Ontology and Fuzzy Measures based System for Information Security Risk Assessment

Raihan Muratkhan, Dauren Kabenov and Dina Satybaldina

L. Gumilyov Eurasian National University, 5 Munaitpasov str., 010000 Astana, Kazakhstan

Abstract. Traditionally the information security risk is defined as a combination of probability of negative event and a potential impact. But risk of the breach of information security of the modern organization is the multidimensional complex concept which is including set of interconnected variables. Often values of risk factors cannot be precisely defined. Therefore the information security risk assessment may be defined as a fuzzy problem. In this paper algorithm of the problem decision of alternative's assessment which has network-like estimation criteria structure is considered. Connections in criteria structure are formalized by means of fuzzy integral of Sugeno. Ontology-based information security knowledge domain has net-like structure incorporating the most relevant information security concepts (assets, threats, vulnerabilities and controls) and relations among them. Slots describe properties of concepts and instances. Each property can be set to a specific fuzzy value. The estimation criteria structure is network-like and is formalized as the oriented graph with one source and many drains. The alternative's estimation result is calculated in criterion-source.

1 Introduction and Related Work

Computational Intelligence (CI) is as advanced low level artificial intelligence that uses computational adaptation to mimic human logic and reasoning. CI can be realized in a number of different ways [1]. CI core methods such as artificial neural networks, fuzzy systems, evolutionary computation, artificial immune systems, swarm intelligence, and soft computing are described in [2]. The authors analyze a significant number of research works and provide useful insights into how CI might be used in an intrusion detection system. It was shown that many of these CI technologies could easily be adapted to be used as mechanisms that can deal with the numerous securities.

On the other hand recent studies have shown that the lack of information security knowledge at the management level is one reason for inadequate or non-existing information security risk management strategies [3].

Authors of [4] identified information security risk management as one of the top ten grand challenges in information technology security and demanded sound theories and techniques to support and enhance existing risk management approaches.

Incomplete knowledge about the information security domain in general and the

Muratkhan R., Kabenov D. and Satybaldina D..
Ontology and Fuzzy Measures based System for Information Security Risk Assessment.
DOI: 10.5220/0004097800770084
In *Proceedings of the 9th International Workshop on Security in Information Systems* (WOSIS-2012), pages 77-84
ISBN: 978-989-8565-15-0

current information security status of the organization was one of the main problems in information security risk management. A creation of ontologies (e.g. General Privacy Ontology [5], Security Ontology [6], NRL Security Ontology [7]) that define the conceptual system of the subject area of information security reduced the severity of the problem.

The essence of estimation problems consists in the following. On the basis of set of alternative's characteristics values it is necessary to receive a unique estimation of this alternative according to the criteria system. The criteria system is considered as the estimation standard (ideal alternative). The estimation is considered as conformity degree of this alternative to ideal alternative. Solutions of the multy-criteria problems of assessment and classification with using of the integral of Sugeno or Choquet are known [8-10]. However hierarchical problems with not crossed branches of hierarchy are mainly considered in publications. It is essential restriction for many applications. Therefore a universal algorithm development for solution of the fuzzy problems of network structure criteria assessment is importance aspect. In this work the information security risk estimation algorithm on the base of fuzzy measures is considered. Reuse-used ontology [6], developed by authoritative experts in the field of ontological modeling is a positive feature of the approach of risk analysis

2 Decision Algorithm of Fuzzy Assessment Problems with Network-like Criteria Structure

The considered algorithm provides the problem decision of alternative's estimation which has network-like estimation criteria structure. Criteria can be quantitative and qualitative. Quantitative criteria correspond to alternative's characteristics which are measured in quantitative scale. Qualitative criteria correspond to alternative's characteristics which are measured in qualitative discrete scales. The algorithm estimates alternative in several criterion contexts. Use of contexts provides the description of network-like criteria structure. Criterion contexts formalize the different view-points on estimation value. Connections in criteria structure are formalized by means of fuzzy measures Sugeno.

Let's consider formal representation of criteria's system with network-like structure. We are denoting set of estimation criteria:

$$C = \{c_i, i = \overline{1, Q^C}\} \tag{1}$$

The criteria system is formed by means of relations set. Relations can have various senses which depend on a problem. For example, relations can reflect functional dependences of criteria or attributive connections. By analogy to the graphs theory, the criteria system is the acyclic oriented graph with one source *cs* (the upper-level criterion) and with many drains (the lower-level criteria)

$$CD = \{cd_j \in C, j = \overline{1, Q^{CD}}\} \tag{2}$$

without dangling tops. The set *CD* is considered to be as the set of alternative's characteristics. This set also is universal set in estimation problem.

Using fuzzy measures and fuzzy integrals, it is possible to construct the algorithm for estimation problem decision. This algorithm will consist of following steps.

1) Transformation of alternative's characteristics values to values which are assigned on discrete set D_i^{CD}

Transformation is performed for formation of membership h_i, which is used for integration in quantitative criterion c_i. Transformation is performed differently for qualitative and quantitative characteristics of alternative.

For Qualitative Characteristics of Alternative. The assignment of qualitative characteristics is performed directly on discrete set. Estimations of alternative's qualitative characteristics are represented as membership

$$h : D_j^{CD} \to [0,1] \qquad (3)$$

For Quantitative Characteristics of Alternative. For quantitative characteristics this transformation is performed by means of linguistic variable, for example as shown in [9].

To each quantitative criterion c_i the linguistic variable is attributed:

$$T_i = \{(d_{ij}^{CD}, t_{ij}), j = \overline{1, Q^{D^i}}; t_{ij} : [R_{ij}^{\min}, R_{ij}^{\max}] \to [0,1] \qquad (4)$$

where $[R_{ij}^{\min}, R_{ij}^{\max}]$ - is numerical interval which can be various for different pairs (d_{ij}^{CD}, t_{ij}).

The linguistic variable T_i is composed of functions which correspond to values set elements of drain-criterion. These functions are assigned on numerical intervals. The membership for integration is determined as the conformity degree of characteristic's value to linguistic descriptions d_{ij}^{CD}:

$$h_i = \{e_{ij} = \max[R_{ij}^{\min}, R_{ij}^{\max}] \min(t_{ij}, r_i), j = \overline{1, Q^{D_i}} \qquad (5)$$

2) Consecutive aggregation of alternative's characteristics values in criteria. To each criterion the set of fuzzy measures according to elements quantity of criterion determination set is attributed:

$$M_i = \{\mu_{ij}(\bullet) : 2^{D^i} \to [0,1], j = \overline{1, Q^{SD_{i_i}{}^{i}}} \qquad (6)$$

This set is named as criterion contexts. For source-criterion the context is the self criterion. Fuzzy measures are determined on values set of criterion.

The fuzzy integral of membership along fuzzy measure μ_{ij} provides calculation of an alternative's estimation in criterion c_i for context j:

$$e_{ij} = (s)\int_{D_i} h_i, j = \overline{1, Q^{S_i}}; \qquad (7)$$

where membership is composed of alternative's estimations in criteria from D_i. Integration is performed consistently in all tops of criteria structure.

3 Security Ontology

Ontology is an explicit formal specification of the terms in explicit specifications the domain and relations among them [11]. Ontologies are useful as means to support sharing and reutilization of knowledge [12]. This reusability approach is based on the assumption that if a modeling scheme, i.e., ontology, is explicitly specified and mutually agreed upon by the parties involved, and then it is possible to share, reutilize and extend knowledge. Many disciplines now develop standardized ontologies that domain experts can use to share and annotate information in their fields. Problem-solving methods, domain-independent applications, and software agents use ontologies and knowledge bases built from ontologies as data [13].

Reusing existing ontologies may be a requirement if our system needs to interact with other applications that have already committed to particular ontologies or controlled vocabularies [13]. There are libraries of reusable ontologies on the Web and in the literature, for example, the Ontolingua ontology library [14], or the DAML ontology library [15].

An ontology is a formal explicit description of concepts in a domain of discourse (*classes* (sometimes called *concepts*)), properties of each concept describing various features and attributes of the concept (*slots* (sometimes called *roles* or *properties*)), and restrictions on slots (facets (sometimes called *role restrictions*)) [15]. Ontology together with a set of individual instances of classes constitutes a knowledge base.

Ontology development includes [15]:

- defining classes in the ontology,
- arranging the classes in a taxonomic (subclass– superclass) hierarchy,
- defining slots and describing allowed values for these slots,
- filling in the values for slots for instances.

Security Ontology [6] was used in this work. It was proposed based on the security relationship model described in the National Institute of Standards and Technology Special Publication 800-12 [16]. Figure 1 shows the high-level concepts and corresponding relations of ontology.

Slots describe properties of classes and instances. Each property can be set to a specific value or a formula to calculate this value of the property. All subclasses of a class inherit the slot of that class. On the other hand, subclasses can have their own properties.

Fragments of the ontology, including the structure and properties of concepts are the basis for description of the situation, which is determined by the input data. The concepts and relationships defined by the input conditions are introduced in addition to these ontology fragments.

The security ontology comprises about 500 concepts and 600 formal restrictions; to ensure a minimal encoding bias the ontology is represented by either graphical, textual, or description logics (DL) representations, which were used to represent knowledge in a structured, formal, and reasonable form.

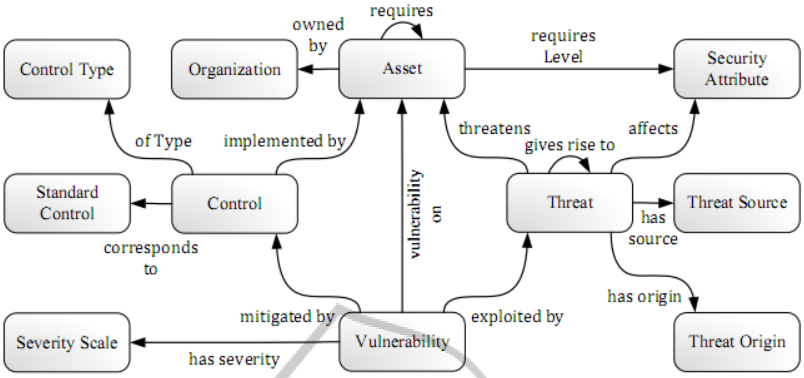

Fig. 1. High-level concepts and corresponding relations of ontology [6].

4 Proposed Concept of Information Security Risk Assessment System

Most existing risk analysis models are based on quantitative techniques such as Monte Carlo Simulation and Annual Loss Expectancy. However, the information that is related to most uncertainty factors is not numerical. FST provides an approximate model for the evaluation of the risk faced by EC projects through a linguistic approach. The procedure for fuzzy risk analysis is based on the works from [17] that consisted of five steps: risk identification, natural language representation, fuzzy assessment aggregation, and linguistic approximation.

The first step is to conduct risk identification and compile a list of the most significant uncertainty factors and their descriptions. Before conducting fuzzy risk analysis, one must identify the components of risks for the assets on the security ontology base.

Knowledge base (metaclasses of the assets, threats, vulnerabilities, evaluation criteria, etc) are developed with based on a comprehensive literature review and interviewed with practicing auditors of an information security management system [18,19].

Information security risk is a function of the likelihood of a given threat-source's a particular potential vulnerability, and the resulting impact of that adverse event on the organization. To determine the likelihood of a future adverse event, threats to an IT system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT systems. The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. Therefore, it is necessary to consider a large set of information sources and uncertainty of the information. On the second step (natural language representation) the linguistic terms sets, characterizing values of input parameters (asset value, asset criticality, threat level, vulnerability level, impact level) and an output parameter (risk level) are defined (see Table 1).

Table 1. Membership functions and the triangular fuzzy numbers of the linguistic term.

Likelihood	Severity		
Unlikely	Low	=1-4x	$0 \le x \le 0.25$
Medium	Moderate	=2(1-2x)	$0.25 \le x \le 0.5$
Likely	High	=3-4x	$0.5 \le x \le 0.75$
Very likely	Critical	=4x-3	$0.75 \le x \le 1$

In third stage (fuzzy assessment aggregation) an aggregate of several experts' fuzzy assessment is performed by using the fuzzy average operation for aggregate method. Adequacy of expert's preferences formalization depends on mathematical properties of aggregation operator. Most effective formalization tool for connections between criteria is the fuzzy measure Sugeno. And most effective aggregation tool is the fuzzy integral.

From the mathematical view-point the Sugeno and Choquet integrals are in detail considered in [10]. The Sugeno and Choquet integrals provide various properties of aggregation procedure which depend from properties of fuzzy measure [20]. For probability measure (0 = l) the fuzzy integral is equivalent to additive aggregation. For possibility measure (1 - = l) the fuzzy integral is equivalent to maximum of membership (fuzzy logic "OR"). For necessity measure (0 >> l) the fuzzy integral is equivalent to minimum of membership (fuzzy logic "And"). Other values l will determine other aggregation properties.

As the result of the calculated fuzzy weighted average is a fuzzy number, it is necessary to translate it back into linguistic terms for easy interpretation. The goal of linguistic approximation is to find the linguistic term with the closest possible meaning to that of a defined fuzzy set. There are three techniques in linguistic approximation: best fit, successive approximation, and piecewise decomposition [17]. The difference between these three techniques was discussed by Schmucker [21]. In the present study, the best fit method is adopted because it is easy to understand and easy to implement on computers [21]. This method is based on the ''Euclidean distance'' between two fuzzy sets, as proposed in [22]. The model then assigns the appropriate natural language expression to the lowest Euclidian distance associated with fuzzy set X.

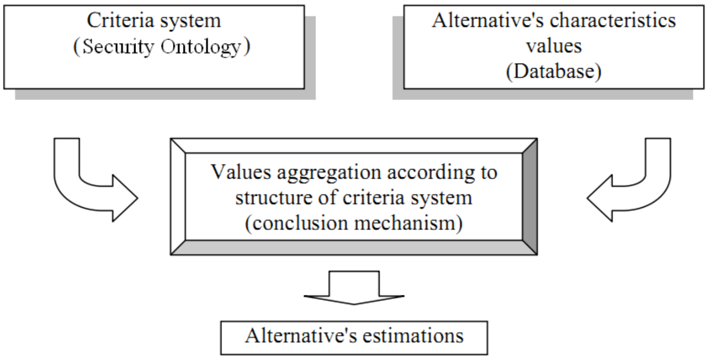
Criteria system
(Security Ontology)
Alternative's characteristics values
(Database)
Values aggregation according to structure of criteria system
(conclusion mechanism)
Alternative's estimations

Fig. 2. Structure of assessment problem decision.

The proposed structure of risk assessment system does not differ from classical structure of expert systems [20]. It is shown in figure 2.

The algorithm is software implemented by authors. The example of the information security risk assessment of the organization according to international standards requirements and preferences of the information assets owner is considered.

5 Conclusions and Future Work

This paper presented an ontology-based approach that addresses the problem of information security risk assessment. The considered algorithm provides the problem decision of alternative's estimation which has network-like estimation criteria structure. Quantitative criteria correspond to alternative's characteristics which are measured in quantitative scale. Qualitative criteria correspond to alternative's characteristics which are measured in qualitative discrete scales.

The algorithm estimates alternative in several criterion contexts. Use of contexts provides the description of network-like criteria structure. Connections in criteria structure are formalized by means of fuzzy measures Sugeno.

The information security risk assessment focused on risk identification, analysis, and prioritization. Less attention was given to the risk management planning, resolution, and monitoring. Further research should be conducted into such risk management planning. In addition, risk monitoring should be conducted regularly to track the status of the identified risks. With such insight and improvement, the proposed approach could be further enhanced to handle the functionality of risk management.

References

1. Mazur, S., Blasch, E., Chen, Y. and Skormin, V.: Mitigating Cloud Computing Security Risks usinga Self-Monitoring Defensive Scheme. Distribution Statement A: Approved for Public Release, (2011) 88ABW-2011-3983.
2. Wu, S. X. and Banzhaf, W.: The use of computational intelligence in intrusion detection systems: A review. Applied Soft Computing, Vol. 10, (2010) 1–35.
3. Straub, D. and Welke, R.: Coping with systems risk: Security planning models for management decision making. MIS Quarterly, Vol. 22(4), (1998) 441-469.
4. Smith, S. and Spaord, E.: Grand challenges in information security: Process and output. IEEE Security & Privacy, Vol. 2(1), (2004) 69-71.
5. Hecker, A., Dillon, T., and Elizabeth, C.: Privacy Ontology Support for E-Commerce, Internet Computing, Issue No. 2, (2008) 54 – 61.
6. Fenz, S. and Ekelhart, A.: Formalizing information security knowledge. ASIACCS ‘09: Proceedings of the 2009 ACM symposium on Information, computer and communications security, ACM, (2009) 183-194.
7. Kim, A, Luo, J. and Myong, K.: Security Ontology for Annotating Resources. Naval Research Lab, NRL Memorandum Report, NRL/MR/5540-05-641: Washington, D.C., (2005).
8. Yeong Min Kima and Chee Kyeong Kimb.: Fuzzy based state assessment for reinforced concrete building structures. Engineering Structures, Vol. 28. 9 (2006) 1286-1297.

9. Magyla, T.: The evaluation implementation impact of centralized traffic control systems in railways. Kaunas University of Technology - Transport, Vol.17, No. 3 (2002) 96-102.
10. Pham, T. and Wagner, M.: Similarity normalization for speaker verification by fuzzy fusion. Pattern Recognition, vol. 33 (2000) 309-315.
11. Gruber, T. R.: Toward principles for the design of ontologies used for knowledge sharing. International. J. of Human-Computer Studies, Vol. 43(5-6), (1195) 907–928.
12. Decker, S., Erdmann, M., Fensel, D. and Studer, D. Ontobroker: Ontology based access to distributed and semi-structured information. DS-8: Semantic Issues in Multimedia Systems, 1999.
13. Noy, Natalya F. and McGuinness, Deborah L.: Ontology Development 101: A Guide to Creating Your First Ontology'. Stanford Knowledge Systems Laboratory Technical Report KSL-01-05 and Stanford Medical Informatics Technical Report SMI-2001-0880, March 2001.
14. The Ontolingua ontology library. [Online] Available from: http://www.ksl.stanford.edu/software/ontolingua/
15. The DAML ontology library. [Online] Available from: http://www.daml.org/ontologies
16. NIST. An Introduction to Computer Security – The NIST Handbook. Technical report, NIST (National Institute of Standards and Technology) (1995). Special Publication 800-12.
17. Ngai, E. W. T. and Wat, F. K. T.: Fuzzy decision support system for risk analysis in e-commerce development. Decision Support Systems, Vol. 40 (2005) 235–255.
18. Satybaldina, D.: A Fuzzy Rule Knowledge-Based System for Information Security Risk Analysis. American Index of Central Asian Scholarship (AICAS), Vol.1, № 2 (2010) 61–67.
19. Satybaldina, D.: A formalized approach to determining security requirements. Proceeding of the Third Congress of the World Mathematical Society of Turkic Countries. Almaty, (2009) 215-221.
20. Sveshnikov,S. and Bocharnikov, V.: Contextual algorithm for decision of fuzzy estimation problems with network-like structure of criteria on the basis of fuzzy measures Sugeno. MPRA Paper No. 17351, posted 17 (2009). [Online] Available from: http://mpra.ub.uni-muenchen.de/17351
21. Schmucker, K. J.: Fuzzy Sets, Natural Language Computations and Risk Analysis, Computer Science Press, Rockville, MD (1984).
22. Dubois, D. and Prade, H.: Fuzzy Sets and Systems, Academic Press, New York (1980).