CONSENSUAL DYNAMICS AND CHOQUET INTEGRAL IN AN ATTACK TREE-BASED FRAUD DETECTION SYSTEM

Alessandro Buoni[1] and Mario Fedrizzi[2]
[1] *IAMSR, Turku Centre for Computer Science, Joukahaisenkatu 3-5 B, 20520 Turku, Finland*
[2] *Department of Computer and Management Sciences, University of Trento, Trento, Italy*

Keywords: Fraud detection, Attack tree, Consensus, Choquet integral.

Abstract: In this paper we extend two modules of the multi-agent system FIDES (Fraud Interactive Detection Expert System) previously introduced in Buoni et al. (2011), and involving the attack tree representation of fraudulent attacks. First, assuming that the opinions of experts involved in the design of the attack tree are represented by fuzzy preference relations, we introduce a dynamical consensus model aiming at finding a shared representation of the attack tree. Second, assuming that the leaf nodes of the attack tree are attribute fuzzy numbers valued and that the attributes are interdependent, we show how to propagate the values up the tree through an aggregation process based on Choquet integral.

1 INTRODUCTION

KPMG Fraud survey (KPMG 2009), conducted on executives of U.S. companies, shows that the most important sources to detect fraud are internal audit (47%) and employee whistle blowers (20%).
An audit team (experts) have to deal with both numerical data and unusual behaviours, create different scenario, develop risk indicators to detect and prevent fraud.

In order to achieve this goal, experts analyse information about the past fraud cases, as collected by inspectors along the processes. Reuse this information and deal with this huge amount of data is a typical knowledge management problem.

A system to support the work of experts has to take into considerations the complexity of managing this kind of information, affected by imprecision, uncertainty, behavioural aspects, and false alarms.

Moreover, one critical issue to address is to aggregate the judgments of the single experts in order to extract useful knowledge in a structured way, develop countermeasures to detect frauds in real time, activate effective strategies to prevent and adapt them when new unusual schemes happen.

Several authors have demonstrated that a multi-agent approach is particularly suitable to address fraud detection when behavioural aspects play a key role, see for instance Chou et al. (2007), Wang et al. (2009), and Zhang et al. (2008).

Accordingly, in Buoni et al. (2011) we introduced FIDES (Fraud Interactive Detection Expert System), a multi-agent system combining think-maps, attack trees, and fuzzy numbers under a Delphi-based team work support framework, to offer to the experts an innovative and suitable way to better understand and manage fraud schemes.

The system has been developed in cooperation with a group of analysts coming from the risk management department of a leading European bank.

The most critical issue to address in FIDES is to perform the Delphi process aiming to select the nodes and connect them in order to design the attack tree that is used to systematically categorize the different ways in which a system can be attacked.

In this paper, at first we extend the Delphi module of FIDES introducing a dynamical consensus model based on individual fuzzy preferences representing the opinions of experts.

Secondly, assuming that to the leaves of the attack tree fuzzy attribute values are associated, we propose an innovative approach for aggregating these values based on Choquet integral.

The paper is organized as follows. The second section is devoted to a short description of FIDES. In the third section we introduce the consensus mechanism based on a dynamical model updating the fuzzy preference of the experts. Section four addresses the aggregation of attribute values using

Buoni A. and Fedrizzi M..
CONSENSUAL DYNAMICS AND CHOQUET INTEGRAL IN AN ATTACK TREE-BASED FRAUD DETECTION SYSTEM.
DOI: 10.5220/0003730602830288
In *Proceedings of the 4th International Conference on Agents and Artificial Intelligence* (ICAART-2012), pages 283-288
ISBN: 978-989-8425-95-9

the Choquet integral. The last section is devoted to conclusions and perspectives on future work.

2 CONSENSUSUAL MODELING OF THE ATTACK TREE

The Fraud Interactive Detection Expert System (FIDES) has been introduced at first in Buoni et al. (2010) and then extended in Buoni et al. (2011).

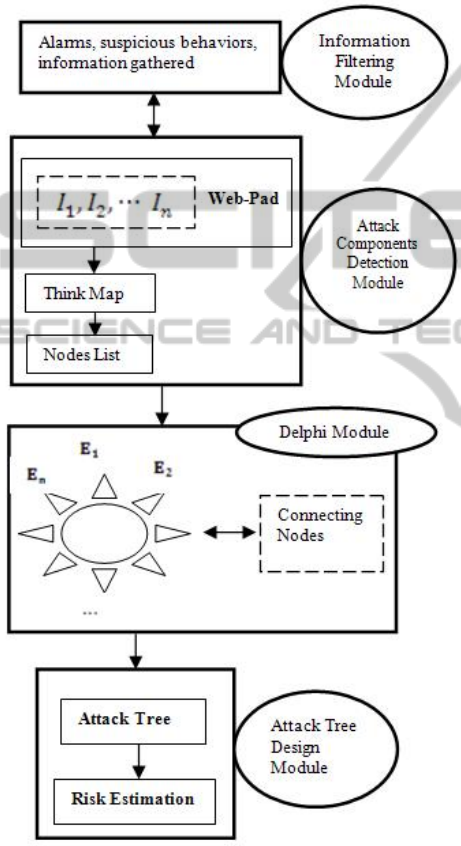

Figure 1: The architecture of FIDES.

As shown in Fig.1, FIDES has four modules. In the Information Filtering Module, alarms, suspicious behaviours and information gathered by inspectors during their inspections or through whistle blowers, are evaluated.

All this information is then processed in the Attack Components Detection Module. Inspectors using Web-Pad (Oxman 2004) can organize all this information in a think-map, i.e. a representation of a possible attack where three main elements are visible and connected: the action perpetrated the suspected person and suspicious behaviours, which might be connected with the other two elements.

Using the think map as a model, inspectors create nodes, which are elementary attacks, to be sent to the audit team experts.

The third module is founded on the Delphi method (Gordon 1994), it is an interactive and iterative method, typically based on questionnaires, where experts, supported by a moderator, try to refine their opinions after each round, in order to structure a description of the components of the fraud attack, based on an attack tree (Schneier, 1999).

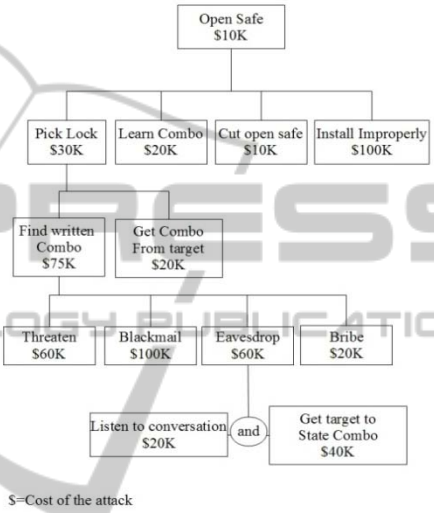

Figure 2: An example of attack tree (Schneier 1999).

The design of the attack tree starts from the set of possible nodes previously determined by the inspectors with the help of the think-maps. Accordingly, the moderator can choose which nodes are parents (V) (with descendant) and which ones are leaves (L) (without descendants, i.e. basic attack components) obtaining two sets $L = \{l_1,..., l_s\}$ and $V = \{v_1,...,v_t\}$.

Then, each expert is asked to elicit his/her own preference with respect to the strength of connections between the elements of L and V. The individual preferences are represented as fuzzy preference relations defined on the set $P = L \times V$. The first goal to achieve is to find a consensual preference setting activating a Delphi session. To this aim, we introduce a dynamical consensus model based on the updating of the individual fuzzy preferences expressed by the group of experts on the set of pairs (l_i, v_j). The modelling framework here used is that one described for first in Kacprzyk and Fedrizzi (1986) and then extended by Fedrizzi et al (1999) through the introduction of a consensual network dynamics that can be regarded as an

unsupervised learning algorithm.

The point of departure is a set of individual fuzzy preference relations defined on $P = \{p_1, \dots, p_M\}$ for each expert in the set $E = \{e_1, \dots, e_N\}$. The fuzzy preference relation of expert e_i, R_i, is given by its membership function $\mu_i: P \times P \rightarrow [0,1]$ such that

$\mu_i(p_k, p_l) = 1$, if p_k is definitely preferred over p_l,

$\in (0.5, 1)$, if p_k is preferred over p_l,

$= 0.5$, if there is indifference between p_k and p_l

$\in (0, 0.5)$, if p_l is preferred over p_k,

$= 0$, if p_l is definitely preferred over p_k.

where $i = 1, \dots N$ and $k, l = 1 \dots M$.

Each individual fuzzy preference relation R_i can be represented by a matrix $[r^i_{kl}], r^i_{kl} = \mu_i(a_k, a_l)$, which is commonly assumed to be reciprocal, that is $r^i_{kl} + r^i_{lk} = 1$. Clearly, this implies $r^i_{kk} = 0.5$ for all $i = 1, \dots, N$ and $i = 1, \dots, M$.

In the soft consensus model each expert is represented by a pair of connected nodes, a primary node and a secondary node. The N primary nodes form a fully connected sub network and each of them encodes the preference of a single expert. The N secondary nodes, on the other hand, encode the individual preferences originally declared by the experts and each of them is connected only with the associated primary node.

Moreover, for the sake of simplicity, let us assume that the alternatives available are only two, that is M=2, which means that each (reciprocal) individual fuzzy preference relation R_i, has only one degree of freedom, denoted by $x_i = r^i_{12}$. Accordingly, the preference originally declared by expert e_i will be denoted s_i.

The iterative process of preference transformation corresponds to the gradient dynamics of a cost function W, depending on both the present and the original network configurations. The value of W combines a measure V of the overall disagreement in the present network configuration and a measure U of the overall change from the original network configuration.

The diffusive interaction between primary nodes i and j is mediated by the interaction coefficient $v_{ij} \in (0,1)$, whereas the inertial interaction between primary node i and the associated secondary node is mediated by the interaction coefficient $u_i \in (0,1)$,

$$v_{ij} = f'((x_i - x_j)^2 \text{ and } u_i = f'((x_i - s_j)^2 \quad (1)$$

The values of the interaction coefficients are given by the derivative of a scaling function f (see Figure 3).

The diffusive component of the network dynamics results from the consensual interaction between each node x_i and the remaining $N-1$ nodes $x_{j \neq i}$ in the network. The aggregated effect of these $N-1$ interactions can be represented as a single consensual interaction between node x_i and a virtual node $\bar{x}_i$ containing a particular weighted average of the remaining preference values.

The interaction coefficient $v_i \in (0,1)$ of this aggregated consensual interaction controls the extent to which expert e_i is influenced by the remaining experts in the group.

$$f(x) = -\frac{1}{\beta} \ln(1 + e^{-\beta(x-\alpha)}) \qquad f'(x) = \frac{1}{1 + e^{\beta(x-\alpha)}}$$

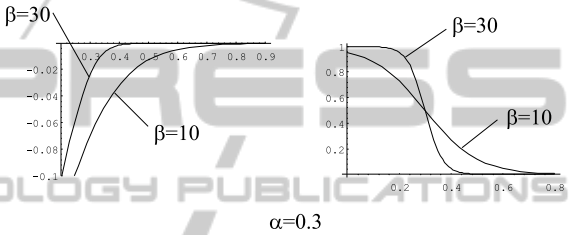

Figure 3: Scaling function f and sigmoid function f′.

In our soft consensus model the value v_i, as well as the weighting coefficients $v_i \in (0,1)$ in the definition of $\bar{x}_i$ as given below, depend non-linearly on the standard Euclidean distance between the opinions x_i and x_j,

$$v_i = \sum_{j \neq i} v_{ij} / (n-1)$$

$$\bar{x}_i = \frac{\sum_{j \neq i} v_{ij} x_j}{\sum_{j \neq i} v_{ij}}$$

The individual disagreement cost $V(i)$ is given by $V(i) = \sum_{j \neq i} V(i,j)/(n-1)$ where $V(i,j) = f((x_i - x_j)^2)$ and the individual opinion changing cost is

$$U(i) = f((x_i - s_j)^2) \quad (2)$$

Summing over the various experts we obtain the collective disagreement cost V and inertial cost U, $V = \frac{1}{4}\sum_i V(i)$ and $U = \frac{1}{2}\sum_i U(i)$, where 1/4 and !/2 are conventional multiplicative factors.

The full cost function W is then

$$W = (1-\lambda)V + \lambda U \text{ with } 0 \leq \lambda \leq 1. \quad (3)$$

The consensual network dynamics, which can be regarded as an unsupervised learning algorithm, acts

on the individual preference x_i through the iterative process

$$x_i \to x_i' = x_i - \varepsilon \frac{\partial W}{\partial x_i}. \quad (4)$$

We can analyse the effect of the two dynamical components V and U separately. The dissensus cost V induces a non-linear process of diffusion based on the gradient term

$$\frac{\partial V}{\partial x_i} = v_i(x_i - \bar{x}_i) \quad (5)$$

As a result, the iterative step of the non-linear diffusion mechanism corresponds to a convex combination (with sufficiently small ε) between the opinion value x_i and the weighted average $\bar{x}_i$ of the remaining preference values x_j,

$$x_i' = (1 - \varepsilon v_i)x_i + \varepsilon v_i \bar{x}_i \quad (6)$$

The inertial cost, on the other hand, leads to a non-linear mechanism which opposes changes from the original opinions x_i, by means of the gradient term

$$\frac{\partial U}{\partial x_i} = u_i(x_i - s_i) \quad (7)$$

The full dynamics associated with the cost function $W = (V + U)/2$ acts iteratively on each decision maker i through convex combinations of the opinion value x_i, the average opinion value $\bar{x}_i$, and the original opinion value s_i.

$$x_i' = \big(1 - \varepsilon(v_i + u_i)\big)x_i + \varepsilon v_i \bar{x}_i + \varepsilon u_i s_i.$$

Accordingly, the expert e_i is in dynamical equilibrium, in the sense that $x' = x_i$, if the following stability equation holds,

$$x_i = (v_i \bar{x}_i + u_i s_i)/(v_i + u_i) \quad (8)$$

that is, if the present preference value x_i coincides with an appropriate weighted average of the original preference s_i and the average preference value $\bar{x}_i$.

3 CHOQUET-BASED VALUATION

In many applications of attack trees, information about attributes is commonly associated to the leaves and one of the main problem to be solved becomes how to promulgate the information up the tree until it reaches the root node. Unfortunately, most of aggregation operators introduced in the literature, e. g. OWA operators (Yager 2008), don't take care of the possible interactions between the nodes. One way to overcome this drawback is to introduce the Choquet integral (Choquet, 1953; Grabisch et alt., 2010) whose distinguished feature is to be able to take into account the interaction between nodes, ranging from redundancy (negative interaction) to synergy (positive interaction).

Moreover, the estimation of the attributes' values is usually based on data type depending on subjective judgements, most commonly represented by natural language expressions. Following Zadeh (1978, 1979), here we assume to translate these expressions into the mathematical formalism of possibility measures and to represent the numeric imprecision of attributes' values using unimodal LR fuzzy numbers, as fuzzy subsets of the set of real numbers (Dubois and Prade, 1987).

Definition 1. An unimodal LR fuzzy number A is defined by

$$A(x) = \begin{cases} L\left(\dfrac{a - x}{a_1}\right) & \text{for } a - a_1 \le x \le a, \\ R\left(\dfrac{x - a}{a_2}\right) & \text{for } a \le x \le a + a_2 \\ 0 & \text{else}, \end{cases} \quad (9)$$

where a∈R is the peak of A, α>0 and β>0 are the left and the right spread, respectively, and L,R:[0,1]→[0,1] are two strictly decreasing continuous shape function such that L(0)=R(0)=1 and L(1)=R(1)=0.

Extending the Choquet integral to a fuzzy domain several forms of information can be handle at the same time, i.e. crisp data, interval values, fuzzy numbers and linguistic variables (Yang, 2005).

At first, the Choquet integral is defined for a measurable interval-valued function (Aumann, 1965), and then it's extended to fuzzy integrand using the alpha-cuts (Grabisch, 1995).

From now on, we introduce the following notations:

- $\mathcal{I}$ the set of interval numbers (rectangular fuzzy numbers)
- N={1,2,…,n} a set of elements
- $F : N \to \mathrm{I}$ an interval-valued function
- $F_L(i)$ and $F_R(i)$ respectively the left end point and the right end point of the interval $F(x)$
- $\mathcal{F}$ the set of all unimodal LR-type fuzzy numbers

- $[{}^{L}A^{\alpha}, {}^{R}A^{\alpha}]$, the alpha-cut of fuzzy number A
- $\Phi : N \rightarrow F$ a unimodal LR fuzzy-valued function
- $\mathcal{F}$-tree, an attack tree whose leaves' values are unimodal LR fuzzy numbers

The following definitions are due to Yang (2005):

Definition 2. $F(i)$ is measurable if both $F_L(i)$ and $F_R(i)$ are measurable functions.

Definition 3. The Choquet integral of $F(i)$ with respect to a fuzzy measure μ is defined as $\int F d\mu = \{ \int G d\mu \mid G(i) \in F(i) \quad \forall i \in N, \text{ and } G(i) \text{ (measurable)} \}$.

Definition 4. $\Phi(i)$ is measurable if its alpha-cuts $\Phi^{\alpha}(i)$ are measurable interval-valued functions for every $\alpha \in (0,1]$.

Definition 5. Given a measurable fuzzy-valued function $\Phi(i)$ on N and a fuzzy measure μ on 2^N, the Choquet integral of $\Phi(i)$ with respect to μ is defined as

$$\int \Phi d\mu = \bigcup_{0 \le \alpha \le 1} \alpha \int \Phi^{\alpha} d\mu \tag{10}$$

Accordingly, the calculation of the Choquet integral with a fuzzy-valued function depends on the calculation of the Choquet integral with interval-valued functions, and the following proposition can be proved (Grabisch, 1995).

Proposition 1. Given the measurable interval-valued function Φ^{α} and the fuzzy measure μ on 2^N, the Choquet integral of Φ^{α} with respect to μ is

$$\int \Phi^{\alpha} d\mu = [\int \Phi_L^{\alpha} d\mu, \int \Phi_R^{\alpha} d\mu] \tag{11}$$

Therefore (5.2) becomes

$$\int \Phi d\mu \bigcup_{0 \le \alpha \le 1} \alpha = [\int \Phi_L^{\alpha} d\mu, \int \Phi_R^{\alpha} d\mu] \tag{12}$$

Consider now an $\mathcal{F}$-tree whose leaves' values are unimodal LR fuzzy numbers.

To prove that the root value is still an unimodal LR fuzzy number, we introduce the following

Proposition 2. The Choquet integral of unimodal LR fuzzy numbers is still an unimodal LR fuzzy number.

Proof. A generic unimodal LR fuzzy number A is characterized by an alpha-cut $[{}^{L}A^{\alpha}, {}^{R}A^{\alpha}]$, where L^{α} and R^{α} are strictly monotonic continuous functions (with respect to α).

Consider now a set of unimodal LR fuzzy numbers $\{A_1, \ldots, A_k\}$. If we aggregate these fuzzy numbers through Choquet integral with respect to a fuzzy measure μ, we obtain a fuzzy number A characterized by the alpha-cut $[{}^{L}A^{\alpha}, {}^{R}A^{\alpha}]$, where,

$$ {}^{L}A^{\alpha} = C_{\mu}[{}^{L}A_1^{\alpha}, \ldots, {}^{L}A_k^{\alpha}], $$
$$ {}^{R}A^{\alpha} = C_{\mu}[{}^{R}A_1^{\alpha}, \ldots, {}^{R}A_k^{\alpha}] . $$

In fact, from the strict monotonicity of the Choquet integral, and given that the lower bound of each alpha-cut is less than the relative upper bound, we have $[{}^{L}A^{\alpha} < {}^{R}A^{\alpha}]$.

Moreover, if we consider $0 \le \alpha_1 \le \alpha_2 \le 1$ since ${}^{L}A_i^{\alpha_1} < {}^{L}A_i^{\alpha_2}$ and ${}^{R}A_i^{\alpha_1} > {}^{R}A_i^{\alpha_2} \quad \forall i = 1, \ldots, k$, from the strict monotonicity of the Choquet integral we have

$$ {}^{L}A^{\alpha_1} < {}^{L}A^{\alpha_2} \qquad {}^{R}A^{\alpha_1} > {}^{R}A^{\alpha_2} . $$

Then L^{α} and R^{α} are strictly monotonic functions (with respect to α). Moreover, since Choquet integral is a continuous aggregation function, all L_i^{α} and R_i^{α} are continuous functions $\forall i = 1, \ldots, k$, and the composition of continuous functions is continuous, then it follows that L^{α} and R^{α} are continuous functions (with respect to α).

Then, as an immediate consequence of Prop. 2, starting from the leaves and carrying on a bottom up Choquet aggregation, the obtained tree root's value is again an unimodal (continuous) LR fuzzy number.

The algorithm proceeds as described below. First of all, the alpha-cuts of each unimodal LR fuzzy number in the leaves will be considered, using a suitable grid. The procedure receives the extremes of the alpha-cut, and computes the aggregated value for both the lower and the upper bounds. Increasing the values of alpha in between [0,1], the two computed values form and interval included in the previous ones (for lower value of alpha). Thus the obtained intervals form the alpha-cuts of the fuzzy root, i.e. the required solution.

4 CONCLUSIONS

In this paper, at first we developed a consensual network dynamics aiming at supporting the negotiation process of a group of experts involved in the description of a fraudulent attack through a tree structure.

Secondly, assuming that the leaves of the attack tree are equipped with attribute values represented

by LR fuzzy numbers, we propose an algorithm for aggregating these values using the Choquet integral, whose distinguished feature is to be able to take into account the interaction between nodes.

Future work will be devoted to the introduction of case-based reasoning techniques combined with multi criteria models to improve the joint evaluation of risk and uncertainty of the attacks useful for estimating the prevention costs.

REFERENCES

Aumann R. J. (1965). Integrals of set-valued functions, Journal of Mathematical Analysis with Applications, 12, 1-12, 1965.

Buoni, A., Fedrizzi, M., Mezei, J. (2010). A Delphi-based approach to fraud detection using attack trees and fuzzy numbers. In *Proceeding of the International Association for Scientific Knowledege*. Oviedo, November 8-10.E-Alt & InterTic.

Buoni, A., Fedrizzi, M., Mezei, J. (2011). Combining attack trees and fuzzy numbers in a multi-agent approach to fraud detection, International Journal of Electronic Business (forthcoming).

Choquet G. (1953). Theory of capacities, Annales de l'Institut Fourier, 5, 131-295.

Chou, C.L-Y, Du, T., Lai, S. V, (2007), Continuous auditing with a multi-agent system. Decision Support Systems, 42 (4) 2274-2292.

Dubois, D. and Prade, H., (1987).Fuzzy numbers: An overview, Analysis of Fuzzy Information - Vol. I: Mathematics and Logic, J. Bezdek, ed., CRC Press, Boca Raton, 3-39.

Kacprzyk, J. and Fedrizzi, M. (1988). A “soft” measure of consensus in the setting of partial (fuzzy) preferences. European Journal of Operational Research, 34, 316–325.

Fedrizzi, M., Fedrizzi, M., and Marques Pereira, R. A. (1999). Soft consensus and network dynamics in group decision making. International Journal of Intelligent Systems, 14, 63–77.

Gordon, T. J. (1994). The Delphi method in futures research methodology. AC/UNU Millenium Project, Washington, AC/UNU.

Grabisch M., Nguyen H. T., Walker E. A. (1995). Fundamentals of Uncertainty Calculi, with Applications to Fuzzy Inference. Kluwer, Boston, MA.

Grabisch, M., Labreuche (2010). A decade of application of the Choquet and Sugeno integrals in multi-criteria decision aid, Annals of Operations Research, 175, 247-286.

Hand, D. J. (2007). Statistical techniques for fraud detection and evaluation. Available at: <http://lang tech.jrc.ec.europa.eu/mmdss2007/htdocs/Presentations /Docs/MMDSS_Hand_PUBLIC.pdf.>

KPMG Fraud survey (2009). Available at: <http://www. kpmginstitutes.com/aci/insights/2009/pdf/kpmg-fraud-survey-2009.pdf>.

Oxman, R. (2004). Think-maps: teaching design thinking in design education. Design Studies. Vol. 25, Number 1.

Schneier, B. (1999). Attack trees. Available at: <http: //www.schneier.com/paper-attacktrees-ddjft.html>.

Yager, R. R. (2006). OWA trees and their role in security modelling using attack trees. Information Sciences, 176, 2933-2959.

Yang R., Wang Z., Heng P. A., and Leung K. S. (2005). Fuzzy numbers and fuzzification of the Choquet integral, Fuzzy Sets and Systems, 153, 95-113.

Wang, D. G., Li, T., Liu, S. J. L, Liang, G., Zhao, K. (2008). An immune multi-agent system for network intrusion. *Proceedings of the third International Symposium on Intelligence Computation and Applications*, (LNCS 5370, Springer-Verlag Berlin Heidelberg), 436-445.

Zadeh, L. (1978). Fuzzy sets as a basis for a theory of possibility, Fuzzy Sets and Systems 1, 3-28.

Zadeh, L. (1979). A theory of approximate reasoning. In Hayes, J., Michie, D., and Mikulich, L., editors, Machine Intelligence 9, Halsted Press, New York, 149-194.

Zhang, L. S., Zhou, N., Wu, J. X. (2008). The fuzzy integrated evaluation of embedded system security. *International Conference on Embedded Software and Systems*, 157-162.