of retained consequences (economic, environmental, social and sanitary). The following sections highlight the developed methodology to conduct each level of analysis.

2.1 Sensitivity analysis

This section aims at better understanding of the concept of sensitivity and more precisely the sensitivity of consumers against a potential contamination of water. The sensitivity of the WDN users can be defined both in terms of water quality and quantity regarding to their uses or potential consequences on health or usual activities. It depends on the typology of water uses and the intrinsic characteristics of consumers. For more clarity, we distinguish between sensitivity of consumers and vulnerability of WDN. One of the goal of this step is to highlight the main dimensions of sensitivity in order to build consistent and reliable criteria that are able to sort or rank users. In order to be exhaustive and transparent, a multi-criteria analysis (MCA) Roy and Bouyssou (1993) approach is implemented. Each step of the method is validated and amended by decision makers. Sensitivity analysis should be conducted through following steps as illustrated by Fig.2.

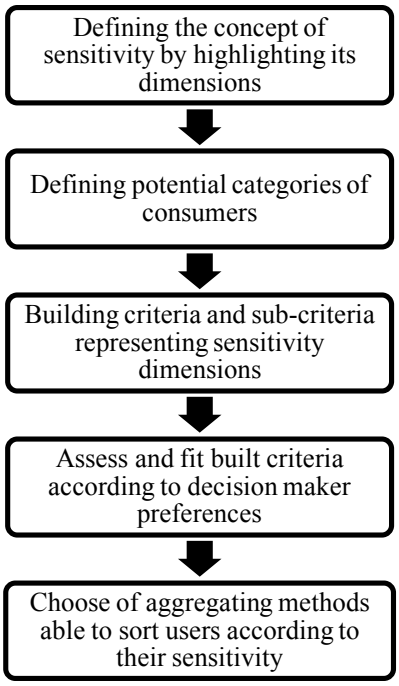


Fig 2. Steps for criteria building and assessment

It is crucial at this step of the analysis to observe water consumers according to their water uses and locations. In order to take into account potential water uses, consumers are sorted into 4 categories: i) Water for human consumption corresponding to the domestic use of water: drinking water, water for food and hygiene. Users included in this group (domestic users, office employees, schoolboys, hotel client…) are human beings (contrary to companies, shops, factories…) ii) Water for medical purposes corresponds to water used within the health facilities and the specific case of home-based patients of dialysis for example, iii) Water for recreational activities concerns all locations where the water is the object of recreational activities. This type of use has to be associated with places as aquatic park, swimming pool and municipal bath but also water jets and public fountains and iv) water for professional uses which concerns water used for industrial or service activities. In this case, the water user could be an organization or an institution (firm, company or shop).

Because water use differs from category to another, sensitivity analysis is based on the comparison of users belonging to the same category. Comparison is achieved based on exhaustive and non-redundant criteria and sub-criteria that handle potential dimensionalities of sensitivity with regard to the decision maker preferences. Because the users of the groups 1, 2 and 3 are individuals, user sensitivity of these 3 groups will be analyzed with the same

criteria. Evaluation of each criterion is done by specific mathematical function called performance function.

Because the group 4 is composed by companies, factories or firms other criteria were defined. The retained criteria and their respective performance functions are summarized in Table 1 and Table 2.

Tab 1. Criteria and sub-criteria for groups 1,2 and 3.

User belonging to groups 1,2 or 3					
Criteria	Definition	Sub-criteria	Definition	Evaluation of performance within normalized scale	Sens of preference
C_1 : Attractiveness as a target	It takes into account the socio-political context that could motivate an intentional contamination.	C_{1a}: Image and media attention	Assesses the representative symbol of the target for authorities or citizens.	P_{C1a} is estimated by step function where the value of criterion depends on the potential media attention focus	Increasing
		C_{1b}: Density of population	Estimates potential harmed people by assuming that attractiveness is higher for crowded locations.	P_{C1b} is calculated based on the density of population around a consumption node $P(d_i) = 0$ if $d_i<D_1$ $P(d_i) = [1/(D_2-D_1)]*d_i + D_1/(D_1-D_2)$ if $D_1 \leq d_i \leq D_2$ $P(d_i) = 1$ if $d_i>D_2$	Increasing
C_2: Level of frailty regarding the health state	Estimates the vulnerability of a part of the population regarding to their health state or age (babies and children, pregnant women, sick persons)	C_{2a}: Likelihood of welcoming vulnerable health persons	Probability of hosting vulnerable persons in the targeted location	$P(n) = \frac{n}{Total\ number\ of\ categories}$ Where n is the number of vulnerable health people categories.	Increasing
		C_{2b}:Age of the population in a given location	Age's repartition of targeted population in a given location	It expresses the likelihood to be ill according to the age of targeted people, its value is close to 0 for peoples between 18 and 60 years.	Decreasing
C_3: level of exposure	Measures the likelihood of ingesting contaminated water depending on the frequency of consumption and the targeted location.			Performance is measured based on the frequency of water consumption, f as follow: $P_{C3}(f) = \left(\frac{f}{3}\right)^3$	Increasing

Tab 2. Criteria and sub-criteria for groups 1,2 and 3.

User belonging to group 4					
Criteria	Definition	Sub-criteria	Definition	Evaluation of performance within normalized scale	Sens of preference
C'_1 : Attractiveness as a target	It takes into account the socio-political context that could motivate an intentional contamination by considering the user as a target.			$P_{C'1a}$ is estimated by step function where the value of criterion depends on the potential media attention focus	Increasing
C'_2: Number of employees	Estimates the potential number of persons that could be harmed in case of direct ingestion or activity interruption due to contamination.			$P_{C'2}(E) = K.\frac{1}{1+ae^{-rE}}$ Where E is the number of employee registered. The coordinates of the inflexion point J are$(\frac{Ln(a)}{r}\ ;\ \frac{K}{2})$.	Increasing
C'_3: Percentage of water supplied by the public WDN within the activity sector	Measures the dependence of considered user to water delivered by WDN. Augeraud and Touaty (2002).			The sensitivity is measured by the proportion of water delivered by WDN.	Increasing
C'_4:Vulnerability of the activity according to the type of water use within the activity sector	It measures the incidence of quality degradation on the considered activity by assuming difference in water quality used for production process or as thermal fluid in processes, 4 levels of water quality are defined: ultrapure water, drinking water, process water, industrial water.	C'_{4a}: Type of preponderant water use	Repartition of water use for the activity or production	Step function resulting from the aggregation of the sub-criteria where the higher level of performance is obtained for ultrapure water and the lowest for industrial water. Obtained function bycrossover between uses and water quality level.	Increasing
		C'_{4b}: Requirement level in terms of water quality	required water quality according to water use		

Once criteria are defined and evaluated, the relative importance of each criterion has to be determined based on the decision makers' preferences. Many approaches exist for the criteria weighting but it does not exist a real consensus in the literature concerning the most appropriate one. In order to ensure transparency and reproducibility of the process, we preconize the use of very simple procedure developed by (Simos 1990) and revised by Figueira and Roy (2002). It offers the advantages to be: i) very easy to implement and to understand ii) non-focused on the scale of the criterion evaluation, iii) involves ex aequo. Simos' procedure consists in assigning card for each criterion and ranking them with regard to decision maker's preferences. Once the cards are ranked, relative criteria weights are computed.

In order to conduct reliable risk analysis, it seems suitable to involve multiple perceptions of decision makers in order to achieve an exhaustive analysis. So, several stakeholders with different background and expertise can be involved in the weighting process. The use of Simos' procedure in this situation is not enough because it leads to a variety of weight sets, one for each involved decider. In order to obtain a compromise set of weights, the use of Ordered Weighted Average Operators (OWA) introduced by (Yager 1998) seems relevant. The OWA-based approach has a number of important benefits because it offers the possibility to involve multiple decision-makers context. The OWA procedure can be implemented in 3 main steps: i) Reordering the performance value of criteria in descending order, ii) Determining the weights[2] associated with the OWA operators and generate the OWA weights with an appropriate probability density function as suggested by Tesfamariam and Sadiq (2006), iii) aggregating process based on OWA weights. Concerning the generation of OWA weights, (Xu 2005) proposed the probability distribution function which the heights represent OWA weights. The λ parameter – i.e. quantile – corresponds to the location of the maximum weights. The normal distribution is obtained for $\lambda = 0.5$. It provides compromising OWA weight distribution. (Yager 1998) introduced the concept of orness α which characterizes the type of aggregation being performed for a particular value of OWA weighting vector.

The last step of sensitivity analysis is the aggregation of criteria in order to estimate the sensitivity of each user. This step consists in choosing the most appropriate aggregation methods considering a ranking problem in order to sort consumers and match the most sensitive.

[2]we will talk further about OWA weights in order to avoid confusion with the weights assigned to the sensitivity criteria by the decision makers

Let's consider $C_1, \ldots, C_n$ criteria, weighted respectively $w_1, \ldots, w_n$ and evaluated by $g_i(C_i)$ performance function. The sensitivity of consumer node j is assessed by the function $S_w(j)$ obtained by the equation (1):

$$\boldsymbol{S_w(j) = \sum_{i=1}^{n} w_i \times g_i(C_i)} \tag{3}$$

For practical reasons, the weighted sum seems the most adapted method because of its simplicity of implementation.

In order to assess the magnitude spread of contaminant, the identification of the most contaminant locations from where contaminant can be introduced and potentially harm sensitive users must be done. A specific inverse model is implemented in order to identify the potential sources of contamination based on backtracking algorithm developed by Ung et al. (2013).

Considering that velocities in the network are known in an extended period simulation, the inverse model is done by resolving the adjoint problem of transport on the graph obtained from the water network. The equation of classical 1D transport model is:

$$\frac{\partial S}{\partial t} + v\frac{\partial S}{\partial x} + KS^{\alpha} = 0,$$

Considering S is the scalar value (the contaminant concentration), V the velocity, X the position, K and α parameters (constant and order) of the kinetic law. We use a conservative law (K == 0) to be in the worst case and a complete and perfect mixing at junctions. The adjoint equations give a solution to reach possible source for a contamination P:

$$\frac{\partial P}{\partial \tau} - v\frac{\partial P}{\partial \chi} = 0,$$

Where $\tau = T_0 - t$ and $\chi = X_0 - x$. This can be interpreted as "turn the clock back". The problem is solved by a Lagrangian characteristic method as described in (Ung 2016) initialized by value of P equals to 1 at the user's node to be contaminated.

(Ung 2016) builds an input/output matrix to show if a node is contaminated from a potential source nodes.

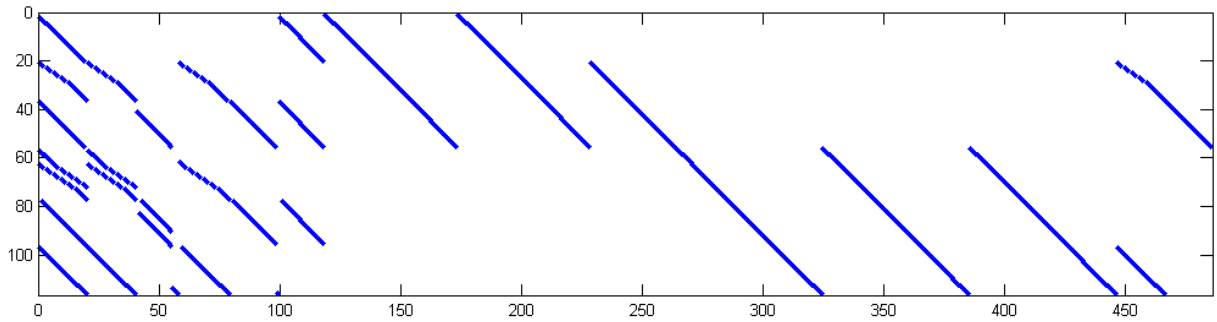


Fig 3. Input/output matrix of contamination, blue points are non-zero (Ung 2016).

Each line of the matrix shows a node with sensitive user, each column potential sources. The points aligned as diagonals show the duration of contamination from sources to surveyed node.

Backtracking matches the paths of contaminant spread between sensitive users' locations and potential intrusion points from where they could be harmed.

Inverse transport model is faster than standard hydraulic simulation. As shown in figure 4, it matches the most frequent contaminant nodes for the most sensitive users. This sub-result combined with the intrinsic vulnerability enables the selection of vulnerable nodes that could constitute potential injection points of contaminants. The preselection of intrusion points allows generating more realistic contamination scenarios and simulating most probable situations based on the hydraulic operation of the WDN. So backtracking enables to link sensitivity analysis with the next section dealing with the vulnerability of WDN components.

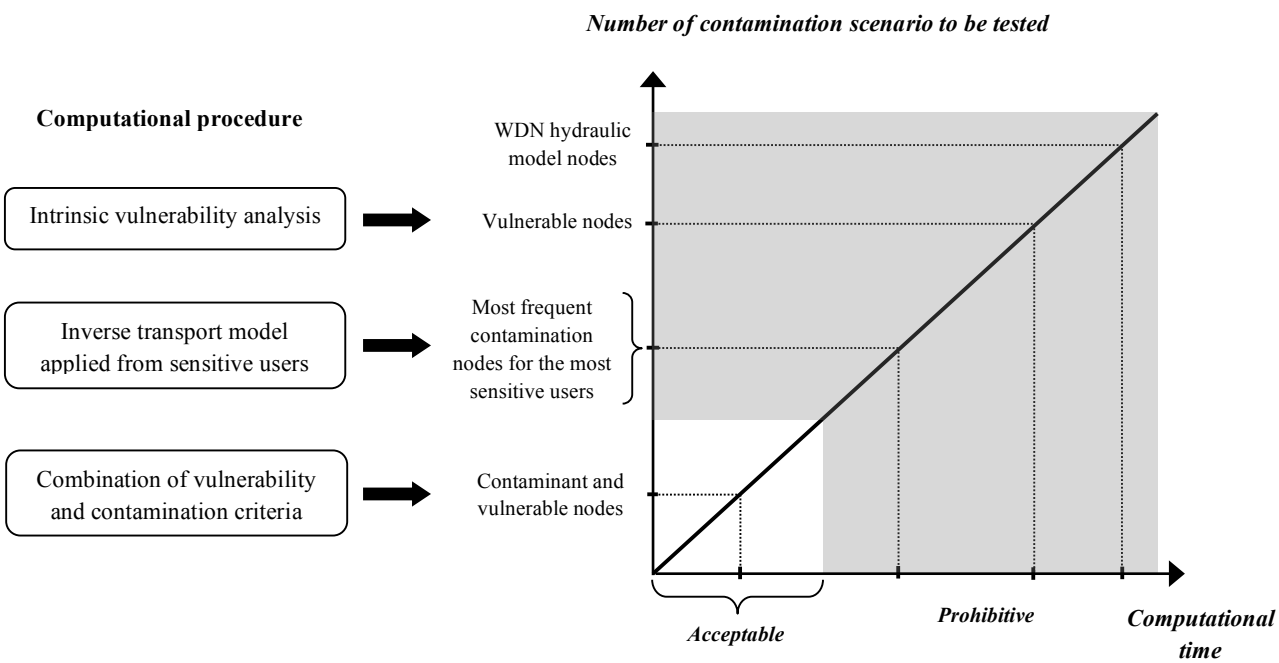


Fig 4. Contamination scenario and computational time

2.2 Vulnerability analysis

Vulnerability analysis estimates the relative preparedness of WDN components to potential attack. Ezell et al. (2000) develop an interesting approach by assigning "access" and "exposure" fuzzy factors. "Access" corresponds to the degree of protection of the device and "exposure" corresponds to its degree of visibility or accessibility. Ezell et al. (2000) assume that the total vulnerability is the product of access and exposure. Torres et al. (2009) implement this approach for risk screening in order to sort WDN nodes that require more attention and to be analyzed in depth. Authors conduct a vulnerability analysis with the help of Geographic Information System (GIS) on virtual city, "Micropolis". We adapt and build specific criteria to deal with the axiom defined by Ezell et al. (2000), even if the basis is quite similar, our approach seems more practical. It improves the understanding and the estimation of vulnerability by crossing information concerning the network and its environment.

The vulnerability analysis is carried out at the scale of each device or asset based on the assessment of an intrinsic vulnerability index obtained from Fuzzy Rule Base (FRB) aggregation scheme of two dimensions of vulnerability, i.e. : i) structural vulnerability and ii) vulnerability linked with the environment of the intrusion site. Each component of WDN represents a potential intrusion site of contaminant. Under the assumption of intentional contamination, the injection device produces the driving force (i.e., pressure) needed to introduce the contaminant, it could be a pump and fittings to connect it to existing paddle clamp or socket clamp. The contaminant to be injected is assumed in a liquid state or contained in a liquid. In order to measure asset's vulnerability, a classification of intrusion sites is done based on the following characteristics: i) control structures equipped with a by-pass system, ii) WDN components connected to the pipe through a paddle clamp, iii) fire-fighting equipment, iv) unburied and unprotected pipes.

The *Intrinsic Vulnerability* describes the level of protection of WDN devices against contaminant intrusion. It corresponds to the combination of the *structural vulnerability* and the *vulnerability linked to the environment of the intrusion point*.

The *structural vulnerability* depends on the technical characteristics of the intrusion site. It could be estimated based on the combination of the following criteria: i) ease of physical access to the intrusion site according to its immediate environment and ii) level of surveillance according to existing devices or observers.

Tab 3. Criteria for vulnerability assessment

Criterion	Linguistic variables	Score	Source of data
Ease of physical access (Cv_1)	- private area - public place as square or garden - roadway	0 – 100	GIS Or specific database
Level of surveillance (Cv_2)	- citizen - sentinel - guard - camera - alarm	0- 100	Feedback from water utility employees

The aggregation of proposed non-commensurate criteria is performed by an uncertainty index-based approach using the Fuzzy Inference System (FIS) developed by Francisque et al. (2009). It combines 3 inference engines as illustrated in Fig. 5.

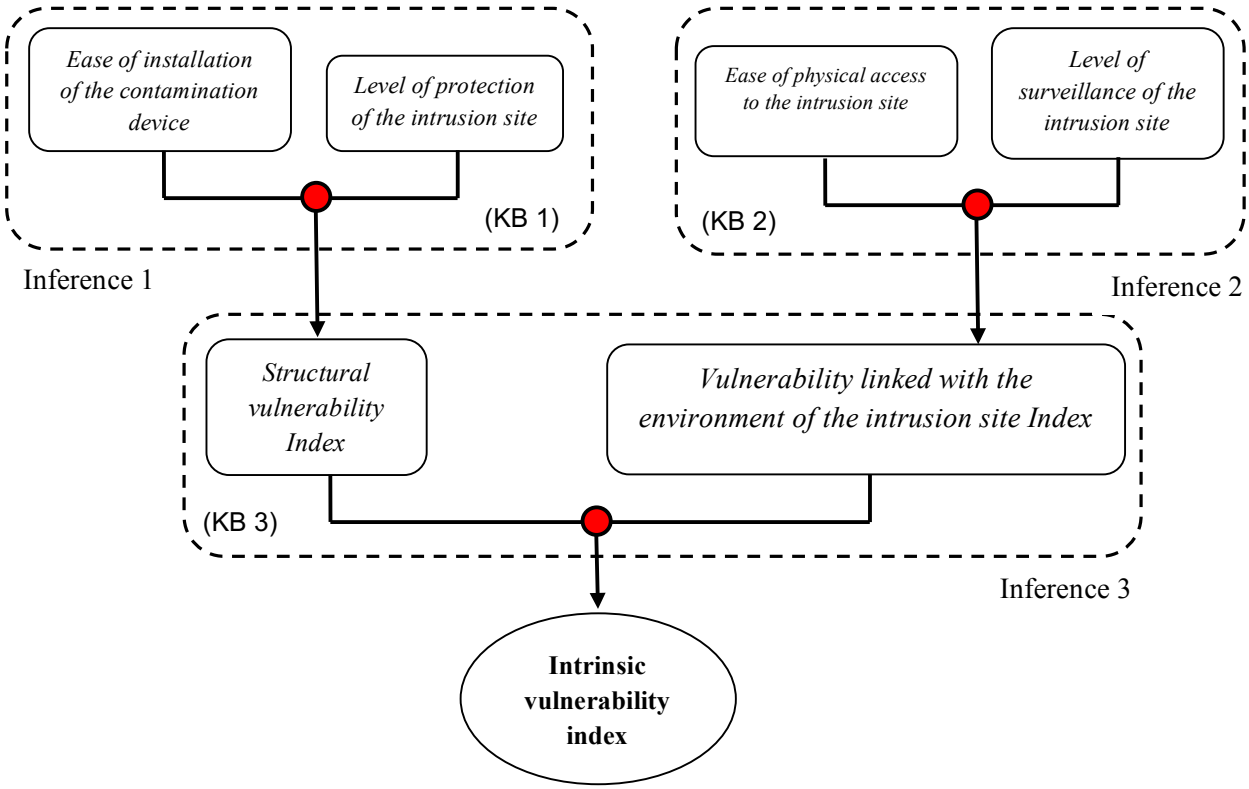


Fig.5. Fuzzy hierarchical structure for the evaluation of the intrinsic vulnerability

The three Inference Engines will be supplied respectively by three knowledge bases (KB) as explained in appendix.

In order to combine the 3 inference engines and implement the Fuzzy Inference Systems, an open source library for fuzzy systems called jFuzzyLogic and developed by Cingolani and Alcala-Fdez (2012) was used. The outputs of the inference engines 1 and 2 – outputs which are crisp values - are then partitioned into 3 levels (Low / Medium / High) and represented by triangular fuzzy set mapped into a relative scale as described for the inputs. These outputs correspond to the input fuzzy sets used by the inference engine 3.

The results of this third inference engine are represented by a triangular fuzzy set partitioned and mapped in the same way as outputs of the inference engine 1 and 2. This last triangular fuzzy set is then defuzzified into a single crisp value; **the intrinsic vulnerability index**.

Remember that the scale of analysis corresponds to a node in hydraulic model that could represent a group of consumers or potential intrusion point. So even if vulnerability analysis deals with assets, the intrinsic vulnerability index has to be affected to the nearest consumption node of intrusion point. The estimation of criticality is also achieved at nodes level, it is obtained by crossing two assessments, the spread magnitude of contaminant which is output of sensitivity analysis and the intrinsic vulnerability index.

3. Case Study

The proposed methodology was applied on an urban WDN delivering about 400 000 inhabitants along 1082 km of pipes. WDN operation was modelled with help of hydraulic model computed by Porteau® 4.0 (Porteau 2016) of about 9 200 consumption nodes, 11 000 pipes and around 2300 loops. The Hydraulic model is mainly used for simulating contaminant spread into the network.

3.1 Sensitivity analysis using multi-criteria approach

The following section details the implementation of the analysis to the water users belonging to the groups 1, 2 and 3 (persons) and the group 4 (organizations). The first step consists in building GIS users database. In order to create the group of users, the water users and their characteristics have been associated with the location where the water is used or consumed. Two different geo-referenced databases have been used for the creation of the GIS user database: i) the postal address database and ii) the "Sirene®"[3] database. The structures of these 2 databases have been modified in order to be aggregated into a single database of

[3]« Système Informatisé du Répertoire National des Entreprises et des Établissements » Governmental database of all French public and private organisations

49,162 users belonging to the group 1, 2 and 3, representing persons and 9,180 users belonging to group 4 representing organizations on the territory of considered WDN. As explained in section 2, specific criteria were defined for each category of user. For group 1, 2 and 3 users, weighting procedure of criteria is based on "Simos" procedure. The following spider plots illustrate weights attributed to the group 1, 2 and 3 criteria by 8 employees – representing stakeholders- from the water quality department of the concerned utility:

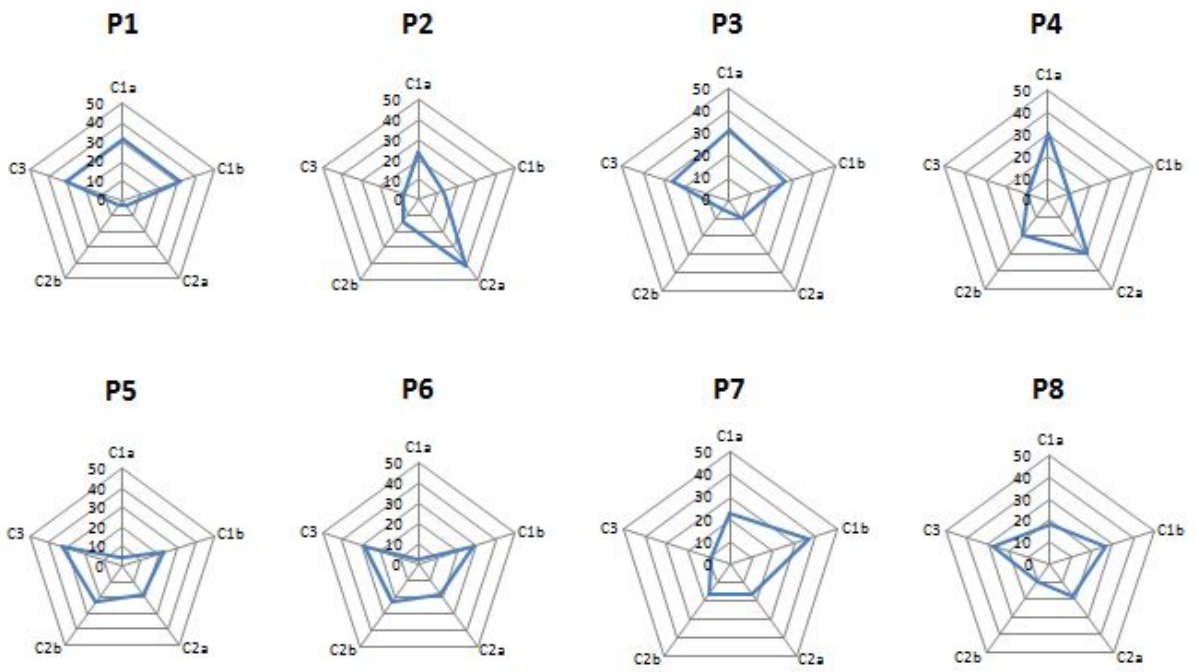


Fig.6. Groups 1,2 and 3 - Criteria weighting with Simos' procedure.

The Fig.6 shows preferences of each decision makers according to their position and role in the operation and the management of the WDN. In order to take into account the 8 decision makers preferences, OWA (Ordered Weighting Averaging) for aggregation operator weights were generated using standard normal distribution (n = 8) with λ = 0.5. The weight vector, W is obtained as follow: W = (0.059, 0.104, 0.152, 0.184, 0.184, 0.152, 0.104, 0.059).

The aggregating results using the Normal distribution are summarized in the following table and are plotted in Fig. 6.

Tab 4. Groups 1, 2 and 3 - OWA aggregating results.

Criterion	**Code**	**Weight (%)**

Attractiveness as a target Image and media attention	C_{1a}	21.3
Attractiveness as a target Density of population	C_{1b}	24.5
Level of frailty regarding the health state Probability of welcoming vulnerable health persons	C_{2a}	18.3
Level of frailty regarding the health state Age of the population in the given location	C_{2b}	14.0
Level of exposure	C_3	21.9

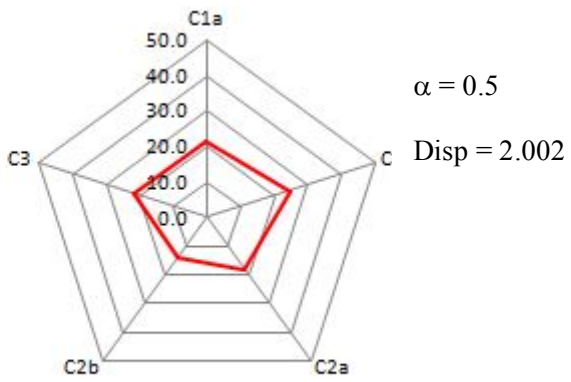


Fig.7. Groups 1, 2 and 3 - OWA aggregating results – Spider graph

The value of *orness* (that measures the degree of disjunction) α is 0.5 as expected. Regarding the dispersion the high value close to maximum value of ln(8) ≈ 2.08 indicates that the OWA weights generated using Normal distribution use information from "most" of the arguments. This situation indicates that OWA aggregating results tends to a trade-off solution regarding to decision maker answers. The following table describes in detail the utility functions, which have been used to evaluate the performance of the criteria according to normalized scale between 0 and 1.

Tab 5. Utility function proposed for group 1, 2 and 3.

Criterion	Code	Utility function	Comments
Attractiveness as a target Image and media attention	C_{1a}	Step function defined as follows: Governmental entities = 1 Hospital = 0.5 Others = 0	We arbitrarily adopted a specific context which identifies the governmental entities as the most attractive target. Hospitals and governmental entities have been selected within the GIS user database using the APE nomenclature
Attractiveness as a target Density of population	C_{1b}	The density has been defined as: - the number of persons per postal address for the domestic users - the number of employees per consumption point D_1= 10 D_2= 40	The following data are not yet available: - Number of patients per hospital - Number of children per school - Number of swimmer per swimming pool We considered that the consumption points gathering 40 and more than 40 persons are considered as equivalent in terms of density Idem for the consumption points gathering 10 or less than 10 persons
Level of frailty regarding the health state Probability of welcoming vulnerable health persons	C_{2a}	P (n) = n / 7 Where n is the number of vulnerable health persons at the level of the consumption point	A total of 7 vulnerable health person categories have been identified. The APE nomenclature has been used in order to define the number of vulnerable people per consumption point
Level of frailty regarding the health state Age of the population in the given location	C_{2b}	The performance of the criteria is proportional to the sum of percentages of persons whose age is less than 13 and more than 65.	The age pyramid is available at the level of IRIS geographical districts. The percentages have been directly affected to the consumption points which represent domestic users. Thanks to the APE nomenclature the following entities received the maximal score of 1: - Hospital - Retirement home - Schools - Nursery The remaining users received zero
Level of exposure	C_3	$P_{C3}(f) = \left(\frac{f}{3}\right)^3$ Where f is the frequency of water consumption in a given location	The table 6 proposes values for the evaluation of the frequency of water consumption according to the location.

For each consumption node a weighted sum is calculated based on defined utility functions. The obtained value serves for nodes sorting in order to identify the most sensitive nodes. Fig.8 illustrates some of them in a part of the WDN.

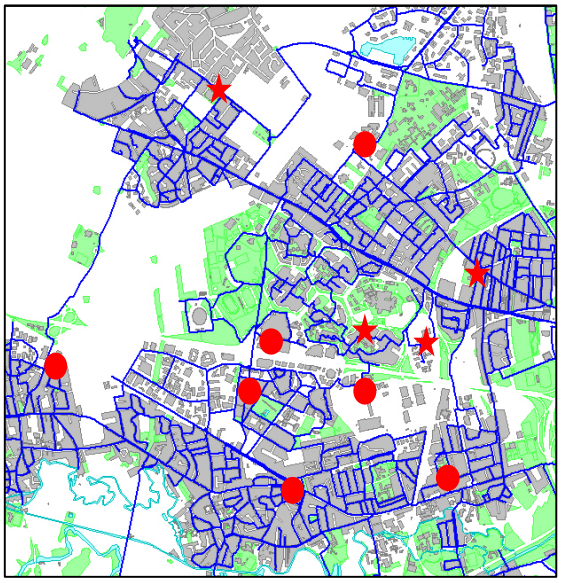


Fig.8. Location of sensitive users from groups 1,2 and 3 (red stars) and group 4 (red dots) in a part of the network.

Results analysis indicates a relatively homogenous geographical distribution of the most sensitive users. It should however be noted a slightly higher density of sensitive users in downtown. The sensitive users' distribution highlights clusters, which are located in different parts of the WDN. The Groups 1, 2 and 3 most sensitive users are mostly composed by hospitals; residential care activities for elderly; collective housing; and governmental buildings.

As for groups 1, 2 and 3, the normal distribution has been used in order to aggregate the preferences of 8 decision makers for the group 4. The aggregating results are summarized in the Table 6.

Tab 6. Group 4 - OWA aggregating results.

Criterion	Code	Weight (%)
Attractiveness	C'_1	23.5
Number of employees	C'_2	19.4
% of water from WDN	C'_3	15.6
Vulnerability of the activity according to the	C'_{4a}	29.5

type of water use within the activity sector		

Table 7 describes in details the utility functions, which have been used to evaluate the performance of the criteria.

Tab 7. Utility functions proposed for the group 4.

Criterion	Code	Utility function
Attractiveness as a target Image and media attention	C'$_1$	-
Number of employees	C'$_2$	$P_{C'2}(E) = \frac{1}{1 + 50e^{-0.15*E}}$ With E number of employees
Percentage of water supplied by the public WDN within the activity sector	C'$_3$	The APE nomenclature has been used in order to characterize activities and make the link with table 7 information
Vulnerability of the activity according to the type of water use within the activity sector	C'$_4$	Step function with θ = 0.2

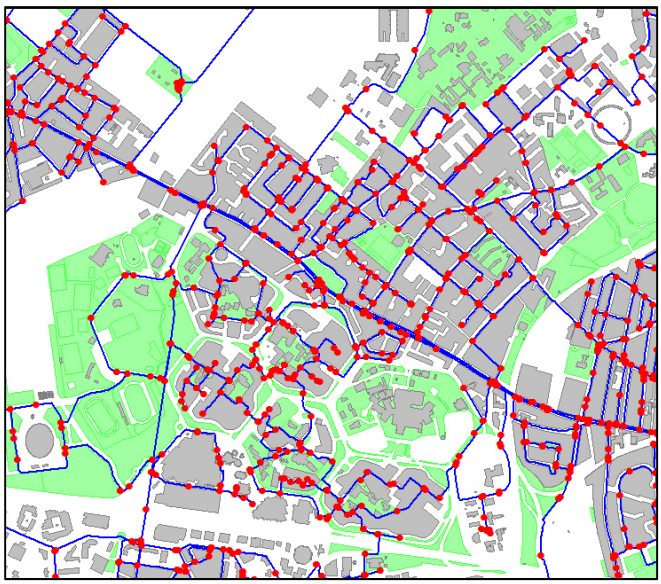


Fig.9. Location of vulnerable nodes (red dots) in part of the WDN.

It seems that a higher density of users from group 4 is in downtown. This finding is consistent with sensitivity criterion definition and weighting which provide a higher sensitivity score to catering, restaurant and food production.

3.2 Vulnerability analysis

The following section describes how the GIS WDN asset database has been built and used for the inference engine which enables to aggregate the vulnerability criteria for assessing vulnerability index.

In order to define as exhaustively as possible the potential intrusion points, several geo-referenced information layers have been collected.

Seven different layers have been combined: private connection (49162 items), fire hydrant (4824 items), underground hydrant (4824 items), flow rate measuring station (83 items), sampling point pit (261 items), air bleeding (141 items) and valves box (382 items). As a result, 58 299 intrusion points among which more than 84% are private connections constitute the GIS WDN asset database.

As a reminder, the intrinsic vulnerability is the combination of the structural vulnerability and the vulnerability linked to the environment of the intrusion point. Four criteria for vulnerability analysis Cv_i have been defined as follow:

- Ease of installation and implementation of the contamination device (Cv_1)
- Level of protection of the intrusion site (Cv_2)
- Ease of physical access to the intrusion site (Cv_3)
- Level of surveillance of the intrusion site (Cv_4)

The evaluation of criteria Cv_1 and Cv_2 has been done according to a specific study related to characteristics of hydraulic devices.

The evaluation of criteria Cv_3 and Cv_4 takes into consideration the environment of the asset. To describe this aspect, the presence of road (primary and secondary) and green spaces (as a public place) has been superimposed on the intrusion point database. Furthermore, the additional information provided by the item itself (private or public) completes the analysis. As a result, the following normalized scores have been applied for the evaluation of criteria:

Tab 8. Vulnerability criteria assessment.

Item	Cv_1	Cv_2	Cv_3	Cv_4

Private connection	80	90	100	90
Fire hydrant	70	90	75	50
Underground hydrant	65	90	75	50
Flow rate measuring station	70	10	*See Table 12*	
Sampling point pit	65	75		
Valve box	75	75		
Air bleeding	75	75		

Tab 9. Assessment of criteria Cv_3 and Cv_4.

Criterion	Primary road	Secondary road	Green space / public garden	Private	Other
Cv_3	25	50	75	100	66
Cv_4	33	33	50	66	66

Thanks to these scores, the vulnerability of each intrusion point is calculated. The list of intrusion points is recorded into an MS Excel® file and is scanned by a fuzzy logic java program which calculates the intrinsic vulnerability using inference engine. As explained before, even if vulnerability analysis is conducted on WDN asset, results should be attached to consumption node in order to be able to link both sensitivity and vulnerability analysis.

It appears that the number of consumption nodes (14,889) is 5 times less than potential intrusion points (58, 299), which means that several WDN assets are connected to the same node after transfer. So, the retained vulnerability value to be assigned to a given node is the maximum value of vulnerability among the WDN assets connected to the node. Finally 8,632 model nodes are assigned with a value of intrinsic vulnerability strictly greater than zero. Among these vulnerable nodes 28.5 % (2,458 nodes) have a maximum value of intrinsic vulnerability.

In order to finalize the vulnerability analysis, it is necessary to assess the contaminant spread magnitude into the WDN. This step uses a specific module in Porteau® software based on an inverse transport module. In our approach this inverse simulation starts from the most sensitive users and enables us to identify the contaminant nodes. The proposed methodology assumes that the correspondence between existing users and consumption nodes as

represented by the hydraulic model is obtained by gathering several users in a given node with the help of specific transfer ratio. This ratio is equal to 50 for users group 1, 2 and 3 and it is equal to 10 for the group 4. This grouping procedure leads to obtain 7,458 model nodes with a value of sensitivity strictly greater than zero. For practical reasons, the 1% most sensitive nodes (75) are selected to be considered as potential targets.

The expected results are the potential sources of contamination of these 75 nodes across a defined elapsed time window. In order to take into account the worst-case scenario, two contamination-time periods have been defined, each time period matching with the two daily water consumption peak periods : i) from 6 to 9 am and ii) from 6 to 8 pm. As a result and represented in yellow in Fig.10, 43 % of total nodes have been identified as potential sources of contamination of the 1 % most sensitive users.

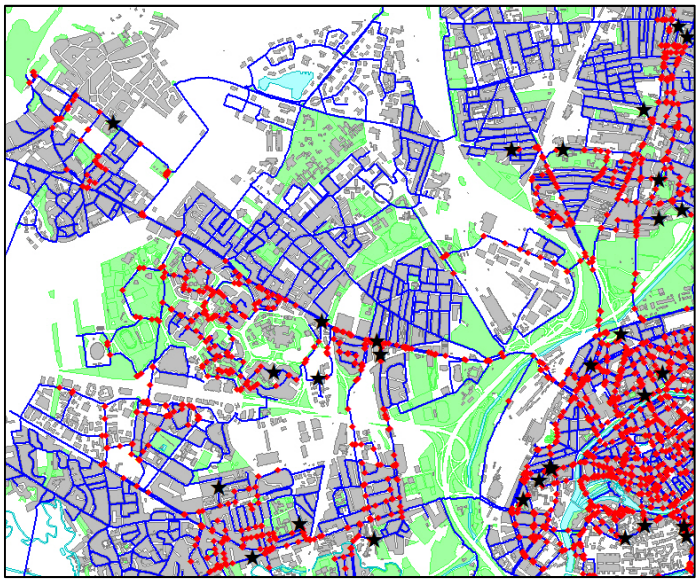


Fig.10. Sample of potential sources of contamination (yellow dots) for the most sensitive users (red dots)

3.3 Criticality analysis

Criticality analysis prioritizes the most contaminant and vulnerable consumption nodes derived from vulnerability analysis.

Among potential sources of contamination obtained by backtracking, 56 % of contaminant nodes are assigned with a value of intrinsic vulnerability strictly greater than zero. By assuming that a critical node is both contaminant and vulnerable, vulnerable nodes have been sorted according to their frequency of occurrence as contaminant nodes. On that basis, nodes

that occur more than one hundred times are considered as the most frequent vulnerable contaminant nodes. At the end, 483 nodes are retained as pathways for the contaminant intrusion and define the set of critical nodes from where an attack could harm severely WDN consumers. The Fig. 11 shows some of critical nodes.

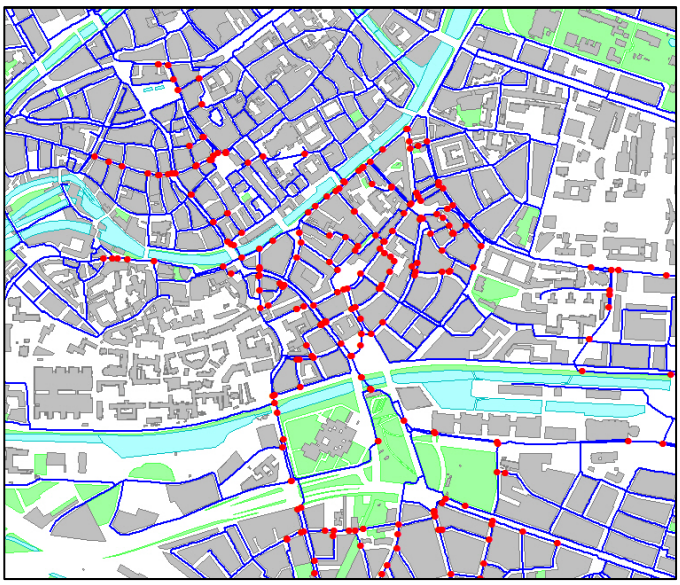


Fig. 11. Location of some critical nodes

The set of critical intrusion points constitute a prerequisite for mitigating the capacity of attackers to contaminate WDN. The assessment of possible pathways is not enough, even if potential actions to secure WDN are not addressed in the current paper, they constitute one of the goals of criticality analysis, the assessment itself is not sufficient. Specific actions should be planned and implemented to secure WDN. The efficacy of these actions can be measured by re-implementing criticality analysis in order to check if number of critical points for example decreases with regard to corrective security actions. It appears that criticality analysis is a continuous process of improvement. Criticality analysis provides relevant intermediate results for risk assessment by defining the potential intrusion points that should be handled in the simulation of contamination scenarios in order to assess potential consequences of an intentional contamination.

4. Conclusions

The developed methodology allows enhancing the knowledge of WDN manager against the capacity of attackers to harm WDN where an EWS is not available. The main added value of presented work concerns the achievement of innovative and integrated analysis by matching both consumption nodes, considered as location of consumption and assets of WDN

considered as potential targets of an attack. The criticality analysis is based on the understanding of sensitivity of consumer according to their uses and the vulnerability of WDN unequipped with sensors and without EWS to potential attacks. For both analysis, the decision maker preference is taken into account by the co-built of specific criteria, evaluation function and fuzzy membership functions which needs a real skills in terms of multi-criteria and fuzzy logic methods in order to understand and translate decision maker preferences. So the effective improvement is on the methodological and practical point of view. A detailed panorama for both methodology and its implementation is presented. One of the main backgrounds of the current work concerns the possible distortion between the conceptual model and reality. Data availability, the existence of hydraulic model and WDN asset GIS are required to conduct a reliable criticality analysis. Many adaptations and modifications of existing data are required in order to implement the proposed methodology. The implementation is not automated; the link between steps is done manually all these aspects render the methodology complex and could constitute a handicap for water utility. As for each model, it simplifies the reality, so consumption nodes of hydraulic model for example correspond to an aggregation of real consumers with certain multiplier factors; this implies that the level of accuracy of the approach depends on the capacity of used models to be close to reality. This aspect does not constitute a shortfall but must be taken into account for the implementation and the interpretation of criticality results. Despite possible improvements of WARNING methodology, it offers the possibility to WDN manager to conduct a risk analysis in structured and reproducible way. It also allows identifying the most critical points that could constitute potential pathways for intentional contamination and possible locations to install sensors for water quality as a part of an EWS.

The step after consists in proceeding risk analysis by generating contamination scenario based on critical points to assess the potential consequences both on consumers and WDN assets. The next step of risk analysis is addressed in the following paper. It deals with the type of potential risks (economic, health, environmental, social, etc.) and how they could be measured. A focus is done on consequences assessment by developing specific indicators combining theoretical and particle knowledge. As result, hotspot or risky areas are matched. They constitute a priority for investigation and protection for WDN manager.

Acknowledgements

The work presented in the paper is part of the French-German collaborative research project *SMaRT-Online*^{WDN} that is funded by the French National Research Agency (ANR project:

ANR-11-SECU-006) and the German Federal Ministry of Education and Research (BMBF; project: 13N12180).

5. References

Ailamaki A, Faloutos C, Fischbeck P.S, Small M.J, VanBriesen J.(2003). An environmental sensor network to determine drinking water quality and security. ACM SIGMOD Record. New York, NY, USA. 32(4): 47-52.

American society for mechanical engineering, ASME (2006).RAMCAP: The Framework. (version 2.0) ASME Innovative Technologies Institute, LLC.

Augeraud P and Touaty M (2002) Consommation d'eau par les secteurs industriels. Planistat France. Rapport final, 97p.

Bernard R, Bouyssou D (1993) Aide multicritère à la décision : Méthodes et cas, Paris, Economica, ISBN 2-7178-2473-1 , 695 pages.

Cingolani P, Alcala-Fdez J (2012). jFuzzyLogic: A Robust and Flexible Fuzzy-Logic Inference System Language Implementation. *In* FUZZ-IEEE Pp. 1–8. Citeseer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.415.3325&rep=rep1&type=pdf, accessed August 31, 2015.

Clark R, Chandrasekaran L and Buchberger S (2008) Modeling the Propagation of Waterborne Disease in Water Distribution Systems: Results from a Case Study. 8 th Water Distribution Systems Analysis Symposium 2006: 1-20. Cincinnati, USA. doi: 10.1061/40941(247)71.

Copeland C (2010). Terrorism and security issues facing the water infrastructure sector, in: Report for Congress, Congressional Research Service, Order Code RS21026, Washington, DC, USA, 21 p. https://www.fas.org/sgp/crs/terror/RL32189.pdf, accessed Mai 10 2016.

Di Nardo A, Di Natale M, Musmarra D, Santonastaso G.F, Tzatchkov V and Alcocer-Yamanaka V-H. (2014) A district sectorization for water network protection from intentional contamination. 12th International Conference on Computing and Control for the Water Industry, CCWI2013. Procedia Engineering 70: 515 – 524. doi: 10.1016/j.proeng.2014.02.057.

Di Nardo A, Di Natale M, Guida M, Musmarra D. (2013). Water Network Protection from Intentional Contamination by Sectorization. Water Resources Management. 27 (6):1837 –1850.

Ezell BC, Farr JVand Wiese I (2000) Infrastructure risk analysis of municipal water distribution system. Journal of Infrastructure Systems 6(3):118–22.

Figueira J and Roy B (2002) Determining the Weights of Criteria in the ELECTRE Type Methods with a Revised Simos Procedure. European Journal of Operational Research 139(2): 317–326.

Francisque A, Rodriguez M J, Sadiq R, Miranda L F and Proulx F (2009). Prioritizing Monitoring Locations in a Water Distribution Network: A Fuzzy Risk Approach. Journal of Water Suppl: Research and Technology-AQUA 58 (7): 488–509.

Hall J, Zaffiro A D, Marx R B, Kefauver P C, Krishnan E R and Herrmann J G (2007) Online water quality parameters as indicators of distribution system contamination. Journal American Water Works Association. 99(1): 66–77.

Hart WE and Murray R (2010). Review of Sensor Placement Strategies for Contamination Warning Systems in Drinking Water Distribution Systems. Journal of Water Resources Planning and Management. 136 (6) : 611-619.

Murray R E, Grayman W M, Savic D A and Farmani R (2010) Effects of DMA redesign on water distribution system performance. Integrating Water Systems – Boxall & Maksimovi´c (eds) © 2010Taylor & Francis Group, London, ISBN 978-0-415-54851-9.

Nilsson K A, Buchberger S G and Clark R M (2005). Simulating Exposures to Deliberate Intrusions into Water Distribution Systems, Journal of Water Resources Planning and Management 131 (3): 228-236

Panigrahi, D P and Mujumdar P P (2000). Reservoir operation modeling with fuzzy logic. Water Res. Manage. 14:,89–109.

Porteau , (2016). Porteau 4.0 , Logiciel de modélisation hydraulique. http://porteau.irstea.fr/. Accessed Mai 10 2016.

Rasekh A, Brumbelow K (2013). Probabilistic analysis and optimization to characterize critical water distribution system contamination scenarios. J. Water Res. Plan. Manag 139 (2): 191-199.

Sadiq R, Kleiner Y, Rajani B (2007) Water quality failures in distribution networks—risk analysis using fuzzy logic and evidential reasoning. Risk analysis 27 (5): 1381-1394.

Simos J (1990). L'évaluation Environnementale: Un Processus Cognitif Négocié. Thèse de doctorat. DGF-Lausanne, Suisse.

Tchórzewska-Cieślak B. (2011). Fuzzy failure risk analysis in drinking water technical system. Reliability: Theory & Applications. 1 (20): 138-148.

Tesfamariam S and Sadiq R (2006) Risk-Based Environmental Decision-Making Using Fuzzy Analytic Hierarchy Process (F-AHP). Stochastic Environmental Research and Risk Assessment 21(1): 35–50

Torres J M, Brumbelow K and Guikema S D (2009) Risk Classification and Uncertainty Propagation for Virtual Water Distribution Systems. Reliability Engineering & System Safety 94(8): 1259–1273.

Ung H (2016) Quasi real-time model for security of water distribution network. Modeling and Simulation. Université de Bordeaux, Phd Thesis. Online version: https://tel.archives-ouvertes.fr/tel-01310849/, accessed March 2017 .

Ung H, Piller O, Gilbert D and Mortazavi I N.d. (2013) Inverse Transport Method for Determination of Potential Contamination Sources with a Stochastic Framework. In World Environmental and Water Resources Congress, ASCE. : 798–812.. http://ascelibrary.org/doi/abs/10.1061/9780784412947.077, accessed August 28, 2015.

US EPA (2003). Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents,17p. Online version: http://www.epa.gov/safewater/watersecurity/pubs/guide_response_overview.pdf. accessed August 28, 2015.

Xu Z (2005). An Overview of Methods for Determining OWA Weights. International Journal of Intelligent Systems 20(8): 843–865.

Yager RR (1998). New Modes of OWA Information Fusion. International Journal of Intelligent Systems 13(7): 661–681.

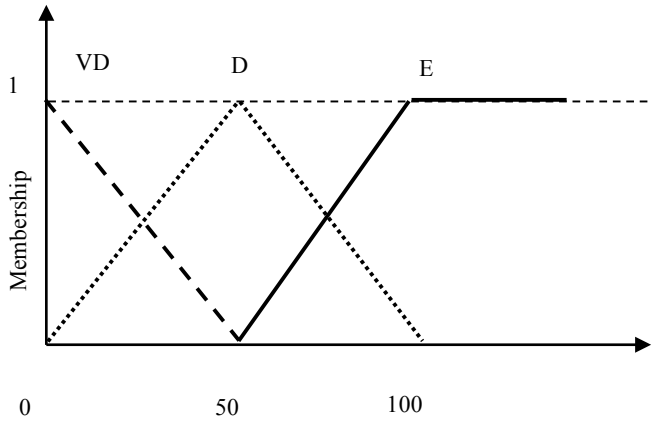
SMaRT-online^{WDN} (2015), http://www.smart-onlinewdn.eu/, last visit on 5th October 2015.

6. Appendix

The first inference engine concerns the assessment of structural vulnerability index as illustrated in the following figures:

Knowledge-base

Ease of installation of the injection device	$\mu_{i,1}$	$\mu_{i,2}$	$\mu_{i,3}$
Easy (E)	50	100	100
Difficult (D)	0	50	100
Very Difficult (VD)	0	0	50



Level of protection of the intrusion site	$\mu_{i,1}$	$\mu_{i,2}$	$\mu_{i,3}$
Low	50	100	100
Medium	0	50	100
High	0	0	50

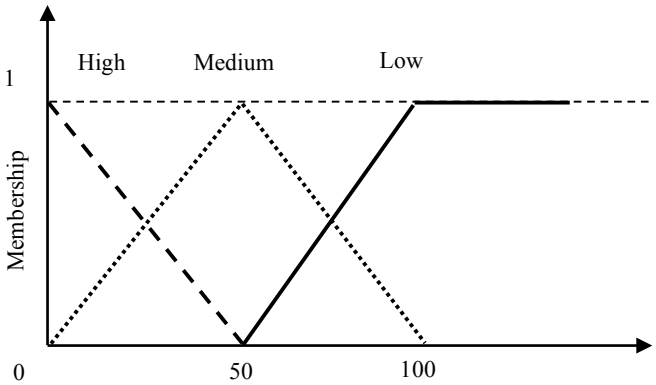


Fig.12. Knowledge-base for the retained criteria: case of structural vulnerability index.

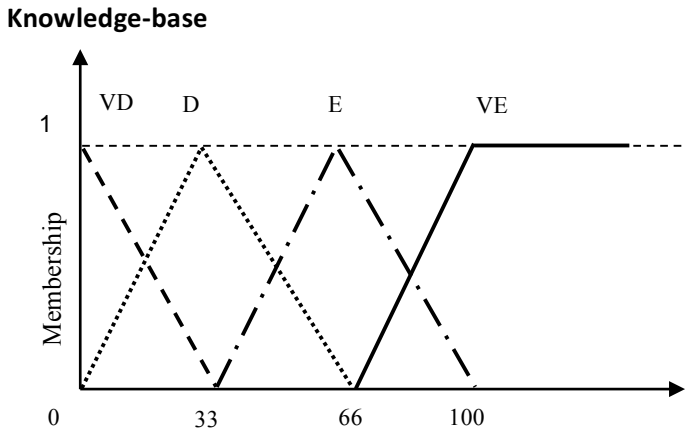
Table10 illustrates the rule base for inference 1 in order to estimate the structural vulnerability. IF *Level of protection* is "P" AND *Ease of installation of the injection device* is "I" THEN Structural vulnerability is "SV".

Tab 10. Rule base for structural vulnerability index assessment

Structural vulnerability (SV)		Ease of installation of the injection device (I)		
		Easy	Difficult	Very Difficult
Level of protection of the intrusion site (P)	Low	High	High	Medium
	Medium	High	Medium	Medium
	High	High	Medium	Low

The second inference engine aims at assessing the vulnerability of intrusion point linked to its environment as illustrated by Figure 12.

Ease of physical access to the intrusion site	$\mu_{i,1}$	$\mu_{i,2}$	$\mu_{i,3}$
Very Easy (VE)	66	100	100
Easy (E)	33	66	100
Difficult (D)	0	33	66
Very Difficult (VD)	0	0	33



Level of surveillance of the intrusion site	$\mu_{i,1}$	$\mu_{i,2}$	$\mu_{i,3}$
Low	50	100	100
Medium	0	50	100
High	0	0	50

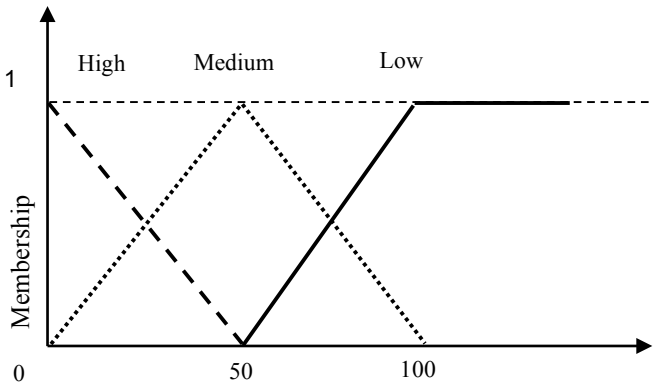


Fig.13. Knowledge-base for the retained criteria: case of vulnerability linked to the environment.

Table 11 illustrates the rule base for inference 2 to estimate the intrinsic vulnerability linked to the environment. **IF** *Level of surveillance* is "S" **AND** *Ease of physical access* is "A" **THEN** Vulnerability linked with the environment is "VE"

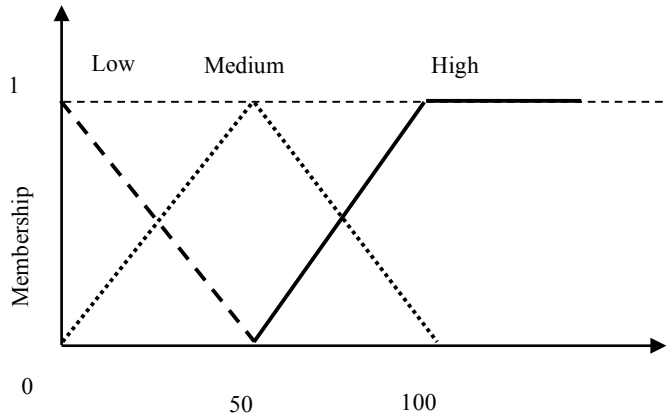
Tab 11. Rule base for vulnerability linked to the environment of intrusion point.

Vulnerability linked with the environment of the intrusion site (VE)		Ease of physical access to the intrusion site (A)			
		Very easy	Easy	Difficult	Very difficult
Level of surveillance of the intrusion site (S)	Low	High	High	Medium	Medium
	Medium	High	High	Medium	Low
	High	High	Medium	Low	Low

The last inference engine concerns the assessment of intrinsic vulnerability index based on the aggregation of previous indexes. The knowledge-base of inference 3 is illustrated by the Figure 13.

Knowledge-base

Structural Vulnerability	$\mu_{i,1}$	$\mu_{i,2}$	$\mu_{i,3}$
High	50	100	100
Medium	0	50	100
Low	0	0	50



Vulnerability linked with the environment of the intrusion site	$\mu_{i,1}$	$\mu_{i,2}$	$\mu_{i,3}$
High	50	100	100
Medium	0	50	100
Low	0	0	50

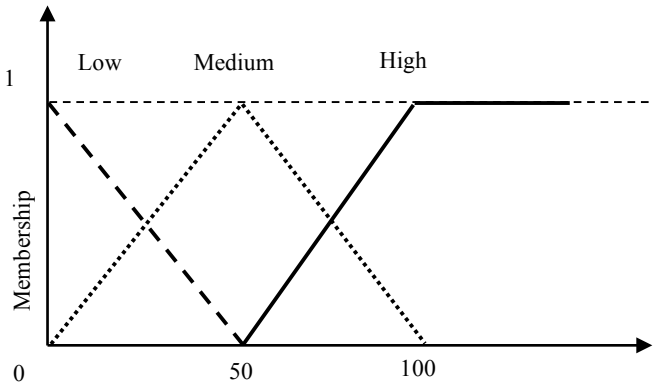


Fig.14. Knowledge-base for the retained indexes:case of intrinsic vulnerability index.

The table 6 illustrates the rule base for inference 3 to estimate the intrinsic vulnerability linked to the environment. **IF** *Vulnerability linked with the environment of the intrusion site (VE)* is "SE" **AND** *Structural Vulnerability* is SV" **THEN** Intrinsic Vulnerability is "IV".

Tab 12. Rule-base for the assessment of intrinsic vulnerability.

Intrinsic vulnerability (IV)		Structural Vulnerability (SV)		
		Low	Medium	High
Vulnerability linked with the environment of the intrusion site (SE)	Low	Low	Medium	Medium
	Medium	Medium	Medium	High
	High	Medium	High	High

.